Chapter 1

Groups

1.1 Definitions and Elementary Properties

Definition 1.1.1. *A **binary operation** $*$ on a set S is a function*

$$\begin{aligned} * : S \times S &\to S \\ (a, b) &\mapsto a * b. \end{aligned}$$

*$*$ is called **associative** if $(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$.*
*$*$ is called **commutative** if $a * b = b * a \quad \forall a, b \in S$.*

Definition 1.1.2. *A **group** consists of a set G together with a binary operation*

$$\begin{aligned} * : G \times G &\mapsto G \\ (g, h) &\mapsto g * h, \end{aligned}$$

such that the following conditions are satisfied:

1. *$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$ (associativity),*
2. *There exists an element $e \in G$ such that $e * a = a$ and $a * e = a \quad \forall a \in G$ (identity),*
3. *For each $a \in G$, there exists an element $b \in G$ such that $a * b = e$ and $b * a = e$ (inverse).*

Definition 1.1.3. *A group $(G, *)$ is called **abelian** (or commutative) if $a * b = b * a \quad \forall a, b \in G$.*

Definition 1.1.4. *Let H be a non-empty subset of the group G. Suppose that the product in G of two elements of H lies in H and that the inverse in G of any element of H lies in H. Then H is called a **subgroup** of G, written $H \leq G$.*

Notation: For $X \subset G$, write

$$\langle X \rangle = \bigcap_{X \subset H \leq G} H.$$

This is called **the subgroup of G generated by X**.
Exercise: show that $\langle X \rangle$ is a subgroup.

Example 1.1.5.

1. ***Cyclic groups C_n***
Let $n \in \mathbb{N}$. $C_n := \{e = x^0, x, x^2, \dots, x^{n-1}\}$, with multiplication $x^j * x^k := x^{(j+k) \bmod n}$.
Also, the infinite cyclic group is $C_\infty := \{x^n \mid n \in \mathbb{Z}\}$ with $x^j * x^k := x^{j+k}$.

2. ***Permutation groups***
Let X be a set. $S_X := \{f : X \mapsto X \mid f \text{ is a bijection}\}$. Multiplication is composition

$$\begin{aligned} S_X \times S_X &\mapsto S_X \\ (f, g) &\mapsto g \circ f. \end{aligned}$$

Notation: *In case $X = \{1, \dots, n\}$ for some $n \in \mathbb{N}$, write S_n for S_X (called a **symmetric group**). If $G \leq S_n$ for some n, G is a **permutation group** of degree n.*

3. ***Linear groups***
*A **field** $(\mathbb{F}, +, \cdot)$ consists of a set $\mathbb{F}$ together with binary operations $+$ and $\cdot$, such that:*

   (a) $(\mathbb{F}, +)$ *forms an abelian group,*

   (b) $(\mathbb{F} - \{0\}, \cdot)$ *forms an abelian group (where 0 is the identity for $(\mathbb{F}, +)$),*

   (c) $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in \mathbb{F}$ *(distributivity).*

   *Let $\mathbb{F}$ be a field. $GL_n(\mathbb{F}) := \{\text{invertible } n \times n \text{ matrices with entries from } \mathbb{F}\}$. The group operation is matrix multiplication. GL_n is called the **general linear group**.*
*If $G \leq GL_n(\mathbb{F})$ for some $\mathbb{F}$ and n then G is called a **linear group** of degree n.*

4. ***Symmetry groups*** *Let $X \subset \mathbb{R}^n$. The group of symmetries of X, denoted $Sym(X)$, is the subgroup of S_X containing only isometries (that is, functions $f : X \mapsto X$ such that $\|f(x) - f(y)\| = \|x - y\| \quad \forall x, y \in X$).*
Notation: *In case $N = 2$ and $X =$ the regular n-gon, $Sym(X)$ is called the n^{th} **dihedral group**, written D_{2n}.*

Proposition 1.1.6. *Let G be a group. Then $\exists$ exactly one element $e \in G$ such that $e * g = g$ and $g * e = g \quad \forall g \in G$.*

Proof. By definition, such an element exists. If $e, e' \in G$ both have the property then

$$e = e * e' = e'.$$

$\square$

Proposition 1.1.7. *Let G be a group and let $g \in G$. Then $\exists$ exactly one element $h \in G$ such that $g * h = e$ and $h * g = e$.*

Proof. By definition, such an element exists. Suppose h, h' are both inverses to g. Then

$$h' = h' * e = h' * (g * h) = (h' * g) * h = e * h = h.$$

$\square$

Notation: The inverse to g will be denoted g^{-1}.

Proposition 1.1.8. *Let G be a group and let $x, y, z \in G$.*

1. *If $xz = yz$ then $x = y$.*
2. *If $zx = zy$ then $x = y$.*

Proof.

1. $x = xe = x(zz^{-1}) = (xz)z^{-1} = (yz)z^{-1} = y(zz^{-1}) = ye = y$.
2. Likewise.

$\square$

Note: $xz = zy \not\Rightarrow x = y$; "mixed" cancellation doesn't work.

Corollary 1.1.9. *Let G be a group and let $g, h \in G$ such that $g * h = e$. Then $h = g^{-1}$ (and $g = h^{-1}$).*

Proof. $g * h = e$ is given; $g * g^{-1} = e$ by the definition of g^{-1}. So by cancellation, $h = g^{-1}$. $\square$

Proposition 1.1.10. *In a group G, $(gh)^{-1} = h^{-1}g^{-1}$.*

Proof.

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e.$$

$\therefore h^{-1}g^{-1}$ is the inverse of gh. $\square$

Proposition 1.1.11. *Let G be a group and $g, h \in G$. Then*

1. $\exists!$ *solution* x *in* G *to the equation* $gx = h$.

2. $\exists!$ *solution* x *in* G *to the equation* $xg = h$.

Proof.

1. $x = g^{-1}h$.

2. $x = hg^{-1}$.

□

Proposition 1.1.12. *A non-empty subset* H *of a group* G *is a subgroup iff* $x, y \in H$ *implies* xy^{-1} *lies in* H.

Proof. Exercise. □

G is called a **finite** group if its underlying set is finite. In this case, the number of elements in G is called the **order** of G, written $|G|$.

Definition 1.1.13. *Let* $x \in G$. *The **order** of* x, *written* $|x|$, *is the least integer* k *(if any) such that* $x^k = e$.

Note: some, or even all elements of a group might have finite order even if $|G|$ is infinite.

Definition 1.1.14. *Let* $(G, *)$ *and* $(H, \triangle)$ *be groups. A function* $f : G \mapsto H$ *is called a (group)* ***homomorphism*** *if* $f(x * y) = f(x) \triangle f(y) \quad \forall x, y \in G$. *A homomorphism* $f : G \mapsto H$ *which is a bijection is called an* ***isomorphism***.

Notation: $\phi : G \overset{\cong}{\longmapsto} H$ means that ϕ is an isomorphism from G to H.
$G \cong H$ means that there exists an isomorphism $\phi : G \overset{\cong}{\longmapsto} H$.

Isomorphisms preserve all group properties. e.g. if $\phi : G \overset{\cong}{\longmapsto} H$ then:

$$\begin{gathered} G \text{ is abelian } \iff H \text{ is abelian,} \\ |x| = |\phi(x)| \quad \forall x \in G, \text{ etc.} \end{gathered}$$

Lemma 1.1.15. *Let* $\phi : G \mapsto H$ *be a homomorphism, and let* e, e' *be the identities in* G, H *respectively. Then* $\phi(e) = e'$.

Proof. Let $h = \phi(e)$.

$$h^2 = \phi(e)\phi(e) = \phi(e^2) = \phi(e) = h = he'$$

$\therefore$ by cancellation, $h = e'$. □

Corollary 1.1.16. *Let* $\phi : G \mapsto H$ *be a homomorphism. Then* $\forall g \in G, \phi(g^{-1}) = \phi(g)^{-1}$.

Proof.
$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e'.$$
Thus, $\phi(g)^{-1} = \phi(g^{-1})$. □

Proposition 1.1.17. *Let $\phi : G \mapsto H$ be a group isomorphism. Let $\phi^{-1} : H \mapsto G$ be the inverse function to the bijection ϕ. Then ϕ^{-1} is an isomorphism.*

Proof. Must show ϕ^{-1} is a homomorphism. Let $h_1, h_2 \in H$. Since ϕ is a bijection, $\exists! g_1, g_2 \in G$ such that $\phi(g_1) = h_1, \phi(g_2) = h_2$.
$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = h_1 h_2$$
So $\phi^{-1}(h_1 h_2) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$. □

Proposition 1.1.18. *The composition of group homomorphisms is a homomorphism.*
The composition of group isomorphisms is a isomorphism.

Proof. Trivial. □

Notation: $Aut(G) = \{\text{self-isomorphisms of } G\} \leq S_G$.

Fundamental Problem of Group Theory:
Make a list of all possible types of groups. ie. Make a list of groups such that every group is isomorphic to exactly one group on the list.

Given two groups (defined, for example, by multiplication tables, or by generators and relations), the problem of determining whether or not the groups are isomorphic is, in general, very difficult (NP-hard).

1.2 New Groups from Old

1.2.1 Quotient Groups

Definition 1.2.1. *Let $\phi : G \mapsto H$ be a homomorphism. The **kernel** of ϕ is*

$$\ker\phi := \{g \in G \mid \phi(g) = e\}.$$

*The **image** of ϕ is*

$$\mathrm{Im}\phi := \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}.$$

Proposition 1.2.2. $\ker\phi \leq G$ *and* $\mathrm{Im}\phi \leq G$.

Proof. Trivial. □

Definition 1.2.3. *For $x, y \in G$, we say y is **conjugate** to x (in G) if $\exists g \in G$ such that $y = gxg^{-1}$.*

Proposition 1.2.4. *Conjugacy is an equivalence relation.*

Proof. Trivial. □

Notation: If A, B are subsets of G, let $AB := \{ab \mid a \in A, b \in B\}$. For $g \in G, H \leq G$, the set gH is called the **left coset** of H generated by g; Hg is the **right coset** of H generated by g.

Definition 1.2.5. *A subgroup N of G is called **normal**, written $N \lhd G$, if $gN = Ng$ for all $g \in G$.*

Proposition 1.2.6. *$N \leq G$ is normal $\iff gxg^{-1} \in N \quad \forall x \in N, g \in G$.*

Proof.

$\Rightarrow$: Suppose N is normal. Then for all $x \in N, g \in G$, $gx \in gN = Ng$, so $gx = yg$ for some $y \in N$. Thus, $gxg^{-1} = y \in N$.

$\Leftarrow$: Suppose $gxg^{-1} \in N \quad \forall x \in N, g \in G$. If $z \in gN$ then $z = gx$ for some $x \in N$. Hence,

$$z = gx(g^{-1}g) = (gxg^{-1})g \in Ng$$

$\therefore gN \subset Ng$. Similarly, $Ng \subset gN$.

□

Corollary 1.2.7. *Let $\phi : G \mapsto H$ be a homomorphism. Then $\ker\phi \lhd G$.*

Proof. Let $x \in \ker \phi$ and let $g \in G$. Then

$$\phi(gxg^{-1}) = \phi(g)e\phi(g)^{-1} = e$$

so $gxg^{-1} \in \ker \phi$. □

Conversely:

Theorem 1.2.8. *Suppose $N \lhd G$. Then $\exists$ a group H and a homomorphism $\phi : G \mapsto H$ such that $N = \ker \phi$.*

Proof. Exercise: check the details of the following:

1. For $g, g' \in G$, define $g \sim g'$ if $g'g^{-1} \in N$.
2. Check that $\sim$ is an equivalence relation.
3. Define $H := G/N :=$ {set of equivalence classes of G under $\sim$}.
4. Define binary operation $*$ on G/N by $\overline{x} * \overline{y} = \overline{xy}$. Check that this is well-defined, ie. suppose $x' \sim x$ and $y' \sim y$. Is $x'y' \sim xy$?
   Well, $x' \sim x$ means $x'x^{-1} = n_1 \in N$, so $x' = n_1 x$. Likewise, $y' \sim y$ means $y'y^{-1} = n_2 \in N$, so $y' = n_2 y$. So
   $$x'y' = n_1 x n_2 y = n_1(x n_2 x^{-1})xy = n_1 n_2' xy,$$
   where $n_2' = x n_2 x^{-1} \in N$ since N is normal. Hence, $x'y' \sim xy$.
5. Check that $(G/N, *)$ forms a group.
6. Define $\phi : G \mapsto H$ by $\phi(x) = \overline{x}$.
7. Check that ϕ is a group homomorphism.
8. Check that $N = \ker \phi$.

□

G/N (as constructed above) is called a **quotient group**.

1.2.2 Product Groups

Let G, H be groups. The **product group** is the set $G \times H$, with multiplication

$$(g, h) \cdot (g', h') := (gg', hh').$$

Clearly the projection maps

$$\begin{aligned} \Pi_G : G \times H &\mapsto G \\ (g, h) &\mapsto g \end{aligned}$$

and

$$\begin{aligned} \Pi_H : G \times H &\mapsto H \\ (g, h) &\mapsto h \end{aligned}$$

are group homomorphisms.

Proposition 1.2.9. *Let A, G, H be groups.*

1. *Universal Property of Product:*
   Given group homomorphisms $p : A \mapsto G$ and $q : A \mapsto H$, $\exists!$ group homomorphism $\phi : A \mapsto G \times H$ such that:

$$\begin{tikzcd} & A \arrow[ddl, "p"'] \arrow[d, dashed, "\exists!\phi"] \arrow[ddr, "q"] & \\ & G \times H \arrow[dl, "\Pi_G"] \arrow[dr, "\Pi_H"'] & \\ G & & H \end{tikzcd}$$

   This says that $G \times H$ is the product of G and H in the category of groups.

2. *Given a function $\phi : A \mapsto G \times H$, ϕ is a group homomorphism if and only if $\Pi_G \circ \phi$ and $\Pi_H \circ \phi$ are group homomorphisms.*

1.2.3 Free Products

Let G, H be groups. The free product of G and H is $G * H := \{\text{words in } G \amalg H\}/\sim$, where $\sim$ is the equivalence relation generated by the following: for $g, g' \in G$,

$$x_1 \cdots x_n g g' y_1 \cdots y_m \sim x_1 \cdots x_n (gg') y_1 \cdots y_m,$$

and for $h, h' \in H$,

$$x_1 \cdots x_n h h' y_1 \cdots y_m \sim x_1 \cdots x_n (hh') y_1 \cdots y_m.$$

Note: Given $A \subset X \times X$, the equivalence relation generated by A is

$$\bigcap \{B \subset X \times X \mid B \text{ is an equivalence relation and } A \subset B\}.$$

Multiplication in $G * H$ is given by juxtaposition: $(v_1 \cdots v_n) * (w_1 \cdots w_m) = v_1 \cdots v_n w_1 \cdots w_m$.

Proposition 1.2.10. *Universal Property of Free Product:*

$$\begin{tikzcd}
G \arrow[dr, "g \mapsto g"] \arrow[ddr, "p"'] & & H \arrow[dl, "h \mapsto h"'] \arrow[ddl, "q"] \\
& G * H \arrow[d, dashed, "\exists! \phi"] & \\
& A &
\end{tikzcd}$$

(Here, G and H each embed into the words of length 1 *in* $G \times H$*).*
This says that $G * H$ *is the coproduct of G and H in the category of groups.*

$F(x) = \{x^n \mid n \in \mathbb{Z}\} (= C_\infty)$ is called the free group on the generator x.
$F(x, y) := F(x) * F(y)$ is the free group on 2 generators.
More generally, given a set S,

$$F(S) = \{\text{words in } S\}$$

is called the **free group on** S. A group homomorphism $F(S) \mapsto G$ is uniquely determined by any (set) function $S \mapsto G$.

1.3 Centralizers, Normalizers, and Commutators

Let G be a group, $X \subset G$.
Notation:

$$\begin{aligned} \mathrm{C}_G(X) &:= \{g \in G \mid gxg^{-1} = x \quad \forall x \in X\} \quad \text{is the } \textbf{centralizer} \text{ of } X \text{ in } G \\ \mathrm{N}_G(X) &:= \{g \in G \mid gXg^{-1} = X\} \quad \text{is the } \textbf{normalizer} \text{ of } X \text{ in } G \\ &= \{g \in G \mid gX = Xg\} \end{aligned}$$

These definitions do not require that X be a subgroup, but note that $\mathrm{C}_G(X) = \mathrm{C}_G(\langle X \rangle)$. Also,

$$\begin{aligned} \mathrm{Z}(G) &:= \mathrm{C}_G(G) \quad \text{is the } \textbf{center} \text{ of } G \\ &= \{g \in G \mid gx = xg \quad \forall x \in G\} \end{aligned}$$

Note: $\mathrm{Z}(G) = G \iff G$ is abelian.

Example 1.3.1. *Let $G = GL_n(\mathbb{F})$. Then $\mathrm{Z}(G) = \{cI \mid c \in \mathbb{F}^\times\}$.*

Proposition 1.3.2. *$\mathrm{C}_G(X)$ and $\mathrm{N}_G(X)$ are subgroups of G.*

Proof.

$$\begin{aligned} g, g' \in \mathrm{C}_G(X) &\Rightarrow (gg')(x)(gg')^{-1} = g(g'xg'^{-1})g^{-1} = gxg^{-1} = x \quad \forall x \in X \\ g \in \mathrm{C}_G(X) &\Rightarrow g^{-1}xg = g^{-1}(gxg^{-1})g = (g^{-1}g)x(g^{-1}g) = x \quad \forall x \in X \end{aligned}$$

Likewise,

$$\begin{aligned} g, g' \in \mathrm{N}_G(X) &\Rightarrow (gg')X(gg')^{-1} = g(g'Xg'^{-1})g^{-1} = gXg^{-1} = X \\ g \in \mathrm{N}_G(X) &\Rightarrow g^{-1}Xg = g^{-1}(gXg^{-1})g = (g^{-1}g)X(g^{-1}g) = X \end{aligned}$$

□

Clearly, $\mathrm{Z}(G) = \mathrm{C}_G(G)$ is always abelian, but for arbitrary H, $\mathrm{C}_G(H)$ need not be abelian. For example, in the extreme case, $\mathrm{C}_G(\{e\}) = G$, which might not be abelian.

For $H \leq G$, by construction, $H \lhd \mathrm{N}_G(H)$, and $H \lhd G \iff \mathrm{N}_G(H) = G$.

Proposition 1.3.3. *For $A \leq B \leq G$,*

$$g \in \mathrm{N}_G(\mathrm{N}_B(A)) \Rightarrow g(\mathrm{N}_B(A))g^{-1} \subset \mathrm{N}_G(A).$$

Proof. If $b \in N_B(A)$ and $g \in N_G(N_B(A))$ then $b' = gbg^{-1} \in N_B(A)$, so

$$(gbg^{-1})a(gbg^{-1})^{-1} = b'a(b')^{-1} \in A$$

$\square$

Note: $K \lhd H$ and $H \lhd G \not\Rightarrow K \lhd G$. For a counterexample, take

$$\begin{aligned} &G = S_4 \\ &H = \langle (1\ 2\ 3\ 4), (1\ 3)(2\ 4) \rangle \cong D_8 \\ &K = \langle (1\ 2\ 3\ 4) \rangle \cong C_4 \end{aligned}$$

Notation: For $a, b \in G$, let $[a, b] := aba^{-1}b^{-1}$.

Definition 1.3.4. *The **commutator subgroup** G' is the subgroup of G generated by*

$$\{[a, b] \mid a, b \in G\}.$$

Proposition 1.3.5. $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$.

Corollary 1.3.6. $G' \lhd G$.

$G_{ab} := G/G'$ is abelian. Universal property: given any homomorphism $\phi : G \mapsto H$ with H abelian,

$$\begin{tikzcd} G \arrow[r, two heads] \arrow[dr, "\phi"'] & G_{ab} \arrow[d, dashed, "\exists!"] \\ & H \end{tikzcd}$$

That is, if $\phi : G \mapsto H$ with H abelian then $G' \subset \ker \phi$.

1.4 Isomorphism Theorems

Theorem 1.4.1 (First Isomorphism Theorem)**.** *Let $\phi : G \mapsto H$ be a group homomorphism. Then $G/\ker\phi \cong \mathrm{Im}\phi$.*

Proof. Set $N := \ker\phi$. Elements of G/N are cosets Ng, where $g \in G$. Define $\psi : G/N \mapsto \mathrm{Im}\phi$ by $\psi(Ng) = \phi(g)$.

1. ψ is well defined:
   Suppose $Ng = Ng'$. Then $g = ng'$ for some $n \in N$. Hence,

   $$\phi(g) = \phi(ng') = \phi(n)\phi(g') = e_H\phi(g') = \phi(g'),$$

   since $n \in N = \ker\phi$.

2. ψ is a homomorphism – easy.

3. ψ is surjective – easy.

4. ψ is injective:
   If $\psi(Ng_1) = \psi(Ng_2)$ then

   $$\phi(g_1) = \phi(g_2) \Rightarrow \ \phi(g_1g_2^{-1}) = e_H \Rightarrow \ g_1g_2^{-1} \in N \Rightarrow \ Ng_1 = Ng_2$$

□

Proposition 1.4.2. *If H, K subgroups of G then $HK \leq G \iff HK = KH$.*

Proof.

⇒: Suppose $HK \leq G$. Let $x \in HK$. Then $x^{-1} \in HK$. Write $x^{-1} = hk$ for some $h \in H, k \in K$. Then

$$x = (hk)^{-1} = k^{-1}h^{-1} \in KH,$$

so $HK \subset KH$, and similarly, $KH \subset HK$.

⇐: Suppose $HK = KH$. Let $x, x' \in HK$. Write $x = kh, x' = h'k'$, for some $h, h' \in H, k, k' \in K$. Then

$$\begin{aligned} x'x^{-1} &= h'k'h^{-1}k^{-1} \\ &= h'h''k''k^{-1}, \quad \text{letting } k'h^{-1} = h''k'', \text{ since } HK = KH \\ &\in HK \end{aligned}$$

□

Corollary 1.4.3. *Let H, K be subgroups of G. If $H \subset \mathrm{N}_G(K)$ then $HK \leq G$ and $K \lhd HK$.*

Proof. Let $x = hk \in HK$. Then $x = (hkh^{-1})h \in KH$, since $hkh^{-1} \in K$. So, $HK \subset KH$. Similarly, if $x = kh \in HK$ then $x = h(h^{-1}kh) \in HK$, whence $KH \subset HK$. Hence

$$HK = KH \leq G.$$

Also, $K \subset \mathrm{N}_G(K)$ (always) and $H \subset \mathrm{N}_G(K)$ (given), so

$$HK \subset \mathrm{N}_G(K) \Rightarrow K \lhd HK.$$

□

Corollary 1.4.4. *If $K \lhd G$ then $HK \leq G$ for any $H \leq G$.*

Proof. If $K \lhd G$ then $\mathrm{N}_G(K) = G$, so automatically, $H \subset \mathrm{N}_G(K)$. □

Theorem 1.4.5 (Second Isomorphism Theorem)**.** *Let H, K be subgroups of G such that*

$$H \subset \mathrm{N}_G(K).$$

Then $H \cap K \lhd H$, $K \lhd HK$, and

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

Proof. $K \lhd HK$ was shown above. Define $\phi : H \mapsto HK/K$ by $\phi(h) = Kh \in HK/K$. ie. ϕ is the composition

$$H \hookrightarrow HK \twoheadrightarrow HK/K$$

1. ϕ is a homomorphism (composition of homomorphisms).

2. ϕ is surjective

   Proof. Let $Kx \in HK/K$, where $x \in HK$. By above, $HK \leq G$, so $HK = KH$; thus let $x = kh$, for some $k \in K, h \in H$. Hence,

   $$Kx = Kkh = Kh = \phi(h)$$

3. $\ker \phi = H \cap K$

   Proof.

   $$\begin{aligned}\ker \phi &= \{y \in H \mid \phi(y) = e\} \\ &= \{y \in H \mid Ky = e\} \\ &= \{y \in H \mid y \in K\} \\ &= H \cap K\end{aligned}$$

$H \cap K \lhd H$ and

$$\frac{H}{H \cap K} = \frac{H}{\ker \phi} \cong \mathrm{Im}\phi = \frac{HK}{K}.$$

□

Theorem 1.4.6 (Third Isomorphism Theorem)**.** *Let $K \lhd G$ and $H \lhd G$ with $K \subset H$. Then $H/K \lhd G/K$ and*

$$\frac{G/K}{H/K} \cong G/H.$$

Proof. Define ϕ by composition

$$G \mapsto\!\!\!\!\rightarrow G/K \mapsto\!\!\!\!\rightarrow \frac{G/K}{H/K}.$$

Check that $\ker \phi = H$ (exercise). □

1.5 The Pullback

Definition 1.5.1. *Let $\phi : G \mapsto H$ and $j : B \mapsto H$ be group homomorphisms. Define the **pullback** $G \times_H B$ of ϕ and j by*

$$G \times_H B := \{(g, b) \in G \times B \mid \phi(g) = j(b)\}.$$

The pullback gives:

$$\begin{tikzcd} G \times_H B \arrow[r, "\Pi_G"] \arrow[d, "\Pi_B"'] & G \arrow[d, "\phi"] \\ B \arrow[r, "j"'] & H \end{tikzcd}$$

Proposition 1.5.2. *$G \times_H B \leq G \times B$.*

Proof. If (g, b) and (g', b') belong to $G \times_H B$ then

$$\phi(gg') = \phi(g)\phi(g') = j(b)j(b') = j(bb').$$

If $(g, b) \in G \times_H B$ then

$$\phi(g^{-1}) = \phi(g)^{-1} = j(b)^{-1} = j(b^{-1}).$$

□

Proposition 1.5.3. *Let $\phi : G \mapsto H$, $j : B \mapsto H$ and $i : A \mapsto B$ be homomorphisms. Then*

$$\begin{tikzcd}
A \times_B (B \times_H G) \arrow[r, "\Pi_{B\times_H G}"] \arrow[d, "\Pi_A"'] \arrow[dr, phantom, "p.b."] & B \times_H G \arrow[r, "\Pi_G"] \arrow[d, "\Pi_B"] \arrow[dr, phantom, "p.b."] & G \arrow[d, "\phi"] \\
A \arrow[r, "i"'] & B \arrow[r, "j"'] & H
\end{tikzcd}$$

and $A \times_B (B \times_H G) \cong A \times_H G$. (Composition of pullbacks is a pullback).

Proof.

$$A \times_B (B \times_H G) = \{(a, (b, g)) \mid a \in A, (b, g) \in B \times_H G, i(a) = \Pi_B(b, g) = b\}$$

In this description, b is redundant because it is determined by a via $b = i(a)$. Also, $(b, g) \in B \times_H G$ means that $j(b) = \phi(g)$. So,

$$A \times_B (B \times_H G) \cong \{(a, g) \mid j(i(a)) = \phi(g)\} = A \times_H G.$$

□

Note some special cases:

1. If $H = \{e\}$ then $j(b) = \phi(g)$ holds $\forall b, g$, so $B \times_{\{e\}} G = B \times G$.
2. If $B \leq H$ and j is the inclusion, then

$$\begin{aligned} B \times_H G &= \{(b, g) \mid j(b) = \phi(g)\}, \quad \text{so } b \text{ is redundant} \\ &\cong \{g \in G \mid \phi(g) \in B\} \\ &= \phi^{-1}(B) \end{aligned}$$

Proposition 1.5.4. *Let*

$$\begin{tikzcd}
B \times_H G \arrow[r, "\Pi_G"] \arrow[d, "\Pi_B"'] & G \arrow[d, "\phi"] \\
B \arrow[r, "j"] & H
\end{tikzcd}$$

be a pullback. Then $\ker \Pi_B \cong \ker \phi$ *and* $\ker \Pi_G \cong \ker j$.

Proof.

$$\begin{aligned}\ker \Pi_B &= \{(b,g) \in B \times G \mid b = e \text{ and } \phi(g) = j(b)\} \\ &= \{(e,g) \in B \times G \mid \phi(g) = j(e) = e\} \\ &= \{e\} \times \ker \phi \subset B \times G \\ &\cong \ker \phi\end{aligned}$$

□

Now consider the special case where $B \leq H$ and j is inclusion. Set $A = B \times_H G = \phi^{-1}(B)$.

Proposition 1.5.5.

1. *If $B \lhd H$ then $A \lhd G$.*

2. *If $B \lhd H$ and ϕ is onto then $G/A \cong H/B$.*

Proof.

1. Suppose $B \lhd H$. Let $a \in A$. Then for $g \in G$,

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in B, \quad \text{since } \phi(a) \in B \lhd H,$$

so $gag^{-1} \in A$.

2. Let ψ be the composition

$$G \overset{\phi}{\longmapsto\!\!\!\!\rightarrow} H \overset{q}{\longmapsto\!\!\!\!\rightarrow} H/B,$$

where q is the quotient map. Then $\phi(A) \subset B = \ker q$ so $A \subset \ker \psi$. If $g \in \ker \psi$ then $\phi(g) \in \ker q = B$, so $g \in \phi^{-1}(B) = A$. Thus, $\ker \psi = A$. Hence,

$$\frac{G}{A} = \frac{G}{\ker \psi} \cong \mathrm{Im}\psi = \frac{H}{B}$$

since both ϕ and q are onto.

□

Theorem 1.5.6 (Fourth Isomorphism Theorem)**.** *Suppose $N \lhd G$. Then the quotient map $q : G \twoheadrightarrow G/N$ induces a bijection between the subgroups of G which contain N and the subgroups of G/N. Explicitly,*

$$\begin{gathered} A \leq G \mapsto q(A) \leq G/N, \quad \textit{and} \\ X \leq G/N \mapsto q^{-1}(X) \leq G \end{gathered}$$

Moreover, this bijection satisfies

1. *$A \leq B$ iff $q(A) \leq q(B)$, and in this case $B : A = q(B) : q(A)$.*
2. *$q(A \cap B) = q(A) \cap q(B)$.*
3. *$A \lhd B$ iff $q(A) \lhd q(B)$.*

Proof. Exercise. $\square$

1.6 Symmetric Groups

$$|S_n| = n!$$

Notation for elements of S_n: Consider $\sigma \in S_6$ given by:

$$\begin{aligned}
\sigma(1) &= 2\\
\sigma(2) &= 4\\
\sigma(3) &= 5\\
\sigma(4) &= 6\\
\sigma(5) &= 3\\
\sigma(6) &= 1
\end{aligned}$$

Mapping Notation:

$$\sigma = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{matrix}$$

Cycle Notation:

$$\sigma = (1\ 2\ 4\ 6)(3\ 5)$$

Usually omit cycles of length one. eg. $\tau = (1\ 4\ 3)$ means $(1\ 4\ 3)(2)(5)(6)$.

The group operation on S_n is $*$ given by

$$\sigma * \tau = \tau \circ \sigma$$

Note: Dummit and Foote use the opposite convention: $\sigma \vartriangle \tau = \sigma \circ \tau$. However, the results are isomorphic; $(S_n, *) \cong (S_n, \vartriangle)$.

Notation: $S_X :=$ permutations of X with $f * g = g \circ f$.

$S'_X :=$ permutations of X with $f * g = f \circ g$.

$$\begin{aligned}
\sigma\tau &= ((1\ 2\ 4\ 6)(3\ 5))(1\ 4\ 3) = (1\ 2\ 3\ 5)(4\ 6)\\
\tau\sigma &= (1\ 4\ 3)((1\ 2\ 4\ 6)(3\ 5)) = (1\ 6)(2\ 4\ 5\ 6)
\end{aligned}$$

So S_n is not abelian.

Note: There is an ambiguity in the cycle notation: $(1\ 2\ 4\ 6)(3\ 5)$ could mean either σ or $(1\ 2\ 4\ 6) * (3\ 5)$. This is not important because these are equal.

1.6.1 Conjugation in S_n

Example 1.6.1. *Let $\sigma = (1\ 2\ 3)(4\ 5), \tau = (2\ 5)$. Then*

$$\tau\sigma\tau^{-1} = (2\ 5)(1\ 2\ 3)(4\ 5)(2\ 5) = (1\ 5\ 3)(4\ 2).$$

This is obtained from σ by switching 2 and 5 (in the cycle notation).

Proposition 1.6.2. *Let $\sigma, \tau \in S_n$, with*

$$\sigma = (a_1^{(1)}\ \cdots\ a_1^{(r_1)})\cdots(a_n^{(1)}\ \cdots\ a_n^{(r_n)}).$$

Then

$$\tau\sigma\tau^{-1} = (\tau^{-1}(a_1^{(1)})\ \cdots\ \tau^{-1}(a_1^{(r_1)}))\cdots(\tau^{-1}(a_n^{(1)})\ \cdots\ \tau^{-1}(a_n^{(r_n)})).$$

Proof. In general, $(\tau\sigma\tau^{-1})(j) = \tau^{-1}(\sigma(\tau(j)))$. So

$$(\tau\sigma\tau^{-1})(\tau^{-1}a_1^{(1)}) = \tau^{-1}(\sigma(\tau(\tau^{-1}a_1^{(1)}))) = \tau^{-1}(\sigma(a_1^{(1)})) = \tau^{-1}a_1^{(2)}$$

etc. $\square$

Notice that $\tau\sigma\tau^{-1}$ has the same cycle type as σ.

Corollary 1.6.3. *σ is conjugate to σ' $\iff$ σ and σ' have the same cycle type.*

Proof. Above shows that any conjugate of σ has the same cycle type as σ. Conversely, suppose that σ, σ' have the same cycle type. Let

$$\sigma = (a_1^{(1)}\ \cdots\ a_1^{(r_1)})\cdots(a_n^{(1)}\ \cdots\ a_n^{(r_n)})$$
$$\sigma' = (a_1^{(1)\prime}\ \cdots\ a_1^{(r_1)\prime})\cdots(a_n^{(1)\prime}\ \cdots\ a_n^{(r_n)\prime})$$

Choose $\tau \in S_n$ such that $\tau^{-1}(a_i^{(j)}) = a_i^{(j)\prime}$. Then $\sigma' = \tau\sigma\tau^{-1}$. $\square$

1.6.2 The Alternating Group

Define the polynomial Δ by

$$\Delta(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$$

For $\sigma \in S_n$, let

$$\sigma(\Delta)(x_1, \ldots, x_n) = \Delta(x_\sigma(1), \ldots, x_\sigma(n)).$$

Here, all the same factors appear, but with some signs reversed.
$\therefore \sigma\Delta = \pm\Delta$.

Define $\epsilon : S_n \mapsto \{1, -1\}$ by

$$\epsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma\Delta = \Delta \\ -1 & \text{if } \sigma\Delta = -\Delta \end{cases}.$$

$\{1, -1\}$ is a group under multiplication ($\cong C_2$), and ϵ is a group homomorphism.
Set $A_n := \ker\epsilon \lhd S_n$. This is the **alternating group**.

Proposition 1.6.4. *Let $\gamma = (p\ q) \in S_n$ be a transposition (ie. 2-cycle). Then $\gamma \notin A_n$ (ie. $\gamma\Delta = -\Delta$).*

Proof. Say $p < q$.

$$\begin{aligned}\Delta &= \prod_{i<j}(x_i - x_j) \\ &= (x_p - x_q)\Big(\prod_{i<p}(x_i - x_p)\Big)\Big(\prod_{i>p}(x_p - x_i)\Big)\Big(\prod_{i<q}(x_i - x_q)\Big)\Big(\prod_{i>q}(x_q - x_i)\Big)\Big(\prod_{\substack{i<j \\ i \neq p,q \\ j \neq p,q}}(x_i - x_j)\Big)\end{aligned}$$

By applying γ to Δ:

- $(x_p - x_q)$ becomes $(x_q - x_p) = -(x_p - x_q)$,
- The factors $(\prod_{i<p}(x_i - x_p))$ and $(\prod_{i<q}(x_i - x_q))$ switch,
- The factors $(\prod_{i>p}(x_p - x_i))$ and $(\prod_{i>q}(x_q - x_i))$ switch, and
- The factor

  $$\Big(\prod_{\substack{i<j \\ i \neq p,q \\ j \neq p,q}}(x_i - x_j)\Big)$$

  is unchanged.

Thus, $\gamma\Delta = -\Delta$. ◻

Any permutation can be written (in many ways) as a product of transpositions.

Corollary 1.6.5. *$\sigma \in A_n \iff \sigma$ is the product of an even number of transpositions.*

1.7 Group Actions

Theorem 1.7.1 (Lagrange's Theorem)**.** *Let G be finite, $H \leq G$. Then $|H|$ divides $|G|$, and*

$$G : H := \frac{|G|}{|H|} = \#\text{ of left cosets of } H \text{ in } G = \#\text{ of right cosets of } H \text{ in } G.$$

*($G : H$ is called the **index** of H in G).*

Proof. Define the equivalence relation $\sim$ by $g \sim g' \iff gH = g'H$. For $g \in G$, $|H| = |gH|$ (because the map $x \mapsto gx$ is a bijection). Hence, $\sim$ partitions G into equivalence classes (cosets of H), each containing $|H|$ elements. ie.

$$\begin{aligned} |G| &= (\text{number of equiv. classes}) \times (\text{number of elts. per equiv. class}) \\ &= (\text{number of left cosets}) \times |H| \end{aligned}$$

Similarly, $|G| = (\text{number of right cosets}) \times |H|$. □

Corollary 1.7.2. *If $H \lhd G$ then $|G/H| = |G|/|H|$.*

Corollary 1.7.3. *For $x \in G$, $|x|$ divides $|G|$.*

Proof. Set $H = \langle x \rangle$. Then $|x| = |H| \,\Big|\, |G|$. □

Corollary 1.7.4. *If $|G| = p$, a prime number, then $G \cong C_p$.*

Proof. Let $x \in G$, $x \neq e$. Then $|x| = p$, so $G = \langle x \rangle \cong C_p(x)$. □

Definition 1.7.5. *A **left action** of a group G on a set X consists of an operation*

$$\begin{aligned} G \times X &\mapsto X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

such that:

1. $(gh) \cdot x = g \cdot (h \cdot x) \quad \forall g, h \in G, x \in X$, *and*
2. $e.x = x \quad \forall x \in X$.

Equivalently, an action of G on X is a group homomorphism $G \mapsto S'_X$.

Example 1.7.6.

1. *$\mathbb{F}$ a field, $G = GL_n(\mathbb{F}), X = \mathbb{F}^n$.*
   G acts on X by matrix multiplication, $A \cdot x = Ax$.

2. *G any group, $X = G$.*
   G acts by left multiplication on X, ie. $g \cdot x = gx$.

3. *G a group, $N \lhd G$.*
   G acts by conjugation on N, ie. $g \cdot x = gxg^{-1}$.

$$(gh) \cdot x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g(h \cdot x)g^{-1} = g \cdot (h \cdot x).$$

In this example, the image of $G \mapsto S'_X$ lies in $\mathrm{Aut}(N)$, ie.

$$g \cdot (xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = (g \cdot x)(g \cdot y).$$

Note special case where $N = G$.

Similarly, we may define a right action (it is a group homomorphism $G \mapsto S_X$). Given a right action $\odot$ of G on X, can define a left action of G on X by

$$g \cdot x := x \cdot g^{-1}.$$

Example 1.7.7. *$G = S_n, X = \{1, \ldots, n\}$. Then*

$$X \times G \mapsto X \text{ by } j \cdot \sigma = \sigma(j)$$

yields a right action of G on X, ie.

$$j \cdot (\sigma\tau) = (\sigma\tau)(j) = (\tau \circ \sigma)(j) = \tau(\sigma(j)) = (j \cdot \sigma) \cdot \tau.$$

$\therefore$ Define left action $G \times X \mapsto X$ by $\sigma \cdot j := j \cdot \sigma^{-1} = \sigma^{-1}(j)$.

Definition 1.7.8. *Let $G \times X \mapsto X$ be a (left) action of G on X. Let $x \in X$. The **orbit** of x is*

$$\mathrm{Orb}(x) := \{g \cdot x \mid g \in G\} \subset X.$$

*The **stabilizer** of x is*

$$\mathrm{Stab}(x) := \{g \in G \mid g \cdot x = x\} \subset G.$$

Proposition 1.7.9. $\mathrm{Stab}(x) \leq G$.

Proposition 1.7.10. $\mathrm{Orb}(x) = \mathrm{Orb}(y) \iff y \in \mathrm{Orb}(x)$.

Proof.

$\Rightarrow$ Suppose $\mathrm{Orb}(x) = \mathrm{Orb}(y)$. Then

$$y = e \cdot y \in \mathrm{Orb}(y) = \mathrm{Orb}(x).$$

$\Leftarrow$ Suppose $y \in \text{Orb}(x)$. Write $y = g \cdot x$, for some $g \in G$.
$\therefore g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = g^{-1}g \cdot x = e \cdot x = x$ and thus $x \in \text{Orb}(y)$.

If $z \in \text{Orb}(y)$ then $z = g' \cdot y = g' \cdot (g \cdot x) = (gg') \cdot x$ so $z \in \text{Orb}(x)$. Hence $\text{Orb}(x) \subset \text{Orb}(y)$, and similarly, $\text{Orb}(y) \subset \text{Orb}(x)$.

□

Corollary 1.7.11. *Given an action of G on X, the relation $x \sim y \iff \text{Orb}(x) = \text{Orb}(y)$ is an equivalence relation.*

Theorem 1.7.12. *Let G be a finite group. Let $G \times X \mapsto X$ be an action of G on X. Then for $x \in X$,*

$$|\text{Orb}(x)|\,|\text{Stab}(x)| = |G|.$$

Note: Lagrange's Theorem is a special case. ie. $H \leq G$, $X = \{\text{left cosets of } H\}$.

$$G \times X \mapsto X \text{ by } g \cdot C = gC$$

defines a left action. Set $x = H$.

Proof.

$$\frac{|G|}{|\text{Stab}(X)|} = G : \text{Stab}(X) = \#\text{ of left cosets of Stab}(X) \text{ in } G$$

Define

$$\theta : \{\text{left cosets of Stab}(X) = H\} \mapsto \text{Orb}(x)$$
$$gH \mapsto g \cdot x$$

1. θ is well-defined:
   Suppose $gH = g'H$. Then $g = g'h$ for some $h \in H$. Hence,
   $$g \cdot x = (g'h) \cdot x = g' \cdot (h \cdot x) = g' \cdot x, \quad \text{since } h \in \text{Stab}(x).$$

2. θ is surjective:
   If $y \in \text{Orb}(x)$ then $y = g \cdot x$, for some $g \in G$. Thus $y = \theta(gH)$.

3. θ is injective:
   Suppose $\theta(gH) = \theta(g'H)$. Then $g \cdot x = g' \cdot x$. Hence,
   $$x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x) = (g^{-1}g') \cdot x.$$
   $\therefore g^{-1}g' \in H$, ie. $g' = gh$ for some $h \in H$. Thus $g'H = gH$.

$\therefore \theta$ is a bijection and the theorem follows. $\square$

Corollary 1.7.13. *Let G be a finite group acting on a finite set X. Then*

$$|X| = \sum \frac{|G|}{|\mathrm{Stab}(x)|},$$

where the sum is taken over one element from each orbit.

Proof. The equivalence relation $x \sim y \iff \mathrm{Orb}(x) = \mathrm{Orb}(y)$ partitions X into disjoint subsets. So

$$\begin{aligned} |X| &= \sum |\mathrm{Orb}(x)|, \quad \text{summed over one element from each orbit} \\ &= \sum \frac{|G|}{|\mathrm{Stab}(x)|} \end{aligned}$$

$\square$

Consider the action of G on itself by conjugation. ie. $X = G$ and $g \cdot x = gxg^{-1}$. Then

$$\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gxg^{-1} = x\} = \mathrm{C}_G(x).$$

Corollary 1.7.14. *Class Formula:*

$$|G| = \sum \frac{|G|}{|\mathrm{C}_G(x)|},$$

summed over one element from each conjugacy class.

Corollary 1.7.15. *Let p be prime and let G be a p-group (ie. $|G|$ is a power of p). Then $\mathrm{Z}(G) \neq \{e\}$.*

Proof. $\mathrm{C}_G(e) = G$. By the class formula,

$$\begin{aligned} |G| &= \sum_{\text{all conj. classes}} \frac{|G|}{|\mathrm{C}_G(x)|} \\ &= \frac{|G|}{|\mathrm{C}_G(e)|} + \sum_{\substack{\text{remaining conj.} \\ \text{classes}}} \frac{|G|}{|\mathrm{C}_G(x)|} \\ \therefore\ p^n &= 1 + \sum_{\substack{\text{remaining conj.} \\ \text{classes}}} \frac{|G|}{|\mathrm{C}_G(x)|} \end{aligned}$$

$\therefore \exists x \neq e$ such that $\frac{|G|}{|\mathrm{C}_G(x)|}$ is not divisible by p. Since $|G| = p^n$, this can happen only when $|\mathrm{C}_G(x)| = p^n$, ie. when $\mathrm{C}_G(X) = G$. ie. $\exists e \neq x \in G$ such that $\mathrm{C}_G(x) = G$, ie. $x \in \mathrm{Z}(G)$. $\square$

Corollary 1.7.16. *If $|G| = p^2$ where p is prime then G is abelian.*

Proof. Let $x \neq e$ such that $x \in Z(G)$. If $G = \langle x \rangle$ then G is abelian. Otherwise, $|x| = p$, and since $x \in Z(G)$, $\langle x \rangle \lhd G$. So, $\exists y \in G$ such that $\overline{y}$ generates $G/\langle x \rangle \cong C_p$. Then x and y generate G, and since $x \in Z(G)$, $x \leftrightarrow y$. Hence G is abelian. $\square$

1.8 Semi Direct Products

Let H, K be subgroups of G. Define $\mu : H \times K \mapsto G$ by $\mu(h, k) = hk$.

Proposition 1.8.1. *If $H \cap K = \{e\}$ then μ is injective.*

Proof. Suppose $hk = h'k'$. Then

$$(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\}$$

so $h'^{-1} = e = k'k^{-1}$. ie. $h = h'$ and $k = k'$. $\square$

Assuming (for the rest of this section) that $H \cap K = \{e\}$, the above says

$$\mu : H \times K \mapsto HK \subset G$$

is a bijection. We wish to compare $H \times K$ to HK (which, in general, may not be a subgroup of G). Suppose that $H \triangleleft G$. Then $HK = KH$ is a subgroup of G, but is not necessarily isomorphic to $H \times K$. Besides $H \times K$, what other possibilities are there for HK?

Suppose $g = hk$ and $g' = h'k'$ lie in HK. Then

$$gg' = hkh'k' = hkh'k^{-1}kk' = h''k''$$

where $h'' = h(kh'k^{-1}) \in H$ and $k'' = kk' \in K$.

ie., Labelling elements of HK by the corresponding element in $H \times K$, the group operation in HK can be written

$$(h, k)(h', k') = (hk \cdot h', kk')$$

where $k \cdot h' := kh'k^{-1}$ (the restriction to K of the conjugation action of G on the normal subgroup H). Recall that this action satisfies $k \cdot (h_1 h_2) = (k \cdot h_1)(k \cdot h_2)$, ie. it is a homomorphism into $\mathrm{Aut}(H)$. Reverse the process:

Definition 1.8.2. *Given groups H, K together with a group homomorphism $\phi : K \mapsto \mathrm{Aut}(H)$, (an action of K on H – denote $k \cdot h = \phi(k)(h)$), the **semidirect product** $H \rtimes K$ is the set $H \times K$ with the binary operation*

$$(h, k)(h', k') := (h(k \cdot h'), kk').$$

Proposition 1.8.3. *$H \rtimes K$ forms a group.*

Proof.

$$\begin{aligned}
((h,k)(h',k'))(h'',k'') &= (h(k\cdot h'),kk')(h'',k'') \\
&= (h(k\cdot h')(kk'\cdot h''),kk'k''), \quad \text{and} \\
(h,k)((h',k')(h'',k'')) &= (h,k)(h'(k'\cdot h''),k'k'') \\
&= \big(h(k\cdot (h'(k'\cdot h''))),kk'k''\big).
\end{aligned}$$

However, since $\mathrm{Im}\phi \subset \mathrm{Aut}(H)$,

$$k\cdot(h'(k'\cdot h'')) = (k\cdot h')(k\cdot(k'\cdot h'')) = (k\cdot h')(kk'\cdot h'').$$

$\therefore$ $((h,k)(h',k'))(h'',k'') = (h,k)((h',k')(h'',k''))$.

$$\begin{aligned}
(e,e)(h',k') = (e(e\cdot h'),ek') = (eh',ek') = (h',k'), \quad \text{and} \\
(h,k)(e,e) = (h(k\cdot e),ke) = (he,ke) = (h,k).
\end{aligned}$$

(Here, $k\cdot e = e$ since $\mathrm{Im}\phi \subset \mathrm{Aut}(H)$.) Hence (e,e) is the identity.

$$\begin{aligned}
(h,k)(k^{-1}\cdot h^{-1},k^{-1}) &= \big(h(k\cdot(k^{-1}\cdot h^{-1})),kk^{-1}\big) \\
&= \big(h((kk^{-1})\cdot h^{-1}),kk^{-1}\big) \\
&= (h(e\cdot h^{-1}),kk^{-1}) \\
&= (hh^{-1},kk^{-1}) \\
&= (e,e), \quad \text{and} \\
(k^{-1}\cdot h^{-1},k^{-1})(h,k) &= ((k^{-1}\cdot h^{-1})(k^{-1}\cdot h),k^{-1}k) \\
&= (k^{-1}\cdot(h^{-1}h),k^{-1}k), \quad \text{since } \mathrm{Im}\phi \subset \mathrm{Aut}(H) \\
&= (k^{-1}\cdot e,e) \\
&= (e,e).
\end{aligned}$$

Hence $(h,k)^{-1} = (k^{-1}\cdot h^{-1},k^{-1})$. □

Define

$$\begin{aligned}
i_H : H &\mapsto H \rtimes K \\
h &\mapsto (h,e), \quad \text{and} \\
i_K : K &\mapsto H \rtimes K \\
k &\mapsto (e,k)
\end{aligned}$$

Proposition 1.8.4. *i_H and i_K are (injective) group homomorphisms.*

Proof.

$$(h,e)(h',e) = (h(e \cdot h'), ee) = (hh', e)$$
$$(e,k)(e,k') = (e(k \cdot e), kk') = (ee, kk') = (e, kk')$$

□

Using i_H and i_K, regard H and K as subgroups of $H \rtimes K$.

$$\text{ie. } H \cong i_H(H) = \{(h,e)\} \leq H \rtimes K$$
$$K \cong i_K(K) = \{(e,k)\} \leq H \rtimes K$$

Proposition 1.8.5. *$H \lhd (H \rtimes K)$ and $(H \rtimes K)/H \cong K$.*

Proof. Define $\phi : H \rtimes K \twoheadrightarrow K$ by $\phi(h,k) = k$. Then

$$\phi((h,k)(h',k')) = \phi(h(k \cdot h'), kk') = kk'$$

so ϕ is a group homomorphism.

$$\ker\phi = \{(h,e) \in H \rtimes K\} = i_H(H) \cong H.$$

□

Returning to the motivating example, $H \lhd G, K \leq G, H \cap K = \{e\}$, and by construction,

$$HK \cong H \rtimes K.$$

Proposition 1.8.6. *If both $H \lhd G$ and $K \lhd G$ with $H \cap K = \{e\}$ then $\mu : H \times K \mapsto HK$ is an isomorphism.*

Proof. For $h \in H, k \in K$,

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K, \quad \text{and}$$
$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$$

So $hkh^{-1}k^{-1} \in H \cap K = \{e\}$.

$$\text{ie. } hk = kh \quad \forall h \in H, k \in K.$$

Hence

$$\mu(h,k)\mu(h',k') = hkh'k' = hh'kk' = \mu(hh',kk') = \mu((h,k)(h',k')).$$

$\therefore$ μ is a homomorphisms, so $\mu : H \times K \xrightarrow{\cong} HK$. □

Proposition 1.8.7. *Let H, K be groups and let $\phi : K \mapsto \mathrm{Aut}(H)$. TFAE:*

1. *$H \times K \cong H \rtimes K$.*
2. *ϕ is the trivial homomorphism.*
3. *$K \lhd (H \rtimes K)$.*

Proof.

$1 \Rightarrow 2$:

$$\forall h, h' \in H, k, k' \in K, \quad (hh', kk') = (h,k)(h',k') = (h(k \cdot h'), kk')$$

$\therefore \phi(k)(h') = k \cdot h' = h' \quad \forall h'$, ie. $\phi(k) = 1_H$.

$2 \Rightarrow 3$: Since H, K generate $H \rtimes K$, it suffices to check $hKh^{-1} \subset K$, $\forall h \in H$. Note that

$$(h,e)^{-1} = (h^{-1}, e),$$

so

$$\begin{aligned}
(h,e)(e,k)(h^{-1},e) &= (h(e \cdot e), ek)(h^{-1}, e) \\
&= (h,k)(h^{-1},e) \\
&= (h(k \cdot h^{-1}), ke) \\
&= (hh^{-1}, ke), \quad \text{by 2} \\
&= (e,k) \in K
\end{aligned}$$

$3 \Rightarrow 1$: This is the previous proposition. ◻

In particular, this proposition says that if G has normal subgroups H, K such that $H \cap K = \{e\}$ and $HK = G$ then $G \cong H \times K$.

Theorem 1.8.8. *Let $\phi : G \mapsto K$ be a group homomorphism. Suppose $\exists$ a group homomorphism $s : K \mapsto G$ such that $\phi s = 1_K$. (s is called a **section** or a **right splitting** of ϕ.) Then*

$$G \cong (\ker \phi) \rtimes K$$

Proof. Observe that existence of a function $s : K \mapsto G$ such that $\phi s = 1_K$ implies that ϕ is onto and s is injective. Let $H = \ker \phi$. Set

$$\tilde{K} = \mathrm{Im} s \xleftarrow{\cong} s\, K.$$

Then

$$(\ker \phi) \rtimes K \cong H \rtimes \tilde{K} \cong H\tilde{K} \leq G$$

so it suffices to show $H\tilde{K} = G$.

Given $g \in G$, let $k = \phi(g) \in K$ and let

$$\tilde{k} = s(k) = s\phi(g) \in \tilde{K}.$$

Then

$$\phi(\tilde{k}) = \phi s\phi(g) = \phi(g),$$

since $\phi s = 1_K$. Hence $g\tilde{k}^{-1} \in \ker\phi = H$, and so $g \in H\tilde{K}$. Thus $G = H\tilde{K}$. $\square$

A right splitting of ϕ does not make G a product. In contrast, a left splitting does imply that G is a product:

Theorem 1.8.9. *Let $H \lhd G$. Let $i : H \mapsto G$ be the inclusion map. Suppose $\exists$ a group homomorphism $r : G \mapsto H$ such that $ri = 1_H$. Then*

$$G \cong H \times G/H.$$

Proof. Define $\theta : G \mapsto H \times (G/H)$ by

$$\theta(g) = (rg, qg)$$

where $q : G \twoheadrightarrow G/H$ is the quotient projection $g \mapsto gH$. Then θ is a homomorphism.

If $\theta(g) = \theta(g')$ then $r(g) = r(g')$ and $gH = g'H$, so let $g' = gh$ for some $h \in H$. Hence

$$r(g) = r(g') = r(g)r(h),$$

so

$$e = r(h) = ri(h) = h.$$

$\therefore g' = gh = ge = g$. Thus θ is injective.

To show θ is surjective, it suffices to show $H \times \{e\} \subset \mathrm{Im}\theta$ and $\{e\} \times (G/H) \subset \mathrm{Im}\theta$, since these generate $H \times (G/H)$.

Given $h \in H$,

$$\theta(h) = (r(h), hH) = (h, e).$$

Given $q(g) = gH \in G/H$, let $h = r(g)$ and set $g' = h^{-1}g$. Then

$$\begin{aligned}\theta(g') &= (r(h^{-1}g), q(h^{-1}g)) \\ &= (r(h^{-1})r(g), q(g)) \\ &= (h^{-1}h, q(g)) \\ &= (e, q(g))\end{aligned}$$

So θ is onto. $\square$

Example 1.8.10. *Use* $\phi = \epsilon : S_3 \mapsto C_2$*. Then* $\ker\phi \cong A_3$*. Let*

$$\begin{aligned} s : C_2 &\mapsto S_3 \quad \text{by} \\ s(1) &= e \\ s(-1) &= (1\ 2) \end{aligned}$$

s is a right splitting. Thus $S_3 \cong A_3 \rtimes C_2$*.*

1.9 Sylow Theorems

Throughout this section, p denotes a prime and G is a finite group.

Suppose $|G| = n$. If $H \leq G$ then by Lagrange, $|H| \,\Big|\, n$. However, the converse is false, eg. if $G = S_5$ then $n = 120$, but G has no subgroups of order $15, 30$, or 40. However, $\exists$ a partial converse:

Theorem 1.9.1 ((First) Sylow Theorem)**.** *If $p^t \,\Big|\, |G|$ then $\exists H \leq G$ such that $|H| = p^t$.*

Proof. Write $|G| = mp^t$. Find $r \geq 0$ such that $p^r \mid m$ but $p^{r+1} \nmid m$.

Lemma 1.9.2. *$p^r \,\Big|\, \begin{pmatrix} mp^t \\ p^t \end{pmatrix}$ but $p^{r+1} \nmid \begin{pmatrix} mp^t \\ p^t \end{pmatrix}$.*

Proof.

$$\begin{pmatrix} mp^t \\ p^t \end{pmatrix} = \frac{(mp^t)(mp^t - 1)\cdots(mp^t - p^t + 1)}{(p^t)(p^t - 1)\cdots 3 \cdot 2 \cdot 1}$$

If $0 < j < p^t$ then

$$\begin{aligned} \#\text{ of times } p \text{ divides } p^t - j &= \#\text{ of times } p \text{ divides } j \\ &= \#\text{ of times } p \text{ divides } mp^t - j \end{aligned}$$

$\therefore$ Powers of p cancel except for those in the factor m. □

Proof of Theorem continued. Let $\mathcal{S} = \{S \subset G \mid |S| = p^t\}$. Define right action

$$\mathcal{S} \times G \mapsto \mathcal{S} \quad \text{by} \quad S \cdot g = Sg.$$

$\mathcal{S}$ has $\begin{pmatrix} mp^t \\ p^t \end{pmatrix}$ elements, so there exists an orbit $X = \{S_1, S_2, \ldots, S_k\}$ (of size k) such that $p^{r+1} \nmid k$. (If p^{r+1} divided the number of elements in each orbit then p^{r+1} would divide $|\mathcal{S}|$).

$\mathrm{Orb}(S_1) = X$ by definition. Set $H := \mathrm{Stab}(S_1) \leq G$. Then

$$|H| = \frac{|G|}{|X|} = \frac{mp^t}{k} = \left(\frac{m}{k}\right) p^t.$$

By construction, $p^{r+1} \nmid k$ so p divides m at least as many times as p divides k. Thus $|H|$ is divisible by p^t, and in particular,

$$|H| \geq p^t.$$

Pick $s \in S_1$. Then $\forall h \in H$, $sh \in S_1$ but $h \neq h' \Rightarrow sh \neq sh'$. Hence

$$p^t = |S_1| \geq |H|.$$

$\therefore |H| = p^t$. □

Definition 1.9.3. *Suppose $|G| = n$. Let p be a prime and let p^t be the largest power of p dividing n. Then a subgroup of G having order p^t is called a **Sylow p-subgroup** of G.*

Notation: $\mathrm{Syl}_p(G) := \{\text{Sylow } p\text{-subgroups of } G\}$.

Corollary 1.9.4 (Corollary to Sylow Theorem)**.** $\mathrm{Syl}_p(G)$ *is non-empty* $\forall p$.

Suppose $H \leq G$. Then $\forall g \in G$, $gHg^{-1} \leq G$ and

$$\begin{aligned} H &\overset{\cong}{\longmapsto} gHg^{-1} \\ x &\mapsto gxg^{-1} \end{aligned}$$

In particular, $|gHg^{-1}| = |H|$. (gHg^{-1} is called a **conjugate subgroup** of H in G.)

$$P \in \mathrm{Syl}_p(G) \Rightarrow \; gPg^{-1} \in \mathrm{Syl}_p(G) \quad \forall g \in G.$$

Pick $P \in \mathrm{Syl}_p(G)$. Let

$$X = \{\text{Sylow } p\text{-subgroups of } G \text{ which are conjugate to } P\}.$$

G acts on X by $g \cdot S = gSg^{-1}$.

If $Q \leq G$, can restrict to get an action of Q on X. For an action of Q on $\mathrm{Syl}_p(G)$, have

$$|Q| = |\mathrm{Orb}_Q(S)|\,|\mathrm{Stab}_Q(S)|.$$

Here,

$$\mathrm{Stab}_Q(S) = \{q \in Q \mid qSq^{-1} = S\} = \mathrm{N}_Q(S).$$

Lemma 1.9.5. *If Q is a p-subgroup then for any Sylow p-subgroup S,*

$$\mathrm{N}_Q(S) = S \cap Q.$$

Proof. Let $H = \mathrm{N}_Q(S)$. From the definition, $S \cap Q \subset H$. Conversely, $H \subset Q$, so it suffices to show $H \subset S$. Consider SH.

$$SH = HS \leq G, \quad \text{since } S \triangleleft H.$$

$$|SH| = \frac{|S|\,|H|}{|S \cap H|} = |S|\frac{|H|}{|S \cap H|} \geq |S|.$$

$H = \mathrm{N}_Q(S) \leq Q \Rightarrow |H|$ is a power of $p \Rightarrow |SH|$ is a power of p. But S is a Sylow p-subgroup and $S \subset SH$, so $S = SH$.

$\therefore H =\subset$. Thus $H = S \cap Q$. $\square$

Lemma 1.9.6. $|X| \equiv 1 \mod p$.

Proof. Write $X = \{P = S_1, \ldots, S_r\}$. For any Q the action of Q on X divides X into orbits:

$$|X| = \sum_{orbits} (\text{\# of elts. in that orbit}).$$

Apply this with $Q = S_1 = P$:

$$\mathrm{Stab}_P(S) = \mathrm{N}_P(S) = P \cap S.$$

$\therefore |\mathrm{Stab}_P(S)| \,\Big|\, |P|$, with equality only when $S = P$. Hence,

$$|\mathrm{Orb}_P(S)| = \frac{|P|}{|\mathrm{Stab}_P(S)|}$$

is one when $S = P$, and is divisible by p otherwise. So

$$\begin{aligned} |X| &= \sum_{\text{orbits}} (\text{\# of elts. in that orbit}) \\ &= 1 + \sum_{\substack{\text{orbits not} \\ \text{containing } P}} (\text{\# of elts. in that orbit}) \\ &\equiv 1 \mod p. \end{aligned}$$

□

Lemma 1.9.7. *If Q is a p-subgroup then $Q \subset P_j$ for some $P_j \in X$.*

Proof. Again,

$$|X| = \sum_{orbits} (\text{\# of elts. in that orbit}).$$

Unless $Q \subset P_j$ for some j then for each j, $Q \cap P_j$ will be a proper subset of Q, so that

$$|\mathrm{Orb}_Q(P_j)| = \frac{|Q|}{|\mathrm{Stab}_Q(P_j)|} \text{ is divisible by } p \quad \forall j.$$

But if $p \mid (\text{\# of elements in orbit})$ for each orbit then $p \,\Big|\, |X|$, contradicting the last lemma.

$\therefore Q \subset P_j$ for some j. □

Corollary 1.9.8. $\mathrm{Syl}_p(G) = X$.

Proof. For $S \in \mathrm{Syl}_p(G)$, $|S|$ is a power of $p \Rightarrow S \subset P_j$ for some $P_j \in X$. But $|S| = |P_j|$ since both are Sylow p-subgroups.

$\therefore S = P_j \in X$. ◻

Lemma 1.9.9. $|\mathrm{Syl}_p(G)| \,\Big|\, |G|$.

Proof. Consider the action of G on $\mathrm{Syl}_p(G)$. Let $P \in \mathrm{Syl}_P(G)$.

$$|G| = |\mathrm{Orb}_G(P)|\,|\mathrm{Stab}_G(P)|$$

$$\mathrm{Orb}_G(P) = \{\text{subgroups of } G \text{ conjugate to } P\} = X = \mathrm{Syl}_p(G).$$

$\therefore |\mathrm{Syl}_P(G)|$ divides G. ◻

In summary:

Theorem 1.9.10 ((Main) Sylow Theorem)**.** *Let G be a finite group and let p be a prime.*

1. $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$.
2. $|\mathrm{Syl}_p(G)| \,\Big|\, |G|$.
3. *Any two Sylow p-subgroups of G are conjugate (and in particular, isomorphic).*
4. *Every p-subgroup of G is contained in some Sylow p-subgroup. In particular, every element whose order is a power of p is contained in some Sylow p-subgroup.*

Proof. Showed that if $X = \{\text{Sylow } p\text{-subgroups conjugate to } P\}$ then $\mathrm{Syl}_P(G) = X \iff 3$.
Also showed $|X| \equiv 1 \mod p \iff 1$.
Also showed: every p-subgroup of G is contained in some $S \in X \iff 4$.
Also showed $|\mathrm{Syl}_P(G)| \,\Big|\, |G| \iff 2$. ◻

Corollary 1.9.11. *Let P be a Sylow p-subgroup of G. Then* $P \lhd G \iff$ *P is the unique Sylow p-subgroup.*

Proof.

$\Leftarrow$: Suppose $\exists!$ Sylow p-subgroup. Since gPg^{-1} is a Sylow p-subgroup $\forall g$,

$$gPg^{-1} = P \quad \forall G,$$

ie. $P \lhd G$.

$\Rightarrow$: Suppose $P \lhd G$. Then the only subgroup of G conjugate to P is P. By Sylow Theorem, 3, P is the only Sylow p-subgroup.

□

Corollary 1.9.12. *Let P be a Sylow p-subgroup of G. Let $N = \mathrm{N}_G(P)$. Then*

$$\mathrm{N}_G(N) = N.$$

In particular, $N \lhd G$ iff $P \lhd G$.

Proof. Set $H := \mathrm{N}_G(N)$. Then $\forall h \in H$, $hPh^{-1} \subset N$ and $|hPh^{-1}| = |P|$, so hPh^{-1} is a Sylow p-subgroup of G. But then hPh^{-1} is also a Sylow p-subgroup of N. However, $P \lhd N$, so P is the unique Sylow p-subgroup of N.

$\therefore hPh^{-1} = P$, so $h \in \mathrm{N}_G(P) = N$. Hence $H \subset N$, so $H = N$.

In particular, if $N \lhd G$ then $N = H = G$ so $P \lhd G$. □

1.10 Applications of Sylow's Theorem

1. Suppose $|G| = 15$. Then

$$\left.\begin{array}{r}|\mathrm{Syl}_5(G)| \equiv 1 \mod 5\\ |\mathrm{Syl}_5(G)| \bigm| 15\end{array}\right. \Rightarrow |\mathrm{Syl}_5(G)| = 1,$$

$\therefore\ \exists!$ element of $\mathrm{Syl}_5(G)$. Let H be the unique Sylow 5-subgroup, so $H \lhd G$. Similarly,

$$\left.\begin{array}{r}|\mathrm{Syl}_3(G)| \equiv 1 \mod 3\\ |\mathrm{Syl}_3(G)| \bigm| 15\end{array}\right. \Rightarrow |\mathrm{Syl}_3(G)| = 1,$$

so $\exists!$ Sylow 3-subgroup K, and so $K \lhd G$.

Pick generators $h \in H, k \in K$; $|h| = 5, |k| = 3$. H, K are normal $\Rightarrow hk = kh$, so $|hk| = 15$. Hence, G has an element of order 15, so $G \cong C_{15}$.

2. Suppose $|G| = 10$.

$$\left.\begin{array}{r}|\mathrm{Syl}_5(G)| \equiv 1 \mod 5\\ |\mathrm{Syl}_5(G)| \bigm| 10\end{array}\right. \Rightarrow |\mathrm{Syl}_5(G)| = 1.$$

Let H be the unique Sylow 5-subgroup. Then $H \lhd G$. Pick a generator h.

$$\left.\begin{array}{r}|\mathrm{Syl}_2(G)| \equiv 1 \mod 2\\ |\mathrm{Syl}_2(G)| \bigm| 10\end{array}\right. \Rightarrow |\mathrm{Syl}_2(G)| = 1 \text{ or } 5.$$

Case I: $|\mathrm{Syl}_2(G)| = 1$. Then $G \cong C_{10}$, using argument above.

Case II: $|\mathrm{Syl}_2(G)| = 5$.
Let K be a Sylow 2-subgroup; $K = \{e, k\}$. If $hk = kh$ then $|hk| = 10$ and we would be in Case I. Hence,

$$hkh^{-1} = k_2 = \text{generator of a different Sylow 2-subgroup.}$$

Similarly, $h^2kh^{-2}, h^3kh^{-3}, h^4kh^{-4}$ must be the generators of the other Sylow 2-subgroups. (Again, if $h^ikh^{-i} = h^jkh^{-j}$ for $i \neq j$ then $h^{j-i}k = kh^{j-i}$ and we would be in Case I.)

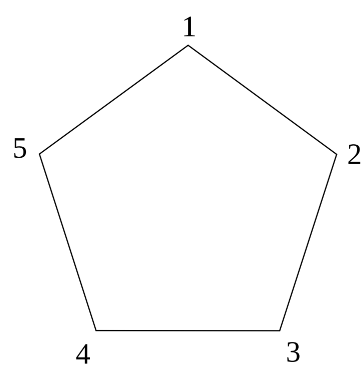
$\therefore$ Can list the ten elements of G:

$$\begin{array}{cc} e & k \\ h & hkh^{-1} \\ h^2 & h^2kh^{-2} \\ h^3 & h^3kh^{-3} \\ h^4 & h^4kh^{-4} \end{array}$$

From this, we can construct the group table. eg. what is hk?
Well, $hk \neq h^j$ for any j, so hk has order 2.

$$\begin{aligned}
\therefore\ hkhk &= e \\
hkh &= k^{-1} = k \\
\therefore\ hk &= h(hkh) \\
&= h^2kh \\
&= h^2(hkh)h \\
&= h^3kh^2 \\
&= h^3kh^{-3}.
\end{aligned}$$

This group must be D_{10}.



$$\begin{aligned}
h &\mapsto (1\ 2\ 3\ 4\ 5) \\
k &\mapsto (2\ 5)(3\ 4)
\end{aligned}$$

Conclusion: If $|G| = 10$ then $G \cong C_{10}$ or $G \cong D_{10}$.
In passing: note the existence of an element k of order 2 in D_{10} gives a splitting

$$D_{10} \underset{s}{\overset{\longrightarrow}{\dashleftarrow}} D_{10}/H \cong C_2$$

where if $C_2 = \{e, x\}$ then $s(x) = k$. Thus

$$D_{10} \cong H \rtimes C_2 = C_5 \rtimes C_2.$$

The corresponding homomorphism $\phi : C_2 \mapsto \mathrm{Aut}(C_5)$ is given by $k \cdot h = h^{-1} = h^4$. ($\mathrm{Aut}(C_5) \cong C_4$ is generated by the map τ, taking h to h^2. The only element of order 2 in $\mathrm{Aut}(C_5)$ is $\tau \circ \tau$, which is $h \mapsto h^4$.)

3. Suppose $|G| = 12$. Then

$$|\mathrm{Syl}_2(G)| = 1 \text{ or } 3,$$
$$|\mathrm{Syl}_3(G)| = 1 \text{ or } 4.$$

Case I: $|\mathrm{Syl}_2(G)| = 3$ and $|\mathrm{Syl}_3(G)| = 4$.
Since two distinct groups of order 3 intersect only in the identity, and each Sylow 3-subgroup has 2 elements of order 3, G has $4 \times 2 = 8$ elements of order 3. The remaining 4 elements must form a Sylow 2-subgroup.

$\therefore$ There aren't enough elements left to form any more Sylow 2-subgroups. This is a contradiction, so Case I doesn't occur.

Case II: $|\mathrm{Syl}_2(G) = 1$.
Let H be the unique Sylow 2-subgroup, so $H \lhd G$. $|H| = 4$, so either $H \cong C_4$ or $H \cong C_2 \times C_2$.

Case IIa: $H \cong C_4(\sigma)$.
Let τ be an element of some Sylow 3-subgroup, $|\tau| = 3$.

$$\begin{matrix} \tau\sigma\tau^{-1} \in H \\ |\tau\sigma\tau^{-1}| = |\sigma| = 4 \end{matrix} \;\Rightarrow\; \tau\sigma\tau^{-1} = \text{either } \sigma \text{ or } \sigma^3.$$

If $\tau\sigma\tau^{-1} = \sigma^3$ then

$$\tau\sigma^3\tau^{-1} = (\tau\sigma\tau^{-1})^3 = \sigma^9 = \sigma.$$

Moreover, $\tau^3 = e$, so

$$\sigma = \tau^3\sigma\tau^{-3} = \tau^2(\tau\sigma\tau^{-1})\tau^2 = \tau^2\sigma^3\tau^{-2} = \tau(\tau\sigma^3\tau^{-1})\tau^{-1} = \sigma^3.$$

This is a contradiction. Thus, $\tau\sigma\tau^{-1} = \sigma$.

Using the fact that τ and σ commute, $|\tau\sigma| = 12$. Thus $G \cong C_{12}$.

Equivalent way of phrasing argument that $\tau\sigma\tau^{-1} = \sigma$: Let $T = \{e, \tau, \tau^2\}$. H is normal $\Rightarrow T$ acts on H via $\tau \cdot \sigma := \tau\sigma\tau^{-1}$.

$$|\mathrm{Orb}(\sigma)|\,|\mathrm{Stab}(\sigma)| = |T| = 3.$$

σ has order $2 \Rightarrow x \cdot \sigma$ has order 2 $\forall x \in T$. So $\mathrm{Orb}(\sigma) \subset \{\sigma, \sigma^3\}$. Since $|\mathrm{Orb}(\sigma)|$ divides 3, $\mathrm{Orb}(\sigma) = \{\sigma\}$.

$\therefore \tau\sigma\tau^{-1} = \sigma$.

Another rephrasing: $H \lhd G$.

$$G \underset{s}{\overset{\longrightarrow}{\leftarrow - - -}} G/H \cong C_3,$$

where s takes the generator a to τ. ie. The existence of an element τ of order 3 in G gives a splitting, so

$$G \cong C_4 \rtimes_\phi C_3$$

for some $\phi : C_3 \mapsto \mathrm{Aut}(C_4)$. However, $\mathrm{Aut}(C_4) \cong C_2 = \{1_{C_4}$ and $\sigma \mapsto \sigma^3\}$. so the only homomorphism $C_3 \mapsto \mathrm{Aut}(C_4)$ is trivial.

$\therefore G \cong C_4 \times C_3 \cong C_{12}$.

Case IIb: $H \cong C_2 \times C_2$.

Let

$$H = \{e, \sigma_1, \sigma_2, \sigma_3\}, \quad \sigma_j^2 = e.$$

Let $T = \{e, \tau, \tau^2\}$ be some Sylow 3-subgroup.

$$G \underset{s}{\overset{\longrightarrow}{\leftarrow - - -}} G/H \cong C_3,$$

and thus,

$$G \cong H \rtimes_\phi T,$$

with $\phi : T \mapsto \mathrm{Aut}(H) \cong$ permutations of $\{\sigma_1, \sigma_2, \sigma_3\} \cong S_3$. So

$$(\phi(\tau))(\sigma_1) = \tau\sigma_1\tau^{-1} = \sigma_1, \sigma_2, \text{ or } \sigma_3.$$

Case IIbi: $\tau\sigma_1\tau^{-1} = \sigma_1$. Then since the order of $\phi(\tau)$ must divide the order of τ, which is 3, $\phi(\tau) = \mathrm{id}$. Hence $\phi = \mathrm{id}$ and

$$G \cong H \times T \cong C_2 \times C_2 \times C_3.$$

Case IIIbii: $\tau\sigma_1\tau^{-1} \neq \sigma_1$.

So $\tau\sigma_1\tau^{-1} = \sigma_2$ or σ_3. By symmetry, assume $\tau\sigma_1\tau^{-1} = \sigma_2$. Then $\phi(\tau)$ must be a 3-cycle, so $\tau\sigma_2\tau^{-1} = \sigma_3$.

Elements of G:

$$\begin{array}{cccc} e & \sigma_1 & \sigma_2 & \sigma_3 \\ \tau & \tau\sigma_1 & \tau\sigma_2 & \tau\sigma_3 \\ \tau^2 & \tau^2\sigma_1 & \tau^2\sigma_2 & \tau^2\sigma_3 \end{array}$$

Each σ_j has order 2, and the elements τ, τ^2, $\tau\sigma_j$ and $\tau^2\sigma_j$ each have order 3. Multiplication is determined by $\tau\sigma_1\tau^{-1} = \sigma_2$ and $\tau\sigma_2\tau^{-1} = \sigma_3$. eg.

$$\sigma_1\tau = \tau\tau^{-1}\sigma_1\tau = \tau\tau^2\sigma_1\tau^{-2} = \tau\tau\sigma_2\tau^{-1} = \tau\sigma_3.$$

What group is this? Let T_1, T_2, T_3, T_4 be the Sylow 3-subgroups. ie.

$$\begin{aligned} T_j &= \{e, \tau\sigma_j, (\tau\sigma_j)^2\} \quad j = 1, 2, 3, \\ T_4 &= \{e, \tau, \tau^2\} \end{aligned}$$

Let $X = \{T_1, T_2, T_3, T_4\}$. Conjugation by elements of G permutes elements of X, ie. have morphism

$$\theta : G \mapsto S_X = S_4.$$

What is $\theta(\tau)$?

$$\begin{aligned} \tau T_1\tau^{-1} &= \{\tau e\tau^{-1}, \tau(\tau\sigma_1)\tau^{-1} = \tau\sigma_2, \tau(\tau\sigma_1)^2\tau^{-1}\} = T_2 \\ \tau T_2\tau^{-1} &= \{\tau e\tau^{-1}, \tau(\tau\sigma_2)\tau^{-1} = \tau\sigma_3, \quad \cdots \quad \} = T_3 \\ \tau T_3\tau^{-1} &= T_1 \\ \tau T_4\tau^{-1} &= T_4 \end{aligned}$$

ie. $\tau \overset{\theta}{\longmapsto} (1\ 2\ 3)$.
What is $\theta(\sigma_1)$? $\sigma_1 T_1\sigma_1^{-1} = ?$
Suffices to compute $\sigma_1(\tau\sigma_1)\sigma_1^{-1}$.

$$\sigma_1(\tau\sigma_1)\sigma_1^{-1} = \sigma_1\tau = \tau\sigma_3.$$

$\therefore\ \sigma_1(\tau\sigma_1)\sigma_1^{-1} = T_3$. $|\sigma_1| = 2 \Rightarrow \sigma_1 T_3\sigma_1^{-1} = T_1$. Likewise, $\sigma_1 T_4\sigma_1^{-1} = T_2$. So $\sigma_1 \mapsto (1\ 3)(2\ 4)$.
What is $\theta(\sigma_2)$?

$$\sigma_2 T_1\sigma_2^{-1} = \sigma_2\tau\sigma_1\sigma_2^{-1} = \tau\sigma_1^2\sigma_2^{-1} = \tau\sigma_2 \in T_2$$

etc., get $\sigma_2 \mapsto (1\ 2)(3\ 4)$.

$$G \cong A_4.$$

Case III: $|\mathrm{Syl}_2(G)| = 3$, so $|\mathrm{Syl}_3(G)| = 1$.
Let $T = \{e, \tau, \tau^2\}$ be the unique Sylow 3-subgroup, so $T \lhd G$. Let H be a Sylow 2-subgroup. $|H| = 4$, so $H \cong C_4$ or $C_2 \times C_2$. Then

$$H \hookrightarrow G \mapsto\!\!\!\!\!\rightarrow G/T$$

is an isomorphism (it is an injection since $H \cap T = \{e\}$ for degree reasons, and since $|H| = 4 = |G/T|$, it is bijective). This splits $q : G \twoheadrightarrow G/T$, so

$$G \cong T \rtimes_\phi H.$$

Case IIIa: $H \cong C_2 \times C_2$.

Let $H = \{e, \sigma_1, \sigma_2, \sigma_3\}$.

$$\phi : H \mapsto \mathrm{Aut}T = \mathrm{Aut}C_3 \cong C_2.$$

If $\phi(h) = 1_T \ \forall h \in H$ then $G = T \times H$, transposing to Case II. So ϕ is non-trivial, ie. $\phi(h)(\tau) = \tau^2$ for some $h \in H$. Then

$$\ker\phi = C_2$$

so $\exists h \in H$ such that $h \neq e$ and $\phi(h) = 1_T$. $\phi(h')(\tau) = \tau^2$ for the other two non-trivial elements h' of H. By symmetry, suppose $\phi(\sigma_3) = 1_T$, ie.

$$\phi(\sigma_1)(\tau) = \sigma_1\tau\sigma_1^{-1} = \tau^2,$$
$$\phi(\sigma_2)(\tau) = \sigma_2\tau\sigma_2^{-1} = \tau^2,$$
$$\phi(\sigma_3)(\tau) = \sigma_3\tau\sigma_3^{-1} = \tau.$$

This determines multiplication in G.

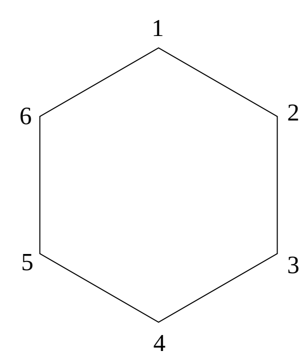
What group is this? $\sigma_3\tau = \tau\sigma_3$, so $|\sigma_3\tau| = |\sigma_3|\,|\tau| = 2 \cdot 3 = 6$. Set $x = \sigma_3\tau$. Elements of G:

$$\begin{array}{cccccc} e & x & x^2 & x^3 & x^4 & x^5 \\ \sigma_1 & x\sigma_1 & x^2\sigma_1 & x^3\sigma_1 & x^4\sigma_1 & x^5\sigma_1 \end{array}$$

Multiplication of elements in this form can be derived from:

$$\sigma_1 x = \sigma_1 x \sigma_1^{-1}\sigma_1 = \sigma_1\sigma_3\tau\sigma_1^{-1}\sigma_1 = \sigma_3(\sigma_1\tau\sigma_1^{-1})\sigma_1 = \sigma_3\tau^2\sigma_1 = \sigma_3^5\tau^5\sigma_1 = x^5\sigma_1.$$

So $G \cong D_{12}$.



$$x \mapsto (1\ 2\ 3\ 4\ 5\ 6)$$
$$\sigma_1 \mapsto (2\ 6)(3\ 5)$$

What are the 3 Sylow 2-subgroups? One is $H = \{e, \sigma_1, \sigma_2, \sigma_3\}$. Note that

$$\begin{aligned} \sigma_3 &= \sigma_3^3\tau^3 = x^3, \\ \sigma_2 &= \sigma_3\sigma_1 = x^3\sigma_1 \end{aligned}$$

$\therefore H = \{e, \sigma_1, x^3\sigma_1, x^3\}$.

To find the others, pick $g \in G$ and compute gHg^{-1}.

$$\begin{aligned} g = x \;\Rightarrow\; gHg^{-1} &= \{e, x\sigma_1x^{-1}, xx^3\sigma_1x^{-1}, xx^3x^{-1}\} \\ &= \{e, x\sigma_1x^5, x^4\sigma_1x^5, x^3\} \\ &= \{e, x(x^5)^5\sigma_1, x^4(x^5)^5\sigma_1, x^3\} \\ &= \{e, x^{26}\sigma_1, x^{29}\sigma_1, x^3\} \\ &= \{e, x^2\sigma_1, x^5\sigma_1, x^3\}. \end{aligned}$$

The other is $\{e, x^4\sigma_1, x\sigma_1, x^3\}$.

Note that different Sylow p-subgroups can intersect non-trivially. eg. Here, x^3 is in all Sylow 2-subgroups.

Case IIIb: $H \cong C_4$.

Let $H = \{e, \sigma, \sigma^2, \sigma^3\}$. Recall

$$G \cong T \rtimes_\phi H,$$
$$T = \{e, \tau, \tau^2\},$$
$$\phi : H \cong C_4 \mapsto \mathrm{Aut}(T) \cong C_2$$

Aside from trivial ϕ (yielding $G \cong T \times H \cong C_3 \times C_4$, which is Case IIa), ϕ acts non-trivially on σ and σ^3. ie. $\sigma\tau\sigma^{-1} = \tau^2$. Elements of G are:

$$\begin{array}{cccc} e & \sigma & \sigma^2 & \sigma^3 \\ \tau & \tau\sigma & \tau\sigma^2 & \tau\sigma^3 \\ \tau^2 & \tau^2\sigma & \tau^2\sigma^2 & \tau^2\sigma^3 \end{array}$$

Multiplication is determined by $\sigma\tau\sigma^{-1} = \tau^2$ (and $\tau^3 = e, \sigma^4 = e$).

In summary, there are 5 (non-isomorphic) groups of order 12: $C_{12},\ C_2 \times C_2 \times C_3,\ A_4,\ D_{12}$, and $C_3 \rtimes C_4$.

1.11 Solvable and Nilpotent Groups

Let G be a group, $A, B \subset G$.
Notation: $[A, B] :=$ subgrp. of G generated by $\{[a, b] \mid a \in A, b \in B\}$. So $[G, G]$ is the commutator subgroup of G.

Inductively define:

$$\begin{aligned} G^{(0)} &:= G, \\ G^{(n)} &:= [G^{(n-1)}, G^{(n-1)}], \quad \text{and} \\ G'^{(0)} &:= G, \\ G'^{(n)} &:= [G^{(n-1)}, G]. \end{aligned}$$

Then

$$\begin{array}{ccccccccccl} G = G^{(0)} & \geq & G^{(1)} & \geq & G^{(2)} & \geq \cdots \geq & G^{(n)} & \geq \cdots & \textbf{Derived (or commutator) series of } G \\ \| & & \| & & \leq & & \leq & & \\ G'^{(0)} & \geq & G'^{(1)} & \geq & G'^{(2)} & \geq \cdots \geq & G'^{(n)} & \geq \cdots & \textbf{Lower central series of } G \end{array}$$

Definition 1.11.1. *G is called **solvable** if $\exists N$ such that $G^{(N)} = \{e\}$. G is called **nilpotent** if $\exists N$ such that $G'^{(N)} = \{e\}$.*

Since $G^{(n)} \leq G'^{(n)}$, nilpotent $\Rightarrow$ solvable. We already showed $[G, G] \lhd G$, so $G^{(n)} \lhd G^{(n-1)}$. In fact:

Proposition 1.11.2.
1. *$G^{(n)} \lhd G$ $\forall n$. In particular, $G^{(n)} \lhd G^{(n-1)}$ (because for $A \leq B \leq G$, if $A \lhd G$ then $A \lhd B$).*
2. *$G'^{(n)} \lhd G$ $\forall n$. In particular, $G'^{(n)} \lhd G'^{(n-1)}$.*

Proof.
1. For $g \in G$ and $[a, b]$ a generator of $G^{(n)}$, where $a, b \in G^{(n-1)}$,

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [G^{(n-1)}, G^{(n-1)}]$$

by induction.

2. For $g \in G$ and $[a, b]$ a generator of $G'^{(n)}$, where $a \in G'^{(n-1)}$ and $b \in G$,

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [G'^{(n-1)}, G]$$

by induction.

□

Notice that $G^{(n-1)}/G^{(n)} = G^{(n-1)}_{ab}$ is abelian. Conversely:

Proposition 1.11.3. *G is solvable iff $\exists$ a finite sequence of subgroups*

$$\{e\} = H_N \lhd H_{N-1} \lhd \cdots \lhd H_0 = G$$

such that H_{n-1}/H_n is abelian for all n.

Proof. Suppose that such a sequence exists. Since H_{n-1}/H_n is abelian, $[H_{n-1}, H_{n-1}] \leq H_n$ for all n. Inductively,

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \leq [H_{n-1}, H_{n-1}] \leq H_n$$

so $G^{(n)} \leq H_n$ $\forall n$. Thus,

$$G^{(N)} \leq H_N = \{e\}$$

$\therefore G^{(N)} = \{e\}$. □

Lemma 1.11.4. *S_n is solvable iff $n < 5$.*

Proof.

$n = 1, 2$: S_n is abelian and thus solvable.

$n = 3$: Note that $[\sigma, \tau]$ is always an even permutation, so

$$[S_n, S_n] \leq A_n \quad \forall n.$$

When $n = 3$, $A_3 \cong C_3$ is abelian, so S_3 is solvable.

$n = 4$: Since $[S_4, S_4] \leq A_4$, in suffices to check that A_4 is solvable. Let

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Then $H \cong C_2 \times C_2$ is abelian, $H \lhd A_4$, and

$$|A_4/H| = 3,$$

so $A_4/H \cong C_3$ is abelian.

$n \geq 5$: Let $\sigma = (1\ 5\ 3)$, $\tau = (1\ 4\ 2)$. Then

$$\begin{aligned}[\sigma, \tau] &= \sigma\tau\sigma^{-1}\tau^{-1} \\ &= (1\ 5\ 3)(1\ 4\ 2)(1\ 3\ 5)(1\ 2\ 4) \\ &= (1\ 2\ 3) \in [S_n, S_n]\end{aligned}$$

Similarly, every 3-cycle is a commutator of 3-cycles, provided $n \geq 5$. Thus, $\forall k$, $A_n^{(k)}$ contains every 3-cycle.

$\therefore A_n^{(k)} \neq \{e\}\ \forall k$, so A_n is not solvable.

□

Theorem 1.11.5. *Suppose $A \triangleleft B$. Then B is solvable $\iff$ both A and B/A are solvable. Furthermore, if $A \leq B$ and B is solvable then A is solvable (even if A is not normal in B).*

Proof. Suppose B is solvable and $A \leq B$. Then $A^{(j)} \leq B^{(j)}\ \forall j$, so $B^{(k)} = \{e\}$ for some $k \Rightarrow A^{(k)} = \{e\}$, so A is solvable.

$\Rightarrow$: Suppose now that $A \triangleleft B$ and let $\pi : B \mapsto B/A$ be the canonical projection. If $x \in B$ lies in B' then $\pi(x) \in (B/A)'$, and conversely, if

$$y = (\overline{u}\,\overline{v}\,\overline{u})^{-1}(\overline{v})^{-1} \in (B/A)'$$

then $y = \pi(uvu^{-1}v^{-1}) \in \pi(B')$. Hence,

$$\begin{aligned}\pi(B') &= (B/A)' \\ \pi(B^{(2)}) &= \pi(B'') = (\pi(B'))' = (B/A)'' = (B/A)^{(2)} \\ &\vdots \\ \pi(B^{(k)}) &= \cdots = (B/A)^{(k)}\end{aligned}$$

Since $\pi(B^{(k)}) = \{e\}$, $(B/A)^{(k)} = \{e\}$, whence B/A is solvable.

$\Leftarrow$: Suppose A and B/A are both solvable. If $\{e\} = (B/A)^{(k)} = \pi(B^{(k)})$ then $B^{(k)} \subset A$. Thus, $B^{(k+j)} = (B^{(k)})^{(j)} \subset A^{(j)}$. So if $A^{(m)} = \{e\}$ then $B^{(k+m)} = \{e\}$. Hence, B is solvable.

□

Theorem 1.11.6. *G is finite and solvable $\Rightarrow \exists$ subgroups*

$$\{e\} = A_m \triangleleft A_{m-1} \triangleleft \cdots \triangleleft A_1 \triangleleft A_0 = G$$

such that A_j/A_{j+1} is cyclic of prime order $\forall j$.

Proof. The proceding theorem reduces the proof to the case where G is abelian, and it is clear that a finite abelian group has such a composition series. $\square$

Upper Central Series:
Given a group G, inductively define $Z_n(G)$ as follows: Set $Z_0 := \{e\}$. Having defined Z_{n-1} such that $Z_{n-1} \lhd G$, define Z_n as the pullback:

$$\begin{tikzcd}
Z_n \arrow[r] \arrow[d] & \mathrm{Z}(G/Z_{n-1}) \arrow[d, "\vartriangle"] \\
G \arrow[r, two heads, "q_{n-1}"] & G/Z_{n-1}
\end{tikzcd}$$

where $q_{n-1} : G \mapsto G/Z_{n-1}$ is the quotient map. ie.

$$Z_n := q_{n-1}^{-1}(\mathrm{Z}(G/Z_{n-1})).$$

$Z_n \lhd G$ because $\mathrm{Z}(G/Z_{n-1}) \lhd G/Z_{n-1}$.

$$q_{n-1}([Z_n, G]) \subset [\mathrm{Z}(G/Z_{n-1}, G/Z_{n-1}] = \{e\},$$

so $[Z_n, G] \subset \ker q_{n-1} = Z_{n-1}$.

Lemma 1.11.7. *G is nilpotent iff $Z_N(G) = G$ for some N.*

Proof.

$\Rightarrow$: Suppose $Z_N = G$.

$$G'^{(1)} = [G, G] = [Z_N, G] \leq Z_{N-1}.$$

Inductively,

$$G'^{(k)} = [G'^{(k-1)}, G] \leq [Z_{N-(k+1)}, G] \leq Z_{N-k}.$$

$\therefore G'^{(N)} \leq Z_0 = \{e\}$ so G is nilpotent.

$\Leftarrow$: Suppose $G'^{(N)} = \{e\}$. Inductively (as k decreases), assume

$$[G'^{(k)}, G] = G'^{(k+1)} \leq Z_{N-k-1}.$$

Suppose $x \in G'^{(k)}$. Given $\overline{g} = q_{N-k-1}(g) \in G/Z_{N-k-1}$,

$$\begin{aligned}
[q_{N-k-1}(x), \overline{g}] &= q_{N-k-1}[x, g] \\
&\in q_{N-k-1}([G'^{(k)}, G]) \\
&\subset q_{N-k-1}(Z_{N-k-1}) \\
&= \{e\}.
\end{aligned}$$

$\therefore q_{N-k-1}(x)$ commutes with $\overline{g}\ \ \forall\, \overline{g} \in G/Z_{N-k-1}$ so

$$q_{N-k-1}(x) \in \mathrm{Z}(G/Z_{N-k-1}).$$

$\therefore x \in Z_{N-k}$.

Thus $G'^{(k)} \leq Z_{N-k}\ \forall k$. Therefore,

$$Z_N \geq G'^{(0)} = G$$

$\therefore Z_N = G$ as required.

$\square$

Corollary 1.11.8. *If G is a finite group then G is nilpotent iff $\forall n$, $\mathrm{Z}(G/Z_n) \neq \{e\}$ unless $G/Z_n = \{e\}$.*

Proof. If $\mathrm{Z}(G/Z_n) = \{e\}$ then $Z_{n+1} = q_{n-1}^{-1}\{e\} = Z_n$, so the series

$$Z_0 \leq Z_1 \leq \cdots Z_n \leq Z_{n+1} \leq \cdots$$

never reaches G (unless $Z_n = G$ already).

Conversely, if $\forall n$, $\mathrm{Z}(G/Z_n) \neq \{e\}$ then

$$Z_n < Z_{n+1} \quad \forall n$$

and since G is finite, eventually $Z_n = G$. $\square$

Corollary 1.11.9. *If G is a p-group then G is nilpotent.*

Lemma 1.11.10. *G is nilpotent iff $G/\mathrm{Z}(G)$ is nilpotent. More precisely, $Z_{N+1}(G) = G$ iff $Z_N(G/\mathrm{Z}(G)) = G/\mathrm{Z}(G)$.*

Proof. Set $H := G/\mathrm{Z}(G)$.

$$\begin{tikzcd}
Z_2(G) \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & \mathrm{Z}(G) = Z_1(H) \arrow[d, hook] \\
G \arrow[r, "q_1"'] & H \ = G/\mathrm{Z}(G) = G/Z_1(G)
\end{tikzcd}$$

Suppose inductively that $Z_{n-1}(G)$ is isomorphic to the pullback

$$\begin{tikzcd}
P_{n-1} \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & Z_{n-2}(H) \arrow[d] \\
G \arrow[r, two heads, "q_1"'] & H
\end{tikzcd}$$

By a property of pullbacks (Proposition 1.5.5),

$$G/Z_{n-1}(G) \cong G/P_{n-1} \cong H/Z_{n-2}(H).$$

So

$$\begin{tikzcd}
P_n \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & Z_{n-1}(H) \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & \mathrm{Z}(H/Z_{n-2}(H)) \cong \mathrm{Z}(G/Z_{n-1}(G)) \arrow[d] \\
G \arrow[r, two heads, "q_1"'] & H \arrow[r, two heads] & H/Z_{n-2}(H) \cong G/Z_{n-1}(G)
\end{tikzcd}$$

Then P_n is isomorphic to the composite pullback, which, by definition, is $Z_n(G)$. So

$$Z_n(G) \cong P_n \quad \forall n.$$

If H is nilpotent then $\exists N$ such that $Z_N(H) = H$. Then

$$\begin{tikzcd}
Z_{N+1}(G) \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & Z_N(H) \arrow[d] \\
G \arrow[r, two heads, "q_1"'] & H
\end{tikzcd}$$

shows $Z_{N+1} = G$.

Conversely, if $Z_{N+1}(G) = G$ for some N then the pullback shows

$$H/Z_N(H) \cong G/Z_{N+1}(G) \cong \{e\}$$

so $Z_N(H) = H$. □

Corollary 1.11.11. *G is nilpotent iff the sequence of surjections*

$$\begin{array}{ccccccccc}
Q_0 & \twoheadrightarrow & Q_1 & \twoheadrightarrow & Q_2 & \twoheadrightarrow \cdots \twoheadrightarrow & Q_n & \twoheadrightarrow \cdots \\
\parallel & & \parallel & & \parallel & & \parallel & \\
G & & G/\mathrm{Z}(G) & & Q_1/\mathrm{Z}(Q_1) & & Q_{n-1}/\mathrm{Z}(Q_{n-1}) &
\end{array}$$

eventually reaches $\{e\}$. ($Q_N = \{e\}$ for some N).

Proof.

⇒: Q_n is nilpotent iff Q_{n+1} is nilpotent. So, if $Q_N = \{e\}$ then Q_N is nilpotent, so $Q_0 = G$ is nilpotent.

⇐: Suppose that G is nilpotent with $Z_N(G) = G$. Then $Z_{N-1}(Q_1) = Q_1$ and inductively, $Z_{N-k}(Q_k) = Q_k\ \forall k$. Then

$$\mathrm{Z}(Q_{N-1}) = Z_1(Q_{N-1}) = Q_{N-1}$$

so $Q_N = Q_{N-1}/\mathrm{Z}(Q_{N-1}) = \{e\}$.

□

Corollary 1.11.12. *A finite product of nilpotent groups is nilpotent.*

Proof. By induction, it suffices to consider the product of two nilpotent groups, G_1 and G_2.

$$\begin{aligned} Q_1(G_1 \times G_2) &= \frac{G_1 \times G_2}{\mathrm{Z}(G_1 \times G_2)} \\ &= \frac{G_1 \times G_2}{\mathrm{Z}(G_1) \times \mathrm{Z}(G_2)} \\ &= G_1/\mathrm{Z}(G_1) \times G_2/\mathrm{Z}(G_2) \\ &= Q_1(G_1) \times Q_1(G_2) \end{aligned}$$

By iterating, $Q_n(G_1 \times G_2) = Q_n(G_1) \times Q_n(G_2)$. So if $Q_{N_1}(G_1) = \{e\}$ and $Q_{N_2}(G_2) = \{e\}$ then $Q_{\max\{N_1,N_2\}}(G_1 \times G_2) = \{e\}$. □

Theorem 1.11.13. *Let G be a finite group. For each prime p, let P_p be a Sylow p-subgroup. Then TFAE:*

1. *G is nilpotent.*
2. *$H < G \Rightarrow H < \mathrm{N}_G(H)$ (every proper subgroup of G is a proper subgroup of its normalizer).*
3. *$P_p \lhd G \quad \forall p$.*
4. *$G \cong \prod_p P_p$.*

Proof.

1 ⇒ 2: Suppose $H < G$. $\mathrm{Z}(G) \leq \mathrm{N}_G(H)$, so unless $\mathrm{Z}(G) \subset H$, it is immediate that $H < \mathrm{N}_G(H)$.

So assume $\mathrm{Z}(G) \subset H$. Write $\overline{G} := G/\mathrm{Z}(G)$ and let

$$q : G \mapsto\!\!\!\rightarrow \overline{G}$$

be the quotient map. Set $\overline{H} = q(H) < \overline{G}$. G nilpotent $\Rightarrow \overline{G}$ nilpotent. By induction (assuming 1 $\Rightarrow$ 2 is known for all groups of order less than $|G|$),

$$\overline{H} < \mathrm{N}_{\overline{G}}\left(\overline{H}\right).$$

But then by the 4th Isomorphism Theorem,

$$H = q^{-1}\left(\overline{H}\right) < q^{-1}\mathrm{N}_{\overline{G}}\left(\overline{H}\right) = \mathrm{N}_G(H).$$

2 $\Rightarrow$ 3: Let $N = \mathrm{N}_G(P_p)$. By a corollary to the Sylow Theorem (Corollary 1.9.12), $\mathrm{N}_G(N) = N$.

$\therefore$ Hypothesis 2 $\Rightarrow N = G$, so $P_p \lhd G$.

3 $\Rightarrow$ 4: Write

$$|G| = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}.$$

Suppose by induction (on m) that

$$H = P_{p_1} \cdots P_{p_{m-1}} \cong P_{p_1} \times \cdots P_{p_{m-1}}.$$

Then $H \lhd G$, $P_{p_m} \lhd G$, and $H \cap P_{p_m} = \{e\}$. Hence,

$$P_{p_1} \cdots P_{p_m} = HP_{p_m} \cong H \times P_{p_m} \cong P_{p_1} \times \cdots P_{p_m}.$$

However, $|P_{p_1} \cdots P_{p_m}| = |G|$ so $P_{p_1} \cdots P_{p_m} = G$.

4 $\Rightarrow$ 1: It was already shown that p-groups are nilpotent and a finite product of nilpotent groups is nilpotent.

$\square$

1.12 Free Groups

Theorem 1.12.1. *A subgroup of a free group is free.*

Proof. Let S be a set and let $G = F(S)$. Suppose $H \leq G$. Let

$$S' = S \amalg \{\text{inverses of elts. in } S\}.$$

Recall that elements of G are finite length words in S and S'. Let $M(S')$ denote the free monoid on S' (so that in $M(S')$, ss^{-1} does not simplify for $s \in S$). $\exists$ a surjective map of monoids $q : M(S') \mapsto F(S)$ given by

$$q(x) = x \quad \forall x \in M(S').$$

Write $\overline{x}$ for $q(x)$.

Say that a word $x = x_1 \cdots x_k \in M(S')$ (where $x_i \in S'$ $\forall i$) is **reduced** (or a reduced representative) if $\nexists$ a shorter word $y \in M(S')$ s.t. $q(x) = q(y) = x_1 \cdots x_k$ in G.

Well-order S'. This induces a well-order on $M(S')$ by ordering the words first by length, and then lexicographically among words of the same length. Let

$$R = \{\text{reduced words}\} \subset M(S').$$

ie. $x \in R$ iff $x = \min q^{-1}\{q(x)\}$. For $g \in G$, define $\tilde{g} \in M(S')$ by

$$\tilde{g} = \min q^{-1}(Hg).$$

ie. $\tilde{g} = \min\{x \in M(S') \mid H\overline{x} = Hg\}$. Let

$$\tilde{R} = \{\tilde{g} \mid g \in G\} \subset M(S')$$

be the set of chosen coset representatives. Clearly, only reduced words can occur: $\tilde{R} \subset R$.

Lemma 1.12.2. *A left substring of an element in $\tilde{R}$ is in $\tilde{R}$.*

Proof. Suppose $b = cu \in M(S')$ with $b \in \tilde{R}$ and c a proper substring. Check that $c \in \tilde{R}$.

Since $b \in \tilde{R}$ and c is shorter than b, $H\overline{b} \neq H\overline{c}$ (or else, c would be the chosen coset rep. for $H\overline{b}$ rather than b). If $c \notin \tilde{R}$ then $c' < c$ and $H\overline{c'} = Hc$. So

$$H\overline{b} = H\overline{cu} = H\overline{c'}\overline{u} = H\overline{c'u}.$$

However, the ordering is such that $x < y \Rightarrow\ xz < yz$. So $c' < c \Rightarrow\ c'u < b$, which contradicts the minimality of b. $\square$

Proof of Theorem continued. Given $r \in \tilde{R}$, $s \in S'$, define $v_{rs} \in H$ by

$$v_{rs} = \overline{r}s(\overline{r'})^{-1}, \quad \text{where } r' = \widetilde{\overline{r}s} \in \tilde{R}.$$

ie. r' is the canonical rep. for $H\overline{r}s$. So $H\overline{r'} = H\overline{r}s$, and thus $v_{rs} \in H$.

Notice $v_{rs}^{-1} = \overline{r'}s^{-1}(\overline{r})^{-1}$, and

$$H\overline{r'} = H\overline{rs} \Rightarrow H\overline{r} = H\overline{r'}s^{-1},$$

and since $r \in \tilde{R}$, r is the canonical rep. for $H\overline{r'}s^{-1}$. Thus

$$v_{r,s}^{-1} = v_{r',s^{-1}},$$

so $\{v_{r,s} \mid r \in \tilde{R}, s \in S'\}$ is closed under inverses. Let

$$T = \{v_{rs} \in H \mid r \in \tilde{R}, s \in S', v_{rs} \neq e\}.$$

Note that it is possible to have $v_{r,s} = v_{r',s'}$ without $r = r'$ and $s = s'$.

Define $\phi : F(T) \mapsto H$ by $\phi(v_{rs}) := v_{rs}\ \forall v_{rs} \in T$. To finish the proof that H is free, we show that ϕ is an isomorphism.

Let $h \in H$. Write $h = s_1 \cdots s_\ell$ in terms of generators of G. Set $b_1 = e$ and inductively set $b_{j+1} = \widetilde{\overline{b_j}s_j}$ (ie. b_{j+1} is the canon. rep. for coset $H\overline{b_j}s_j$).

$\therefore$ By construction, $v_{b_j,s_j} = \overline{b_j}s_j\overline{b_{j+1}}^{-1}$. By induction,

$$H\overline{b_{j+1}} = H\overline{b_j}s_j = H\overline{b_{j-1}}s_{j-1}s_j = \cdots H\overline{b_1}s_1 \cdots s_j = Hs_1 \cdots s_j.$$

$\therefore H\overline{b_{\ell+1}} = Hs_1 \cdots s_\ell = Hh = H$, so $\overline{b_{\ell+1}} = e$.

$$\phi(v_{b_1,s_1}v_{b_2,s_2} \cdots v_{b_\ell,s_\ell}) = \overline{b_1}s_1(\overline{b_2})^{-1}\overline{b_2}s_2(\overline{b_2})^{-1} \cdots \overline{b_\ell}s_\ell(\overline{b_{\ell+1}})^{-1} = s_1 \cdots s_\ell = h.$$

$\therefore \phi$ is onto.

Suppose $\phi(x) = e$ for some $x \in F(T)$ and $x \neq e$. Let $x = x_1 \cdots x_\ell$ be an expression for x as a reduced word in the elts. of T. Recall that the elemnts of T can be written as $v_{r,s}$ in many ways. For each $i = 1, \ldots, \ell$, pick the expression $x_i = v_{b_i,s_i}$ in which $b_i \in \tilde{R}$ be minimal. Then v_{b_i,s_i} contains an occurrence of s_i, since if s_i cancelled then, using the fact that $\tilde{R}$ is closed under left substrings, a shorter b_i' and an s_i' could be picked such that $x_i = v_{b_i',s_i'}$.

Since $\phi(x) = e$, within G, the string $\phi(x)$, which initially contains all of $s_1, \ldots, s_\ell$, must reduce to eliminate them. So $\exists m$ such that $\phi(v_{b_m,s_m}v_{b_{m+1},s_{m+1}})$ reduces to eliminate s_m or s_{m+1} (or both). Write $v_{b_m,s_m}v_{b_{m+1},s_{m+1}}$ as:

$$\overline{b_m}s_m(\overline{y})^{-1}\overline{b_{m+1}}s_{m+1}(\overline{z})^{-1},$$

where y = canon. rep. for $H\overline{b_m}s_m$ and z = canon. rep. for $H\overline{b_{m+1}}s_{m+1}$. Cancellation of at least one of s_m, s_{m+1} can happen in one of three ways:

1. $\overline{y} = \overline{b_{m+1}}$ and $s_m = s_{m+1}^{-1}$, or

2. $\overline{b_{m+1}} s_{m+1}$ is a left substring of $\overline{y}$, or

3. $\overline{y} s_m^{-1}$ is a left substring of $\overline{b_{m+1}}$.

If 1: $H\overline{z} = H\overline{b_{m+1}} s_{m+1} = H\overline{y} s_m^{-1} = H\overline{b_m}$, so $z = b_m$ (both lie in $\tilde{R}$ and they represent the same coset). So $v_{b_{m+1},s_{m+1}} = (v_{b_m,s_m})^{-1}$ and the word x was not reduced, which is a contradiction.

If 2: Since $b_m, y, b_{m+1}, z \in \tilde{R} \subset R$, all are reduced, so $\overline{b_{m+1}} s_{m+1}$ is a left substring of $\overline{y} \Rightarrow b_{m+1} s_{m+1}$ is a left substring of y. Hence $b_{m+1} s_{m+1} \in \tilde{R}$. So $b_{m+1} s_{m+1}$ and z are canon. reps. for the coset $Hb_{m+1} s_{m+1}$, so $z = b_{m+1} s_{m+1}$. But then $v_{b_{m+1},s_{m+1}} = e$ so $v_{b_{m+1},s_{m+1}} \notin T$, which is a contradiction.

If 3: As in case 2, ys_m^{-1} is a left substring of b_{m+1} so $ys_m^{-1} \in \tilde{R}$ and represents the same coset as b_m. So $b_m = ys_m^{-1}$ and so $v_{b_m,s_m} = e \notin T$, which is a contradiction.

$\therefore$ None of these cases can occur, so $\phi(x) = e$ for $x \neq e$ is not possible. Hence ϕ is an injection. □

Note: it is possible that H is not finitely generated, even if G is finitely generated. e.g. Let $G = F(x, y)$ and let $H = [G, G]$ (the commutator subgroup). Then

$$H = F(x, y, [y, x], [[y, x], x], \ldots, [\cdots [[y, x], x]x \cdots, x], \ldots \}.$$

Chapter 2

Rings and Modules

2.1 Rings

Definition 2.1.1. *A **ring** consists of a set R together with binary operations $+$ and $\cdot$ satisfying:*

1. $(R, +)$ *forms an abelian group,*

2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in R$,

3. $\exists 1 \neq 0 \in R$ *such that* $a \cdot 1 = 1 \cdot a = a$ $\forall a \in R$, *and*

4. $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$ $\forall a, b, c \in R$.

Note:

1. Some people (e.g. Dummit + Foote) do not require condition 3, and refer to a "ring with identity" if they want to assume $\cdot$ has an identity element.

2. People who include existence of a unit in their defn. of a ring refer to a "ring without identity" for an object satisfying the other three axioms. Some people (e.g. Jacobson) call this a "rng".

3. Some people (e.g. Lang) do not require $1 \neq 0$ in condition 3.

Definition 2.1.2. *R is called **commutative** if its multiplication is commutative, ie.*

$$ab = ba \quad \forall a, b \in R.$$

Definition 2.1.3. *A **ring homomorphism** from R to S is a function $f : R \mapsto S$ such that $\forall a, b \in R$:*

1. $f(a + b) = f(a) + f(b)$,

2. $f(ab) = f(a)f(b)$, *and*

3. $f(1) = 1$.

A bijective ring homomorphism is called an ***isomorphism****.*

Definition 2.1.4. *A* ***subring*** *of R is a subset A which forms a ring such that the inclusion $A \hookrightarrow R$ is a ring homomorphism. A subgroup I of the abelian group $(R, +)$ is called a (two -sided)* ***ideal*** *if*

$$x \in I, r \in R \Rightarrow \; rx \in I \text{ and } xr \in I.$$

Similarly if a subgroup I satisfies

$$x \in I, r \in R \Rightarrow \; rx \in I,$$

I is called a ***left ideal****, and if it satisfies*

$$x \in I, r \in R \Rightarrow \; xr \in I,$$

it is called a ***right ideal****.*

Example 2.1.5. *If $f : R \mapsto S$ is a homomorphism then* $\ker f := \{x \in R \mid f(x) = 0\}$ *is an ideal in R. (An ideal is always a subrng but never a subring, unless it is all of R.)*

Theorem 2.1.6. *Let $I \subsetneq R$ be a proper ideal. Then $\exists$ a ring R/I and a surjective ring homomorphism $f : R \twoheadrightarrow R/I$ such that* $\ker f = I$.

Proof. Define an equivalence relation on R by $x \sim y \iff x - y \in I$. Let

$$R/I := \{\text{equiv. classes}\}.$$

Define operations on R/I by

$$[x] + [y] := [x + y],$$
$$[x] \cdot [y] := [xy].$$

Check that these are well-defined and produce a ring structure on R/I.

Define $f : R \mapsto R/I$ by $f(x) = [x]$. f is a ring homomorphism. Moreover, $f(x) = 0$ iff $[x] = 0$ iff $x = x - 0 \in I$. ◻

Definition 2.1.7. *The ring R is called a* ***division ring*** *if $(R - \{0\}, \cdot)$ forms a group. A commutative division ring is called a* ***field****.*

An element $u \in R$ for which $\exists v \in R$ such that $uv = vu = 1$ is called a **unit**.

Notation: $R^\times = \{\text{units of R}\}$. This forms a group under multiplication.

A non-zero element $x \in R$ is called a **zero divisor** if $\exists y \neq 0$ such that either $xy = 0$ or $yx = 0$. A commutative ring with no zero divisors is called an **integral domain**.

Proposition 2.1.8. *If $x \neq 0$ is not a zero divisor and $xy = xz$ then $y = z$.*

Proof. $x(y - z) = 0$ and x is not a zero divisor so either $x = 0$ or $y - z = 0$. But $x \neq 0$ so $y = z$. ◻

Theorem 2.1.9 (First Isomorphism Theorem)**.** *Let $f : R \mapsto S$ be a ring homomorphism. Then $R/\ker f \cong \mathrm{Im} f$.*

Theorem 2.1.10 (Second Isomorphism Theorem)**.** *Let $A \subset R$ be a subring and let $I \subsetneq R$ be a proper ideal. Then $A + I := \{a + x \mid a \in A, x \in I\}$ is a subring of R, $A \cap I$ is a proper ideal in A, and*

$$(A + I)/I \cong A/(A \cap I).$$

Theorem 2.1.11 (Third Isomorphism Theorem)**.** *Let $I \subset J$ be proper ideals of R. Then $J/I := \{[x] \in R/I \mid x \in J\}$ is an ideal in R/I, and*

$$\frac{R/I}{J/I} \cong R/J.$$

Theorem 2.1.12 (Fourth Isomorphism Theorem)**.** *Let I be a proper ideal of R. Then the correspondence $J \mapsto J/I$ is a bijection between the ideals of J containing I and the ideals of R/I.*

Let I, J be ideals in R. Define ideals

$$\begin{aligned} I + J &:= \{x + y \mid x \in I, y \in J\}, \\ I \cap J&, \\ IJ &:= \left\{ \sum_{i=1}^{n} x_i y_y \mid n \in \mathbb{N}, x_i \in I, y_i \in J \right\} \end{aligned}$$

Then

$$IJ \subset I \cap J \subset I \cup J \subset I + J.$$

(Note that $I \cup J$ may not be an ideal.) $I + J$ is the smallest ideal containing both I and J.

2.2 Maximal and Prime Ideals

Definition 2.2.1. *An ideal $M \subsetneq R$ is called a* ***maximal ideal*** *if $\nexists$ an ideal I s.t. $M \subsetneq I \subsetneq R$.*

Lemma 2.2.2. *Given an ideal $I \subsetneq R$, $\exists$ a maximal ideal M s.t. $I \subset M$.*

Proof. Let
$$\mathcal{S} = \{\text{ideals } J \mid I \subset J \subsetneq R\}.$$
Then $\mathcal{S}$ is a partially ordered set (ordered by inclusion). If $\mathcal{C} \subset \mathcal{S}$ is a chain (ie. a totally ordered subset) then
$$J = \bigcup_{C \in \mathcal{C}} C$$
is an ideal which forms an upper bound for $\mathcal{C}$ in $\mathcal{S}$ (it is indeed a proper ideal since $1 \notin J$).
$\therefore$ Zorn's Lemma $\Rightarrow \mathcal{S}$ has a maximal element M. □

For the rest of this section, suppose that R is commutative.

Proposition 2.2.3. *R is a field $\iff$ the only ideals of R are $\{0\}$ and R.*

Proof.

$\Rightarrow$: Let R be a field and let $I \subset R$ be an ideal. If $I \neq \{0\}$ then $\exists x \neq 0 \in I$.
R a field $\Rightarrow \exists y \in R$ such that $xy = yx = 1$. Since I is an ideal, $1 \in I$, so $r \in I$ $\forall r \in R$. Thus $I = R$.

$\Leftarrow$: Suppose the only ideals in R are $\{0\}$ and R. Let $x \neq 0 \in R$. Let
$$I = Rx := \{rx \mid r \in R\}.$$
I is an ideal and $x = 1x \in R$, so $I \neq 0$. Hence $I = R$, so $1 \in I$. ie. $1 = yz$ for some $y \in R$.

$\therefore$ Every $x \neq 0 \in R$ has an inverse, so R is a field.

□

Corollary 2.2.4. *Let $f : F \mapsto S$ be a ring homomorphism where F is a field. Then f is injective.*

Proof. $\ker f$ is a proper ideal in F, so $\ker f = 0$. □

Theorem 2.2.5. *M is a maximal ideal $\iff R/M$ is a field.*

Proof. The 4^{th} iso. thm. says $\exists$ a bijection between the ideals of R containing M and the ideals of R/M.
$\therefore \exists I$ s.t. $M \subsetneq I \subsetneq R \iff \exists J$ s.t. $\{0\} \subsetneq J \subsetneq R/M$. ie. M is not maximal $\iff R/M$ is not a field. □

Definition 2.2.6. *An ideal $\mathcal{P} \subsetneq R$ is called a* ***prime ideal*** *if $ab \in \mathcal{P}$ implies $a \in \mathcal{P}$ or $b \in \mathcal{P}$.*

Theorem 2.2.7. *$\mathcal{P}$ is a prime ideal $\iff R/\mathcal{P}$ is an integral domain.*

Proof.

$\Rightarrow$: Suppose $\mathcal{P}$ is a prime ideal. If $[xy] = [x][y] = 0$ in $R/\mathcal{P}$ then $xy \in \mathcal{P}$, so either $x \in \mathcal{P}$ or $y \in \mathcal{P}$. ie. either $[x] = 0$ or $[y] = 0$. Thus $R/\mathcal{P}$ has no zero divisors.

$\Leftarrow$: Suppose $R/\mathcal{P}$ is an integral domain. If $xy \in \mathcal{P}$ then $[x][y] = 0$ in $R/\mathcal{P}$, so $[x] = 0$ or $[y] = 0$. ie. either $x \in \mathcal{P}$ or $y \in \mathcal{P}$.

□

Corollary 2.2.8. *A maximal ideal is a prime ideal.*

Proof. A field is an integral domain. □

Notation: $a \mid b$ means $\exists c$ s.t. $b = ac$ (say a **divides** b).

Proposition 2.2.9. *In an integral domain, if $a \mid b$ and $b \mid a$ then $b = ua$ for some unit u.*

Proof. $a \mid b \Rightarrow b = ua$ for some $u \in R$. $b \mid a \Rightarrow a = vb$ for some $v \in R$.
$\therefore b = ua = uvb$, and since b is not a zero divisor, $1 = uv$. Thus, u is a unit. □

Definition 2.2.10. *q is called a* ***greatest common divisor*** *of a and b if:*

1. *$q \mid a$ and $q \mid b$, and*
2. *If c also satisfies $c \mid a, c \mid b$ then $c \mid q$.*

Notation: $q = \gcd(a, b)$ means q is the greatest common divisor of a and b.
We say a and b are **relatively prime** if $\gcd(a, b) = 1$.

Proposition 2.2.11. *Let R be an integral domain. If $q = \gcd(a, b)$ and $q' = \gcd(a, b)$ then $q' = uq$ for some unit u. Conversely, if $q = \gcd(a, b)$ and $q' = uq$ where u is a unit then $q' = \gcd(a, b)$.*

Proof. Let $q = \gcd(a, b)$. If $q' = \gcd(a, b)$ then $q' \mid q$ and $q \mid q'$ so $q' = uq$ for some unit u.
Conversely, if $q' = uq$ for some unit u then $q' \mid q$ so $q' \mid a$ and $q' \mid b$. Also $q \mid q'$ so whenever $c \mid a$ and $c \mid b$, $c \mid q$ so $c \mid q'$. □

Definition 2.2.12. *A non-unit $p \neq 0 \in R$ is called a* ***prime*** *if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.*

Notation: Let $x \in R$. $(x) := Rx = \{rx \mid r \in R\}$ is called the **principal ideal** generated by x. Thus $y \in (x)$ iff $x \mid y$.

Likewise, for $x_1, \dots, x_n \in R$, let $(x_1, \dots, x_n)$ denote the following ideal:

$$\{r_1 x_1 + \cdots + r_n x_n \mid r_1, \dots, r_n \in R\},$$

ie. the ideal generated by $x_1, \dots, x_n$.

Proposition 2.2.13. *If $p \neq 0$ then p is prime $\iff$ (p) is a prime ideal.*

Proof.

$\Rightarrow$: Suppose p is prime. If $ab \in (p)$ then $ab = rp$ for some r, so $p \mid ab$. So $p \mid a$ or $p \mid b$. ie. $a \in (p)$ or $b \in (p)$.

$\Leftarrow$: Suppose (p) is a prime ideal. If $p \mid ab$ then $ab \in (p)$ so $a \in (p)$ or $b \in (p)$.

$\therefore p \mid a$ or $p \mid b$.

□

Nonzero elements x and y are called **associates** if $\exists$ a unit u s.t. $x = uy, y = u^{-1}x$. Thus, x, y are associate $\iff (x) = (y)$. ie. For associates x and y, $x \mid a$ iff $y \mid a$.

$x \sim y$ iff x, y are associate forms an equivalence relation on $R - \{0\}$.

Definition 2.2.14. *$x \in R$ is* ***irreducible*** *if $x \neq 0$, x is not a unit, and whenever $x = ab$, either a is a unit or b is a unit.*

Definition 2.2.15. *Ideals I and J are called* ***comaximal*** *or* ***relatively prime*** *if $I + J = R$.*

Theorem 2.2.16 (Chinese Remainder Theorem)**.** *Let R be a commutative ring. Let*

$$I_1, \dots, I_k \subset R$$

be ideals. Suppose I_i and I_j are comaximal whenever $i \neq j$. Let

$$\begin{aligned} \phi : R &\mapsto R/I_1 \times R/I_2 \times \cdots \times R/I_k \\ r &\mapsto (r + I_1, r + I_2, \dots, r + I_k). \end{aligned}$$

Then ϕ is surjective and

$$\ker \phi = I_1 \cap I_2 \cap \cdots \cap I_k = I_1 \cdots I_k.$$

Proof. Consider first the case when $k = 2$. Suppose I, J are comaximal. Then $\exists x \in I, y \in J$ s.t. $x + y = 1$. So $\phi(x) = (0, 1)$ and $\phi(y) = (1, 0)$. Since $(0, 1)$ and $(1, 0)$ generate $R/I \times R/J$, ϕ is surjective.

Clearly $\ker \phi = I \cap J$, and in general, $IJ \subset I \cap J$. For any $c \in I \cap J$,

$$c = c1 = cx + cy \in IJ.$$

$\therefore IJ = I \cap J$.

General case: set $I = I_1$, $J = I_2 \cdots I_k$. For each $i = 2, \ldots, k$, $\exists x_i \in I$ and $y_i \in I_i$ s.t. $x_i + y_i = 1$. Since $x_i + y_i \equiv y_i \mod I$,

$$1 = 1 \cdots 1 = (x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k) \equiv y_2 \cdots y_k \mod I$$

So $1 \in I + J$.
$\therefore R \twoheadrightarrow R/I \times R/J$ and by induction,

$$R/I \times R/J \twoheadrightarrow R/I_1 \times R/I_2 \times R/I_3 \times \cdots \times R/I_k$$

and

$$I_1 I_2 \cdots I_k = IJ = I \cap J = I_1 \cap I_2 \cap \cdots I_k.$$

$\square$

2.3 Polynomial Rings

Let R be a ring.

$$R[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid n \geq 0 \in \mathbb{Z} \text{ and } a_j \in R \text{ for } j = 0, \cdots, n\}$$

(modulo $0x^n + a_{n-1}x^{n-1} + \cdots + a_0 \sim a_{n-1}x^{n-1} + \cdots + a_0$). Operations are

$$\sum_{i=1}^{n} a_i x^i + \sum_{i=1}^{n} b_i x^i := \sum_{i=1}^{n} (a_i + b_i) x^i, \quad \text{and}$$
$$\left(\sum_{i=1}^{n} a_i x^i\right)\left(\sum_{i=1}^{m} b_i x^i\right) := \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

More formally,

$$(R[x], +) = \bigoplus_{n=0}^{\infty} R,$$

with multiplication defined by

$$(a_i)_{i\geq 0}(b_j)_{j\geq 0} = (c_k)_{k\geq 0} \quad \text{where } c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Inductively, set

$$R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])[x_n].$$

(called the **polynomial ring in n variables**). For an arbitrary set S, set

$$R[S] := \bigcup_{T=\text{finite subset of } S} R[T].$$

If $q(x) = \sum_{i=0}^{n} a_i x^i$ and $a_n \neq 0$ then n is called the **degree** of q. Embed $R \hookrightarrow R[x]$ via

$$r \mapsto r \quad \text{(polynomial of degree 0)}.$$

Some properties:

1. $R[x]$ is commutative $\iff R$ is commutative.
2. $R[x]$ is an integral domain $\iff R$ is an integral domain.
3. If R is an integral domain then $q(x) \in R[x]$ is invertible $\iff q(x) \in R$ and is invertible in R.

Proposition 2.3.1. *Let $I \subset R$ be an ideal. Let $I[x]$ denote the ideal of $R[x]$ generated by I. Then $R[x]/I[x] \cong (R/I)[x]$.*

Proof. Define $\phi : R[x] \mapsto (R/I)[x]$ by

$$\phi(\sum a_i x^i) := \sum \overline{a_i} x^i.$$

Then ϕ is onto and $\ker \phi = I[x]$, so

$$R[x]/I[x] \cong (R/I)[x].$$

□

Corollary 2.3.2. *$I[x]$ is a prime ideal $\iff$ I is a prime ideal.*

2.4 Modules

Definition 2.4.1. *Let R be a ring. A (left) **R-module** consists of an abelian group $(M, +)$, together with a function $\cdot : R \times M \mapsto M$ s.t.*

1. $(r + s)m = rm + sm\ \forall r, s \in R, m \in M$,
2. $r(m + n) = rm + rn\ \forall r \in R, m, n \in M$,
3. $(rs)m = r(sm)\ \forall r, s \in R, m \in M$, *and*
4. $1m = m\ \forall m \in M$.

*If R is a field, an R-module is also called a **vector space** over R.*

Definition 2.4.2. *An **R-module homomorphism** $f : M \mapsto N$ is a function satisfying*

1. $f(a + b) = f(a) + f(b)\ \forall a, b \in M$ *and*
2. $f(ra) = rf(a)\ \forall r \in R, a \in M$.

*If R is a field, an R-module homomorphism is also called a **linear transformation**. A bijective homomorphism is called an **isomorphism**.*

Definition 2.4.3. *A **submodule** of M is a subset A which forms an R-module s.t. the inclusion $A \hookrightarrow M$ is an R-module homomorphism. The R-module M is **simple** if its only submodules are M and $\{0\}$.*

Example 2.4.4.

1. *$M = R$ with $R \times M \mapsto M$ given by mult. in R. Submodules of R are left ideals.*
2. *$R = \mathbb{Z}$ and $M =$ abelian grp., with*

$$n \cdot x := x + \cdots + x, \quad \text{for } n \geq 0, \text{ and}$$
$$(-n) \cdot x := -(n \cdot x), \quad \text{for } n \geq 0.$$

   Conversely, any $\mathbb{Z}$-module is just an abelian group.

3. *F a field, V a vector space over F, $T : V \mapsto V$ a linear transformation. Let $R = F[x]$ and $M = V$. Define*

$$x^n \cdot v := T^n(v) = T(T^{n-1}v) \quad \forall v \in V$$

   and extend linearly to an action of $F[x]$ on V.

If $f : M \mapsto N$ is an R-module homomorphism then $\ker f$ is a submodule of M and $\mathrm{Im} f$ is a submodule of R. If M, N are R-modules, set

$$\hom_R(M, N) := \{R\text{-module homomorphisms from } M \text{ to } N\}.$$

$\hom_R(M, N)$ is an abelian group in general, and if R is commutative, it becomes an R-module via

$$(rf)(m) = f(rm).$$

Let N be a submodule of M. On the abelian group M/N, define the action of R by $r \cdot \overline{m} := \overline{r \cdot m}$. This is well-defined and produces an R-module structure on M/N.

Theorem 2.4.5.

1. *First Isomorphism Theorem*
   Let $f : M \mapsto N$ be an R-module homomorphism. Then $M/\ker f \cong \mathrm{Im} f$.

2. *Second Isomorphism Theorem Let A, B be submodules of M. Then*

$$(A + B)/B \cong A/(A \cap B)$$

   where $A + B = \{a + b \mid a \in A, b \in B\}$, which itself forms a submodule.

3. *Third Isomorphism Theorem Let $A \subset B \subset M$ be R-modules. Then*

$$\frac{M/A}{B/A} \cong M/B.$$

4. *Fourth Isomorphism Theorem Let $N \subset M$ be R-modules. Then $A \leftrightarrow A/N$ sets up a bijection between the submodules of M containing N and the submodules of M/N.*

A sequence

$$0 \longrightarrow A \xrightarrow{j} B \xrightarrow{f} C \longrightarrow 0$$

of R-module homomorphisms s.t. j is injective, f is surjective, and $\ker f = \mathrm{Im} j$ is called a **short exact sequence** of R-modules. 1^{st} iso. thm. $\Rightarrow C \cong B/\mathrm{Im} j$.

Proposition 2.4.6. *Let*

$$0 \longrightarrow A \xrightarrow{j} B \xrightarrow{f} C \longrightarrow 0$$

be a short exact sequence of R-modules. Then TFAE:

1. $\exists s : C \mapsto B$ *s.t.* $fs : C \mapsto C$ *is an isomorphism.*

2. $\exists r : B \mapsto A$ *s.t.* $rj : A \mapsto A$ *is an isomorphism.*

3. $B \cong A \oplus C$.

Remarks:

1. The fact that the above are isomorphic as abelian groups was discussed in the section on semidirect products, since for abelian groups, all subgroups are normal and semidirect products become products.

2. As discussed in semidirect product section, $2 \iff 3$, even for nonabelian groups, but in that situation, $1 \not\Rightarrow 2$ or 3.

Given a set S, $\exists$ an R-module M having the property that for any R-module M,

$$\hom_R(M, N) = \text{morphisms}_{\text{sets}}(S, N).$$

ie. An R-module homomorphism from M is uniquely determined by the images of the elts. of S. Explicitly,

$$M \cong R^S \equiv \bigoplus_S R.$$

M is called the **free R-module** with basis S. An R-module which possesses a basis is called a free R-module. An arbitrary elt. of a free R-module can be uniquely written as a finite linear combination

$$x = \sum r_i s_i$$

where $r_i \in R$ and $s_i \in S$. When $R = \mathbb{Z}$, the free $\mathbb{Z}$-module on S is also called the **free abelian group** on S, denoted $F_{ab}(S)$.

Let M be a right R-mod. and let N be a left R-mod. Define an abelian group $M \otimes_R N$ (tensor product of M, N over R) by

$$M \otimes_R N = F_{ab}(M \times N)/\sim$$

where

1. $(m, n_1 + n_2) \sim (m, n_1) + (m, n_2)\ \forall m \in M, n_1, n_2 \in N$,

2. $(m_1 + m_2, n) \sim (m_1, n) + (m_2, n)\ \forall m_1, m_2 \in M, n \in N$, and

3. $(m \cdot r, n) \sim (m, r \cdot n)\ \forall r \in R, m \in M, n \in N$.

Write $m \otimes n$ for the equiv. class of (m, n) in $M \otimes_R N$. So an arbitrary elt. of $M \otimes_R N$ has the form

$$\sum_{i=1}^{k} c_i(m_i \otimes n_i)$$

where $m_i \in M, n_i \in N, c_i \in \mathbb{Z}$.

Note that $R \otimes_R N \cong N$ and $M \otimes_R R \cong M$.

$M \otimes_R N$ has the universal property: q is R-bilinear and given bilinear $f : M \times N \mapsto A$,

$$\begin{tikzcd} M \times N \arrow[r, two heads, "q"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, dashed, "\exists! \overline{f}"] \\ & A \end{tikzcd}$$

f bilinear means:

$$\begin{aligned} f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n), \\ f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2), \quad \text{and} \\ f(mr, n) &= f(m, rn) \end{aligned}$$

If R is commutative then $M \otimes_R N$ becomes an R-module via

$$r \cdot (m \otimes n) := m \otimes (r \cdot n).$$

More generally, if M is an R-bimodule (ie. has both a left and a right R-module action which commute with each other) then $M \otimes_R N$ becomes a left R-module via

$$r \cdot (m \otimes n) := (r \cdot m) \otimes n.$$

Notice that R is an R-bimodule even if R is not commutative. (ie. Left multiplication commutes with right multiplication – R is associative.)

More generally, let $f : R \mapsto S$ be a ring homomorphism. Then S becomes an R-bimodule via

$$\begin{aligned} r \cdot s &:= f(r)s \\ s \cdot r &:= sf(r) \end{aligned}$$

This induces a map from R-modules to S-modules given by $N \mapsto S \otimes_R N$.

Example 2.4.7 (Extension of Coefficients)**.** *Let N be a vector space over a field F. Let $F \hookrightarrow K$ be an extension field. Elts. of N are finite sums*

$$\sum a_i e_i$$

where $\{e_i\}_{i\in T}$ forms a basis for N. Then elts. of $K \otimes_F N$ are finite sums

$$\sum a_i e_i$$

where $a_i \in K, i \in T$. (So $\{e_i\}$ forms a basis for $K \otimes_F N$ as a vector space over K.)

In general,

$$M \otimes_R (\bigoplus_{i\in T} N_i) \cong \bigoplus_{i\in T}(M \otimes_R N_i),$$

so

$$S \otimes_R (\bigoplus_{i\in T} R) \cong \bigoplus_{i\in T}(S \otimes_R R) \cong \bigoplus_{i\in T} S.$$

Thus if N is a free R-module with basis T then $S \otimes_R N$ forms a free S-module with basis T.

Theorem 2.4.8 (Steinitz Exchange Theorem)**.** *Let R be a commutative ring. Let B and T be bases for a free R-module N. Then* $\mathrm{Card}B = \mathrm{Card}T$.

Proof. If $g : R \mapsto S$ is any ring homomorphism then $S \otimes_R N$ is a free S-module with both B and T as bases. Letting $g : R \twoheadrightarrow R/M$ where M is a maximal ideal in R, we may reduce to the case where R is a field.

Case I: At least one of $\mathrm{Card}B, \mathrm{Card}T$ is finite. Say $\mathrm{Card}B \le \mathrm{Card}T$ and suppose $\mathrm{Card}B < \infty$. Write $B = \{b_1, \dots, b_n\}$. $\exists t_1 \in T$ s.t. when t_i is written in the basis B, the coeff. of b_1 is nonzero (or else $b_2, \dots, b_n$ would span N). Then $\{t_1, b_2, \dots, b_n\}$ forms a basis for N. Inductively, $\forall j = 1, \dots, n$, find t_j s.t. $\{t_1, \dots, t_j, b_{j+1}, \dots, b_n\}$ forms a basis for N. Then $\{t_1, \dots, t_n\}$ forms a basis for N, so

$$T = \{t_1, \dots, t_n\}$$

and $|T| = |B|$.

Case II: Both $\mathrm{Card}B$ and $\mathrm{Card}T$ are infinite. For each $b \in B$, set

$$T_b = \{\text{elts. of } T \text{ occuring in the expression for } b \text{ in basis } T\} \in 2^T.$$

Then T_b is finite $\forall b$. Define $f : B \mapsto 2^T$ by $f(b) = T_b$. If $X \subset T$ is finite with say $|X| = n$, at most n elts. of B lie in the span of X. So $|f^{-1}(X)| \le |X|$.

$$B = \bigcup_{\substack{X \subset T \\ X \text{ finite}}} f^{-1}(X) = \bigcup_{n=1}^{\infty} \bigcup_{\substack{X \subset T \\ |X| = n}} f^{-1}(X).$$

Since T is infinite, the cardinality of

$$\{X \subset T \mid |X| = n\}$$

is equal to the cardinality of $|T|$. Since $|f^{-1}(X)| \leq |X|$,

$$\begin{aligned}
\mathrm{Card} B &= \mathrm{Card} \bigcup_{n=1}^{\infty} \bigcup_{\substack{X \subset T \\ |X| = n}} f^{-1}(X) \\
&\leq \mathrm{Card}(\bigcup_{n=1}^{\infty} \mathrm{Card} T) \\
&= \mathrm{Card} T.
\end{aligned}$$

Similarly, $\mathrm{Card} T \leq \mathrm{Card} B$.

□

Note: Once we reduced to the case of a division ring, we no longer needed the commutativity of R, so the thm. also holds whenever R is a division ring, or indeed when R admits a homomorphism to a division ring. However, we used commutativity of R to produce our map $R \mapsto$ (division ring), since

$$R/2\text{-sided max. ideal}$$

need not be a division ring if R is not commutative.

If R is a commutative ring and N is a free R-module, the cardinality of any basis for N is called the **rank** of N. If R is a field then every R-module is free and its rank is called its **dimension**.

Proposition 2.4.9. *If $\phi : M \twoheadrightarrow N$ is a surjective R-module homomorphism and N is a free R-module then $\exists$ an R-module homomorphism $s : N \mapsto M$ s.t. $\phi s = 1_N$. In particular, $M \cong N \oplus \ker \phi$.*

Proof. Let S be a basis for N. For each $x \in S$, choose $m \in M$ s.t. $\phi(m) = x$ and set $s(x) = m$. Since N is free, this extends (uniquely) to an R-module map. □

An R-module P is called **projective** if given a surjective R-mod. homom. $\phi : M \mapsto P$, $\exists$ an R-mod. homom. $s : P \mapsto M$ s.t. $\phi s = 1_P$. Equivalently, P is surjective iff $\exists Q$ s.t. $P \oplus Q \cong R^N$ for some N. Equivalently, P is projective iff

$$\begin{tikzcd}
P \arrow[d, dashed, "\exists s"'] \arrow[dr, "\theta"] & & \\
M \arrow[r, two heads, "f"] & N \arrow[r] & 0
\end{tikzcd}$$

$\exists$ a lift s (not necessarily unique).
$\therefore$ Free $\Rightarrow$ Projective.

Example 2.4.10 (A projective module which is not free)**.** *Let $R = M_{n\times n}(F)$ ($n\times n$ matrices with entries in a field F), with $n > 1$. Let*

$$P = \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \cdots & 0 \end{pmatrix}$$

(matrices which are 0 beyond the first column). Then P forms a left ideal in R, ie. P is a left R-module.

Let

$$Q = \begin{pmatrix} 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

(matrices which are 0 in the first column). Then $P \oplus Q = R$, so P is projective. But P is not free, because if $P \cong R^s$ then, regarded as vector spaces over F, we would have

$$n = \dim P = \dim R^s = sn^2.$$

This is a contradiction since $n > 1$.

Definition 2.4.11. *Let R be an integral domain. An elt. x in an R-module M is called a **torsion element** if $\exists r \neq 0 \in R$ s.t. $rx = 0$. M is called a **torsion module** if x is a torsion elt. $\forall x \in M$. M is called **torsion-free** if it has no torsion elements.*

x, y torsion elts. $\Rightarrow x + y$ is a torsion elt. If x is a torsion elt. and $r \in R$ then rx is a torsion elt. Hence,

$$\mathrm{Tor}M := \{x \in M \mid x \text{ is a torsion elt.}\}$$

forms a submodule of M.

The **annihilator** of $x \in M$ is the left ideal

$$\mathrm{Ann}(x) := \{r \in R \mid rx = 0\}.$$

The **annihilator** of M is the 2-sided ideal

$$\mathrm{Ann}M := \{r \in R \mid rx = 0 \ \forall x \in M\}.$$

2.5 Localization and Field of Fractions

From the 4th isomorphism theorem we get:

Proposition 2.5.1. *A left ideal I is maximal if and only if the quotient module R/I is a simple (left) R-module.*

Note: It is important to remember that R/I (when I is a left ideal) is a quotient module and not (necessarily) a quotient ring.

Definition 2.5.2. *A ring with a unique maximal left ideal is called a* ***local ring****.*

While it appears initially that replacing "left ideal" by "right ideal" might give a different concept, as we shall see, "left local" equals "right local". That is, a ring has a unique maximal left ideal if and only if it has a unique maximal right ideal. Note however that while, as we shall see, a unique maximal left ideal must in fact be a 2-sided ideal, the existence of a unique maximal 2-sided ideal is not sufficient to guarantee that a ring be local. For example, when $n > 1$, $\{0\}$ forms a unique maximal ideal for matrix rings $M_{n\times n}(F)$ over a field F, but these rings are not local since they contain nontrivial left ideals, as we saw in the previous section.

Theorem 2.5.3. *Let R be a local ring with max. left ideal M. Then M is a 2-sided ideal.*

Proof. Suppose $y \in R$. Must show $My \subset M$. If $y \in M$ this is trivial since M is a left ideal, so assume $y \notin M$. Let $I_y := \{x \in R \mid xy \in M\}$. To finish the proof, we must show that $M \subset I_y$.

For $r \in R$ and $x \in I_y$, $(rx)y = r(xy) \in rM \subset M$, using that M is a left ideal. Therefore I_y is a left ideal. Note that $1 \notin I_y$, since $y \notin M$. Thus I_y is a proper left ideal so $I_y \subset M$. Let $\bar{y}$ denote the equivalence class of y in the quotient module R/M. Define $\phi : R \to R/M$ by $\phi(r) = r\bar{y}$. Then $\ker\phi = I_y$ by definition of I_y. Since M is maximal, R/M is a simple module, so $\mathrm{Im}\phi = R/M$. Therefore as left R-modules we have $R/I_y \cong \mathrm{Im}\phi = R/M$, which is simple and so I_y is a maximal left R-module. Thus $I_y = M$. □

Corollary 2.5.4. *Let R be a local ring with max. left ideal M. Then*

1. *$x \in R - M$ iff x is a unit.*
2. *R has a unique maximal right ideal.*
3. *The unique maximal right ideal of R is M.*
4. *R/M is a division ring.*

Conversely, if R is a ring with an ideal M s.t. x is a unit $\forall x \in R - M$ then R is a local ring.

Proof. Since no proper ideal can contain a unit, parts (2), (3), and (4) are immediate consequences of part (1).

Given $x \in R - M$, maximality of M shows that $Rx = R$ so $\exists\, y \in R$ such that $yx = 1$. Since M is a 2-sided ideal and $x \in R - M$ it follows that y cannot lie in M. Therefore the same argument applies to y and shows that $\exists\, z \in R$ such that $zy = 1$. But then $z = z(yx) = (zy)x = x$, so y forms a 2-sided inverse to x, establishing (1).

Conversely if every element of $R - M$ is a unit, then the fact that no proper ideal can contain a unit shows that R is a local ring. □

For the rest of this section, suppose that R is commutative.

A subset $S \subset R$ containing 1 and s.t. $0 \notin S$, which is closed under the multiplication of R is called a **multiplicative subset**. For example, let $\mathcal{P} \subset R$ be a prime ideal. Then $R - \mathcal{P}$ is a multiplicative subset. Form a ring called the **localization of** R w.r.t. S, denoted $S^{-1}R$. As a set,

$$S^{-1}R := R \times S / \sim,$$

where $(r, s) \sim (r', s')$ if $\exists t \in S$ s.t. $t(rs' - r's) = 0$. Think of (r, s) as $\frac{r}{s}$. Check $\sim$ is an equiv. reln.:

If $(r, s) \sim (r', s')$ and $(r', s') \sim (r'', s'')$ then

$$\begin{gathered} \exists t \in S \text{ s.t. } t(rs' - r's) = 0 \\ \text{and } \exists t' \in S \text{ s.t. } t'(r's'' - r''s') = 0 \end{gathered}$$

Then

$$s'tt'rs'' = tt'r'ss'' = tt'r''s's$$

ie. $s'tt'(rs'' - r''s) = 0$, (and $s'tt' \in S$) so $(r, s) \sim (r'', s'')$.

Define addition by $(r, s) + (r', s') = (rs' + r's, ss')$. Check $+$ is well-defined: suppose

$$(r', s') \sim (r'', s''), \quad \text{so } tr's'' = tr''s'.$$

Is $(rs' + r's, ss') \sim (rs'' + r''s, ss'')$?

Formally, $s^2tr's'' = s^2tr''s'$ so

$$t\left(ss''(rs' + r's) - ss'(rs'' + r''s\right) = t(s^2r's'' - s^2r''s) = 0.$$

Define $\cdot$ by $(r, s) \cdot (r', s') = (rr', ss')$ (easy to check $\cdot$ is well-defined). $(S^{-1}R, +, \cdot)$ becomes a commutative ring ring with identity $(1, 1)$.

Define the ring homomorphism

$$\begin{aligned} \psi : R &\mapsto S^{-1}R \\ r &\mapsto (r, 1) \end{aligned}$$

Note that $\psi(s)$ is a unit in $S^{-1}R$ $\forall s \in S$. ie. $(1,s)\psi(s) = (1,s)(s,1) = (s,s) \sim (1,1)$.

$\psi : R \mapsto S^{-1}R$ has the universal property: If $f : R \mapsto A$ is a ring homomorphism s.t. $f(s)$ is a unit in A $\forall s \in S$ then

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[dr, "f"'] & S^{-1}R \arrow[d, dashed, "\exists!"] \\ & A \end{tikzcd}$$

Proposition 2.5.5. *If R is an integral domain then $\psi : R \mapsto S^{-1}R$ is injective.*

Proof. Suppose $(r,1) = \psi(r) = 0 = (0,1)$. Then $t(r-0) = 0$ for some $t \in S$, so $r = 0$. $\square$

Note: if R is an integral domain, we can define the equiv. reln. simply by

$$(r,s) \sim (r',s') \text{ iff } rs' = r's$$

Special cases:

1. R an integral domain, $S = R - \{0\}$. Then $S^{-1}R$ is a field called the **field of fractions** of R.

2. $S = R - \mathcal{P}$ where $\mathcal{P}$ is a prime ideal. Then $\psi(\mathcal{P})$ forms an ideal in $S^{-1}R$ and every element of $S^{-1}R$ outside of $\psi(\mathcal{P})$ is invertible (quotient of images of elts. in S).

   $\therefore S^{-1}R$ is a local ring with max. ideal $\psi(\mathcal{P})$. $S^{-1}R$, also written $R_{\mathcal{P}}$, is called the **localization of** R **at the prime** $\mathcal{P}$.

3. $S = I - \{0\}$, where I is an ideal without 0-divisors. $S^{-1}R$ is sometimes called R with I inverted.

   e.g. $R = \mathbb{Z}$, $I = \mathbb{Z}p$. Then
$$S^{-1}R = \mathbb{Z}[\frac{1}{p}] = \{\frac{m}{p^t} \in \mathbb{Q}\}$$
   is "$\mathbb{Z}$ with p inverted" or "$\mathbb{Z}$ with $\frac{1}{p}$ adjoined". Sometimes called the localization of $\mathbb{Z}$ **away** from p.

2.6 Noetherian Rings and Modules

Definition 2.6.1. *An R-module M is called* ***Noetherian*** *if, given any increasing chain of submodules*

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$$

$\exists N$ s.t. $M_n = M_N$ $\forall n \geq N$. The ring R is called a ***Noetherian ring*** *if it is Noetherian when regarded as an R-module.*

If R is not commutative, notions of Noetherian, "right Noetherian", and "2-sided Noetherian" do not necessarily coincide.

Theorem 2.6.2. *Let R be a ring and let M be a left R-module. Then TFAE:*

1. *M is a Noetherian R-module.*
2. *Every non-empty set of submodules of M contains a maximal element.*
3. *Every submodule of M is finitely generated (and in particular, M is finitely generated).*

Proof.

$1 \Rightarrow 2$: Let Σ be a nonempty collection of submodules of M. Choose $M_1 \in \Sigma$. If M_1 is not maximal in Σ then $\exists M_2 \in \Sigma$ s.t. $M_1 \subsetneq M_2$. Having chosen $M_1, \ldots, M_{n-1}$, if M_{n-1} is not maximal in Σ then $\exists M_n \in \Sigma$ s.t.

$$M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n.$$

By hypothesis, no infinite chain of this sort exists, so eventually reach a max. elt.

$2 \Rightarrow 3$: Let N be a submodule of M. Let Σ be the collection of all finitely generated submodules of N. By the hypothesis, Σ contains a maximal element N'. If $N' \neq N$ then pick $x \in N - N'$. Then $\langle N', x\rangle$ is f.g. and properly contains N', which is a contradiction.

$\therefore N' = N$, so N is f.g.

$3 \Rightarrow 1$: Suppose every submod. of M is f.g. Let

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

be a chain of submodules. Let $N = \bigcup_{i=1}^{\infty} M_i$. Then $N \subset M$ is a submodule, so

$$N = \langle a_1, a_2, \ldots, a_n\rangle$$

for some finite set $a_1, \ldots, a_n \in N$.

Since $a_i \in N$, each $a_i \in M_k$ for some k. So $\exists K$ s.t. M_K contains all of $a_1, \dots, a_n$. But then $N \subset M_K$, so

$$M_K = M_{K+1} = \cdots = M_{K+m} = \cdots = N.$$

ie. $M_n = M_K \ \forall n \geq K$.

$\square$

Corollary 2.6.3. *Let $f : M \mapsto N$ be an R-module homomorphism. Then M is Noetherian iff* $\ker f$ *and* $\mathrm{Im} f$ *are Noetherian.*

Proof.

$\Rightarrow$: Suppose M is Noetherian. Every submodule of $\ker f$ is a submodule of M, and thus is f.g., so $\ker f$ is Noetherian.

If $A \subset \mathrm{Im} f$ then $f^{-1}(A)$ is a submodule of M, thus f.g. But then the images of the generators of $f^{-1}(A)$ generate A, so A is f.g.

$\Leftarrow$: Suppose $\ker f$ and $\mathrm{Im} f$ are f.g. Let $B \subset M$ be a submodule of M. Let

$$\Delta = f(B) \subset \mathrm{Im} f.$$

Pick a set $\overline{x_1}, \dots, \overline{x_k}$ of generators for Δ and let $x_1, \dots, x_k$ be pre-images in B.
Claim. $B = \langle \ker f \cap B, x_1, \dots, x_k \rangle$.

Proof. Given $b \in B$, $f(b) \in f(B)$ so

$$f(b) = \sum_{i=1}^{n} r_i \overline{x_i}, \quad \text{for some } r_1, \dots, r_k \in R.$$

Then $f(b - \sum_{i=1}^{n} r_i x_i) = 0$ so

$$b - \sum_{i=1}^{n} r_i x_i \in \ker f \cap B.$$

ie. $b \in \langle \ker f \cap B, x_1, \dots, x_k \rangle$.

But $\ker f \cap B \subset \ker f$ is f.g., so B is f.g.

$\square$

Corollary 2.6.4. *Let R be Noetherian. Then R/I is Noetherian.*

Proof. It follows from the preceding corollary that R/I is Noetherian when regarded as an R-module. However an increasing chain of R/I-submodules of R/I is also a increasing chain of R-submodules of R/I and so the corollary follows. $\square$

Theorem 2.6.5 (Hilbert Basis Theorem)**.** *Let R be a commutative Noetherian ring. Then $R[x]$ is Noetherian.*

Note: The converse is trivial, since $R \cong R[x]/R[x]x$.

Proof. Let $I \subset R[x]$ be an ideal. Let $L \subset R$ be the set of leading coefficients of elts. in I. That is,

$$L = \{a \in R \mid ax^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in I, \text{ for some } c_{n-1}, \ldots, c_0\}.$$

Then L is an ideal in R, so

$$L = (a_1, \ldots, a_n), \quad \text{for some } a_1, \ldots, a_n.$$

For each $i = 1, \ldots, n$, choose $f_i \in I$ s.t. leading coeff. of f_i is a_i. Let $N := \max\{N_1, \ldots, N_n\}$ where $N_i = \deg f_i$. For each $d = 0, \ldots, N-1$, let

$$L_d := \{0\} \cup \{\text{leading coefficients of elts. of } I \text{ of degree } d\}.$$

Then $L_d \subset R$ is an ideal, so

$$L_d = (b_1^{(d)}, \ldots, b_{n_d}^{(d)}), \quad \text{some } b_1^{(d)}, \ldots, b_{n_d}^{(d)} \in I.$$

Let $f_i^{(d)}$ be a polynomial of degree d with leading coeff. $b_i^{(d)}$. To finish the proof, it suffices to show:
Claim. I is generated by

$$\{f_1, \ldots, f_n\} \cup \bigcup_{d=0}^{N-1} \{f_i^{(d)}\}_{i=1,\ldots,n_d}.$$

Proof. Let I' be the ideal generated by this set. If $I' \subsetneq I$ then $\exists f \in I$ of minimal degree s.t. $f \notin I'$. Let $e = \deg f$ and let a be the leading coeff. of f.

Suppose $e \geq N$. $a \in L$ so

$$a = \sum_{i=1}^{n} r_i a_i, \quad \text{for some } r_1, \ldots, r_n \in R.$$

Then

$$\sum_{i=1}^{n} r_i x^{e-N_i} f_i \in I'$$

has degree e and leading coeff. a. So $f - \sum r_i x^{e-N_i} f_i \in I - I'$ has degree less than e, which is a contradiction.

$\therefore e < N$. Hence $a \in L_e$, so

$$a = \sum_{i=1}^{n_e} r_i b_i^{(e)}, \quad \text{for some } r_1, \ldots, r_{n_e} \in R.$$

Then $\sum r_i f_i^{(e)}$ has degree e and leading coeff. a, so $f - \sum r_i f_i^{(e)} \in I - I'$ and has degree less than e. This is a contradiction, so $I = I'$ and I is f.g. $\square$

2.7 Unique Factorization Domains

Note: For the remainder of this chapter, all the rings considered are integral domains, and in particular, are commutative.

$x \in R$ is called **irreducible** if $x \neq 0$, x is not a unit, and whenever $x = ab$, either a is a unit or b is a unit.

Proposition 2.7.1. *In an integral domain, prime $\Rightarrow$ irreducible.*

Proof. Let R be an integral domain. Let $p \in R$ be a prime and suppose $p = ab$. Then $p \mid a$ or $p \mid b$. Say $p \mid a$, so $a = zp$ for some $z \in R$. Thus $p = ab = zpb$ so $1 = zb$.
$\therefore$ b is a unit. Similarly, if $p \mid b$ then a is a unit. Hence p is irreducible. $\square$

Example 2.7.2. *Let*

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 + 5).$$

Claim. *2 is irreducible but not prime in R. To see 2 is irreducible, consider $N : R \mapsto \mathbb{Z}$ given by*

$$N(a + b\sqrt{-5}) = |a + b\sqrt{-5}|^2 = a^2 + 5b^2,$$

(the "norm" map). N is not a ring homorphism but $N(yz) = N(y)N(z)$.
$\therefore$ If $2 = \alpha\beta$ then $4 = N(\alpha)N(\beta)$, so $N(\alpha) \leq 4$ and $N(\beta) \leq 4$. The only elements with norm ≤ 4 are $1, -1, 2, -2$, so

$$\alpha, \beta \in \{1, -1, 2, -2\}.$$

Since $\alpha\beta = 2$, either $\alpha = \pm 1$ or $\beta = \pm 1$, so 2 is irreducible.

However, in $R/(2)$,

$$(1 + \sqrt{5})^2 = 6 + 2\sqrt{5} \equiv 0$$

so $R/(2)$ has zero divisors.
$\therefore$ $R/(2)$ is not an integral domain, so 2 is not prime. What are the primes in R?

Consider first $y \in \mathbb{Z}^+ \subset R$. If y is not prime in $\mathbb{Z}$ then y is reducible so it is not prime in R. We already saw that 2 is not prime in R and since $5 = (-\sqrt{-5})(\sqrt{-5})$ is reducible, 5 is not prime in R. Therefore suppose y is a prime $p \in \mathbb{Z}^+$ with $p \neq 2$ or 5. $R/(y)$ fails to be an integral domain iff $\exists$ nonzero $s = a + b\sqrt{-5}$ and $t = c + d\sqrt{-5}$ such that

$$st = (ac - 5bd) + (ad + bc)\sqrt{-5}$$

is zero in $R/(y) = (\mathbb{Z}/p)[\sqrt{-5}]$. That is, $ac = 5bd$ and $ad = -bc$ in $\mathbb{Z}/p$. None of a, b, c, d can be 0 in $\mathbb{Z}/p$ since otherwise these equations would imply either $s = 0$ or $= 0$ in $R/(y)$. But then the equations yield

$$\frac{a^2}{b^2} = \frac{c^2}{d^2} = -5,$$

so if $R(y)$ fails to be an integral doman than -5 is a square modulo p.

Conversely, if $\exists\, z$ such that $z^2 \cong -5 \pmod p$, then

$$(z+\sqrt{-5})(z-\sqrt{-5}) = z^2+5 = 0$$

in $R/(y)$ so $R/(y)$ is not an integral domain. Thus $y \in \mathbb{Z}$ is a prime in R iff $|y|$ is a prime $p \neq 5$ in $\mathbb{Z}$ such that -5 is not a square modulo p.

Now consider $y = a + b\sqrt{-5}$ with $b \neq 0$.

$$a^2+5b^2 = (a-b\sqrt{-5})y \in (y)$$

so $R \mapsto\!\!\!\!\twoheadrightarrow R/(a^2+5b^2) \xrightarrow{q} R/(y)$. q is not injective since $y \notin (a^2+5b^2)$.

If a^2+5b^2 is not a prime in $\mathbb{Z}$ then we can see that y is not prime in R as follows. Suppose that $a^2+5b^2 = cd$ $(c, d \neq \pm 1)$ and suppose that y is prime in R. Then $y \mid cd$ so either $y \mid c$ or $y \mid d$. Say $y \mid c$. Write $c = \lambda y$ for some $\lambda \in R$. λ is not a unit since application of the norm map shows that the only units in R are ± 1, and $c \neq \pm y$ because $c \in \mathbb{Z}$, $y \notin \mathbb{Z}$. Letting $\bar{x}$ denote the complex conjugate of x, we have

$$y\bar{y} = N(y) = cd = \lambda y d$$

so $\bar{y} = \lambda d$. Thus $y = \bar{\lambda}\bar{d}$ and since $\bar{\lambda}$ and $\bar{d} = d$ are not units, this shows that y is reducible and therefore not prime.

If a^2+5b^2 is a prime p in $\mathbb{Z}$ then

$$x^2+5 \equiv 0 \mod p$$

has a solution $x = a/b$, so -5 is a square mod p. Set $c := a/b \in \mathbb{Z}/p$.

Define $\phi : R/(y) \mapsto \mathbb{Z}/p \cong \mathbb{F}_p$ by $\phi(\sqrt{-5}) = c$ and extending linearly. Then

$$\phi(y) = a + bc \equiv 0 \mod p$$

so ϕ is well-defined. $\left|R/(a^2+5b^2)\right| = p^2$ and q is not injective so $|R/(y)| = p$ and ϕ is an isomorphism. $\therefore\ y = a + b\sqrt{-5}$ is prime in R whenever a^2+5b^2 is prime in $\mathbb{Z}$.

Remark 2.7.3. *The question of which primes p have the property that -5 is a square modulo p can be solved with the aid of Gauss' Law of Quadratic Reciprocity, which says that for odd primes p and q,*

$$\left(\begin{matrix} p \\ - \\ q \end{matrix}\right)\left(\begin{matrix} q \\ - \\ p \end{matrix}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

where $\begin{pmatrix} p \\ - \\ q \end{pmatrix}$ *is the Legendre symbol, defined by*

$$\begin{pmatrix} x \\ - \\ p \end{pmatrix} = \begin{cases} 1 & \text{if } x \text{ is a square modulo } p; \\ -1 & \text{if } x \text{ is a not square modulo } p. \end{cases}$$

Therefore

$$\begin{pmatrix} -5 \\ - \\ p \end{pmatrix} = \begin{pmatrix} -1 \\ - \\ p \end{pmatrix}\begin{pmatrix} 5 \\ - \\ p \end{pmatrix} = \begin{pmatrix} -1 \\ - \\ p \end{pmatrix}(-1)^{4(\frac{p-1}{2})}\begin{pmatrix} p \\ - \\ 5 \end{pmatrix} = \begin{pmatrix} -1 \\ - \\ p \end{pmatrix}\begin{pmatrix} p \\ - \\ 5 \end{pmatrix}.$$

Since $\begin{pmatrix} -1 \\ - \\ p \end{pmatrix} = \begin{cases} 1 & p \cong 1 \mod 4; \\ -1 & p \cong 3 \mod 4, \end{cases}$ *and* $\begin{pmatrix} p \\ - \\ 5 \end{pmatrix} = \begin{cases} 1 & p \cong 1 \text{ or } 4 \mod 5; \\ -1 & p \cong 2 \text{ or } 3 \mod 5, \end{cases}$*, we get* $\begin{pmatrix} -5 \\ - \\ p \end{pmatrix} = 1$ *iff one of the following* 4 *pairs of congruences holds:*

$$\begin{matrix} p \cong 1 \mod 4 \\ p \cong 1 \mod 5 \end{matrix} \quad \text{or} \quad \begin{matrix} p \cong 1 \mod 4 \\ p \cong 4 \mod 5 \end{matrix} \quad \text{or} \quad \begin{matrix} p \cong 3 \mod 4 \\ p \cong 2 \mod 5 \end{matrix} \quad \text{or} \quad \begin{matrix} p \cong 3 \mod 4 \\ p \cong 3 \mod 5. \end{matrix}$$

By the Chinese Remainder Theorem, this is equivalent to saying that -5 *is a square modulo the prime* p *iff* $p \cong 1, 3, 7,$ *or* $9 \mod (20)$.

Definition 2.7.4. *An integral domain R is called a* ***unique factorization domain*** *(UFD) if every nonzero element can be factored into primes.*

Lemma 2.7.5. *In an integral domain, a factorization into primes (should one exist) is always unique up to associates. ie. If* $x = p_1 \cdots p_n$ *and* $x = q_1 \cdots q_k$ *then* $k = n$ *and* $\exists$ *some renumbering* σ *of the q's such that* p_j *and* $q_{\sigma(j)}$ *are associate primes* $\forall j$.

Proof. Suppose

$$p_1 \cdots p_n = q_1 \cdots q_k$$

and say $n \leq k$. Then $p_1 \mid q_1 \cdots q_k$ so $p_1 \mid q_j$ for some j. Renumber so that q_j is q_1.
$\therefore q_1 = ap_1$ for some a. But q_1 is a prime and thus irreducible, so either a or p_1 is a unit. Since p_1 is prime, it is not a unit, so a is a unit. ie. p_1 and q_1 are associates.
$\therefore p_1 \cdots p_n = q_1 \cdots q_k = ap_1q_2 \cdots q_k$,
$\therefore p_2 \cdots p_n = q_2'q_3 \cdots q_k$ where $q_2' = aq_2$ is associate to q_2. Continuing, $\forall i = 1, \ldots, n$, after renumbering q_j associate to p_i, eventually reach

$$1 = q_{n+1}' \cdots q_k$$

where q_{n+1}' is associate to q_{n+1}. If $k > n$ this is a contradiction since prime q_{n+1} is not invertible. Hence $k = n$. ◻

Proposition 2.7.6. *In a UFD, prime $\iff$ irreducible.*

Proof. Prime $\Rightarrow$ irreducible in any integral domain, so must show irreducible $\Rightarrow$ prime. Let $x \in R$ be irreducible. Write $x = p_1 \cdots p_n$ be a product of primes and suppose $n > 1$. Since x is irreducible, p_1 is a unit or $p_2 \cdots p_n$ is a unit. But p_1 is not a unit since p_1 is prime and $p_2 \cdots p_n$ is not a unit since $p_2, \dots, p_n$ are primes. So this is a contradiction and thus $n = 1$ and $x = p_1$ is prime. □

Theorem 2.7.7. *An integral domain is a UFD iff every nonzero elt. can be factored uniquely (up to associates) into irreducibles.*

Proof.

$\Rightarrow$: Suppose R is a UFD. Then prime $\iff$ irreducible and every nonzero elt. has a unique factorization into primes.

$\Leftarrow$: Suppose every nonzero elt. has a unique factorization (up to associates) into irreducibles. It suffices to show that x is prime iff x is irreducible. ie. Show irreducible $\Rightarrow$ prime.

Let $x \neq 0$ be irreducible. Suppose $x \mid ab$. Then $ab = zx$ for some z. Let

$$a = a_1 \cdots a_n \quad \text{and} \quad b = b_1 \cdots b_k$$

be the factorizations of a, b into irreducibles. So

$$zx = a_1 \cdots a_n b_1 \cdots b_k$$

is the factorization of zx into irreducibles, so by uniqueness, x is associate to some factor on the RHS.

$\therefore$ x is assoc. to a_j for some j, in which case $x \mid a$, or x is assoc. to b_j for some j, in which case $x \mid b$. Thus x is prime.

□

Proposition 2.7.8. *In a UFD, every pair of elts. has a g.c.d.*

Proof. Let R be a UFD and suppose $x \neq 0, y \neq 0 \in R$. Factor x into primes and, replacing primes by associate ones when necessary, write

$$x = up_1^{r_1} \cdots p_n^{r_n}$$

where u is a unit and $p_1, \dots, p_n$ are primes with p_i not associate to p_j for $i \neq j$. Similarly, write

$$y = vq_1^{s_1} \cdots q_k^{s_k}$$

where, replacing by associate if necessary, we may assume that if q_j is associate to p_i for some i then $q_j = p_i$. Letting $z_1, \ldots, z_m$ be the union $\{p_1, \ldots, p_n, q_1, \ldots, q_k\}$ of all primes occurring, we can write

$$x = uz_1^{e_1} \cdots z_m^{e_m} \quad \text{and} \quad y = vz_1^{f_1} \cdots z_m^{f_m}$$

for some exponents $e_1, \ldots, e_m, f_1, \ldots, f_m \geq 0$. Let

$$d = \prod z_j^{\min\{e_j, f_j\}}.$$

Then $d = (x, y)$. $\square$

2.8 Principal Ideal Domains

Definition 2.8.1. *A* ***principal ideal domain*** *(PID) is an integral domain in which every ideal is principal.*

Proposition 2.8.2. *In a PID, every nonzero prime ideal is maximal.*

Proof. Let $I \neq 0$ be a prime ideal. Suppose $I \subsetneq J \subsetneq R$. Write $I = (x), J = (y)$. Since I is a prime ideal, x is prime. Since $I \subset J$, $x \in J$ so $x = ay$ for some $a \in R$. Thus $x \mid a$ or $x \mid y$.

If $x \mid a$ then $a = bx$ for some $b \in R$. Then $x = ay = abxy \Rightarrow 1 = by$, so y is a unit and $J = R$.

If $x \mid y$ then $y \in (x) = I$, so $J \subset I$, contradiction $I \subsetneq J$. Hence I is maximal. □

Example 2.8.3. *Let* $R = \mathbb{Z}[x]$. $R/(x) \cong \mathbb{Z}$ *is an integral domain but not a field. So* (x) *is a prime ideal which is not maximal.*
$\therefore \mathbb{Z}[x]$ *is not a PID. In fact,* $I = (2, x)$ *is an example of a non-principal ideal in* R.

Theorem 2.8.4. *Every PID is Noetherian*

Proof. Every ideal in R is generated by a single element, so in particular, every ideal is finitely generated. By Theorem 2.6.2, this means that R is Noetherian. □

Theorem 2.8.5. *Every PID is a unique factorization domain.*

Proof. Let R be a PID and let $x \neq 0 \in R$ be a non-unit. Must show that x can be factored into primes. $(x) \subsetneq R$ so $\exists$ a maximal ideal M_1 s.t.
$$(x) \subset M_1 \subsetneq R.$$
Write $M_1 = (p_1)$. M_1 is maximal and thus prime, so p_1 is prime. $x \in (p_1)$ says $x = p_1 x_1$ for some $x_1 \in R$. If x_1 is a unit then $p_1 x_1$ is a prime associate to p_1 and we are done, so suppose not. Continuing, we get
$$x_n = p_n x_{n+1} \quad \forall n.$$
$\therefore x_n \in (x_{n+1})$ so $(x_n) \subset (x_{n+1})$. If x_n is a unit for some n then we have a factorization of x into primes. If not, we get a chain of ideals
$$(x) \subset (x_1) \subset \cdots \subset (x_n) \subset \cdots$$
Since R is Noetherian, $\exists N$ s.t. $(x_n) = (x_N)\ \forall n \geq N$. So $x_{N+1} \in (x_N)$ so $x_{N+1} = \lambda x_N = \lambda p_{N+1} x_{N+1}$ so that $1 = \lambda p_{N+1}$ showing that p_{N+1} is a unit, which is a contradiction.

So the infinite chain does not exist, so the procedure terminated giving a factorization of x. □

Proposition 2.8.6. *Let R be a PID. Let $a, b \in R$ and let $q = \gcd(a, b)$. Then $\exists s, t \in R$ s.t. $q = sa + tb$.*

Proof. Let $I = \langle a, b\rangle = \{xa + yb \mid x, y \in R\}$. Then I is an ideal so $I = (c)$ for some $c \in R$. $c \in I$ so $c = xa + yb$ for some x, y. $a \in I$ so $c \mid a$ and $b \in I$ so $c \mid b$. Moreover, if $z \mid a$ and $z \mid b$ then let $a = \alpha z$ and $b = \beta z$ for some α, β. Then

$$c = xa + yb = x\alpha z + y\beta z = (x\alpha + y\beta)z$$

and thus $z \mid c$. So $c = \gcd(a, b)$.

If q is another g.c.d. of a, b then $q = uc$ for some unit u, so

$$q = (ux)a + (uy)b.$$

□

2.9 Norms and Euclidean Domains

Definition 2.9.1. *A **Euclidean domain** is an integral domain R together with a function $d : R - \{0\} \mapsto \mathbb{Z}^+ = \{n \in \mathbb{Z} \mid n \geq 0\}$ s.t.*

1. *$d(a) \leq d(ab)$ $\forall a, b \neq 0$, and*

2. *Given $a, b \neq 0 \in R$, $\exists t, r$ s.t. $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.*

Example 2.9.2.
1. *$R = \mathbb{Z}$, $d(n) = |n|$.*

2. *$R = F[x]$ where F is a field. $d(p(x))$ = polynomial degree of p.*

Notice that if (R, d) is a Euclidean domain then so is (R, d') where

$$d'(x) = d(x) + c, \quad \text{for some constant } c \in \mathbb{Z}^+.$$

$\therefore$ May assume that d takes values in $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 1\}$. Then extend d by defining $d(0) = 0$.

Definition 2.9.3. *A **Dedekind-Hasse norm** on an integral domain R is a function $N : R \mapsto \mathbb{Z}^+$ s.t.*

1. *$N(x) = 0$ iff $x = 0$, and*

2. *For $a, b \neq 0 \in R$ either $a \in (b)$ or $\exists$ a nonzero $x \in (a, b)$ s.t. $N(x) < N(b)$.*

If (R, d) is a Euclidean domain then d (modified s.t. $d(0) = 0$) is a Dedekind-Hasse norm: given $a, b \neq 0$,

$$a = tb + r$$

for some t and r, so either $b \mid a$ (ie. $r = 0$) or $r = a - tb \in (a, b)$ with $d(r) < d(b)$.

Theorem 2.9.4. *Let R be an integral domain.*

1. *R is a PID iff R has a Dedekind-Hasse norm. In particular, a Euclidean domain is a PID.*

2. *If R has a Dedekind-Hasse norm then it is has a multiplicative Dedekind-Hasse norm (ie. one satisfying $N(ab) = N(a)N(b)$.)*

Proof.
1. $\Rightarrow$: Suppose R has a Dedekind-Hasse norm. Let $I \subset R$ be a nonzero ideal. Choose $0 \neq b \in I$ s.t. $N(b)$ is minimum. Let $a \in I$. Then $(a, b) \subset I$ so $\nexists$ nonzero $x \in (a, b)$ s.t. $N(x) < N(b)$. Hence $a \in (b)$. Thus $I = (b)$.

$\Leftarrow$: Suppose R is a PID. Define $N : R \mapsto \mathbb{Z}^+$ as follows: $N(0) := 0$. If $u \in R$ is a unit, set $N(u) = 1$. If $x \neq 0 \in R$ is a nonunit, write $x = p_1 \cdots p_n$ where each p_j is prime and set $N(x) = 2^n$. Notice that N is multiplicative.

Suppose $a, b \neq 0 \in R$. R is a PID so $(a, b) = (r)$ for some $r \in R$, so $b = xr$ for some $x \in R$. If $a \notin (b)$ then $r \notin (b)$ so x is not a unit, and thus

$$N(b) = N(x)N(r) > N(r),$$

ie. $\exists r \in (a, b)$ s.t. $N(r) < N(b)$.

2. If R has a Dedekind-Hasse norm then by part 1, it is a PID, in which case it has a multiplicative Dedekind-Hasse norm as constructed above.

□

2.9.1 Euclidean Algorithm

Let (R, d) be a Euclidean domain. Then R is a PID, so given $a, b \in R$, $\exists s, t \in R$ s.t.

$$as + bt = \gcd(a, b).$$

The Euclidean algorithm is an algorithm for finding s and t (and thus $\gcd(a, b)$).
Procedure:
Say $d(b) \geq d(a)$. Set $r_{-1} := b$, $r_0 := a$. Write

$$\begin{aligned} r_{-1} &= q_1 r_0 + r_1, \quad \text{some } q_1, r_1 \text{ with } d(r_1) < d(r_0), \\ &\vdots \\ r_{j-1} &= q_{j+1} r_j + r_{j+1}, \quad \text{some } q_{j+1}, r_{j+1} \text{ with } d(r_{j+1}) < d(r_j) \end{aligned}$$

$\therefore d(r_{-1}) \geq d(r_0) > d(r_1) > \cdots > d(r_j) > \cdots$. Continue until $r_{k+1} = 0$, some k. Set

$$\begin{aligned} s_0 &:= 0 \\ s_1 &:= 1 \\ s_j &:= -q_{j-1} s_{j-1} + s_{j-2} \\ t_0 &:= 1 \\ t_1 &:= 0 \\ t_j &:= -q_{j-1} t_{j-1} + t_{j-2} \end{aligned}$$

Claim. $r_k = \gcd(a, b)$ and $r_k = sa + tb$ where $s = s_{k+1}$ and $t = t_{k+1}$.

Proof. $r_{k+1} = 0$ so $r_{k-1} = q_{k+1}r_k + 0$. Suppose by induction that $r_k \mid r_i$ for $i \geq j$. Then $r_{j-1} = q_{j+1}r_j + r_{j+1}$ so $r_k \mid r_{j-1}$, concluding induction step.
$\therefore r_k \mid r_j \; \forall j$ and in particular, $r_k \mid r_0 = a$ and $r_k \mid r_{-1} = b$.

Conversely, suppose z divides both a and b. Since $r_{j+1} = r_{j-1} - q_{j+1}r_j$, induction (going the other way) shows $z \mid r_j \; \forall j$. In particular, $z \mid r_k$. So $r_k = \gcd(a,b)$. $\square$

Also,

$$\begin{aligned}
as_0 + bt_0 &= a \cdot 0 + b \cdot 1 = b = r_{-1} \\
as_1 + bt_1 &= a \cdot a + b \cdot 0 = a = r_0 \\
as_2 + bt_2 &= a(-q_1 s_1 + s_0) + b(-q_1 t_1 + t_0) = -q_1(as_1 + bt_1) + (as_0 + bt_0) \\
&= -q_1 r_0 + r_{-1} = r_1 \\
&\vdots \\
as_j + bt_j &= a(-q_{j-1}s_{j-1} + s_{j-2}) + b(-q_{j-1}t_{j-1} + t_{j-2}) = -q_{j-1}(as_{j-1} + bt_{j-1}) + (as_{j-2} + bt_{j-2}) \\
&= -q_{j-1}r_{j-2} + r_{j-3} = r_{j-1}
\end{aligned}$$

By induction, $as_j + bt_j = r_{j-1} \; \forall j$. In particular, $as + bt = as_{k+1} + bt_{k+1} = r_k = \gcd(a,b)$.

Remark: In Computer Science, the speed of the Euclidean Algorithm over $\mathbb{Z}$ is important. Estimate of the number of steps required: The faster the r's go down, the quicker the algorithm goes, so the worst case scenario is when all the q's are only 1. In this case,

$$r_{j-1} = r_j + r_{j+1}.$$

ie. Worst case scenario occurs when a, b are consecutive terms of the Fibonacci Sequence. The smallest possible numbers requiring N steps would be when:

$$r_N = 1 \quad r_{N-1} = 2 \quad r_{N-2} = 3 \quad r_{N-3} = 4 \cdots r_{N-j} = j^{\text{th}} \text{ Fibonacci Number}$$

$\therefore r_0 = N^{\text{th}}$ Fibonacci Number F_N. ie. N steps can handle all numbers up to F_N.

$F_{n+1} = F_n + F_{n-1} \Rightarrow \frac{F_{n+1}}{F_n} = 1 + \frac{F_{n-1}}{F_n}$. So if $L = \lim_{n\to\infty} \frac{F_{n+1}}{F_n}$ then $L = 1 + \frac{1}{L}$. So

$$\begin{aligned}
L^2 - L - 1 &= 0 \\
L &= \frac{1 \pm \sqrt{5}}{2} \\
L &= \frac{1 + \sqrt{5}}{2} = G
\end{aligned}$$

So $F_n \approx G^N$, ie. for large N, the number of steps required is no worse than around $\log_G(r_0)$.

Lemma 2.9.5 (Gauss)**.** *Let R be a UFD and let F be its field of fractions. Let $q(x) \in R[x]$. If $q(x)$ is reducible in $F[x]$ then $q(x)$ is reducible in $R[x]$. Futhermore, if $q(x) = A(x)B(x)$ in $F[x]$ then in $R[x]$, $q(x) = a(x)b(x)$ where $A(x) = \frac{a(x)}{r}$ and $B(x) = \frac{b(x)}{s}$ for some nonzero $r, s \in F$.*

Proof. Suppose $q(x) = A(x)B(x)$ where the coefficients of A, B lie in F. Multiplying by a common denominator we get

$$dq(x) = a'(x)b'(x)$$

for some $d \in R$ and polynomials $a'(x), b'(x) \in R[x]$. If $d \in R$ is a unit, we can divide by d to get $q(x) = \frac{a'(x)}{d}b'(x)$.
$\therefore$ Suppose d is not a unit. Write $d = p_1 \cdots p_n$ as a product of primes in R. Let

$$\begin{aligned} R[x] &\twoheadrightarrow \frac{R[x]}{p_1R[x]} \cong (\frac{R}{p_1R})[x] \\ f(x) &\mapsto \overline{f(x)} \end{aligned}$$

Reducing modulo $(p_1R)[x]$ gives $0 = \overline{a'(x)}\,\overline{b'(x)}$ in the integral domain $(\frac{R}{p_1R})[x]$. Hence $\overline{a'(x)} = 0$ or $\overline{b'(x)} = 0$. Say $\overline{a'(x)} = 0$. Then all the coeffs. of $a'(x)$ are divisible by p_1, so can divide $dq(x) = a'(x)b'(x)$ by p_1 to get

$$p_2 \cdots p_n g(x) = \frac{a'(x)}{p_1}b'(x) = a''(x)b'(x)$$

with $a'', b' \in R[x]$. Continuing, eventually reach $q(x) = a(x)b(x)$ with $a(x), b(x) \in R[x]$ and $a(x), b(x)$ obtained from $a'(x), b'(x)$ by multiplying by nonzero elements of F. $\square$

A polynomial whose leading coefficient is 1 is called **monic**.

Corollary 2.9.6. *Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$. Suppose*

$$gcd\{coeffs.\ of\ p\} = 1.$$

Then $p(x)$ is irreducible in $R[x]$ iff it is irreducible in $F[x]$. In particular, if $p(x)$ is monic and irreducible in $F[x]$ then it is irreducible in $R[x]$.

Proof. If $p(x)$ is reducible in $F[x]$ then Gauss implies $p(x)$ is reducible in $R[x]$.

Conversely, if $p(x)$ is reducible in $R[x]$ then the hypothesis on gcd $\Rightarrow$ $p(x) = a(x)b(x)$ where neither $a(x)$ nor $b(x)$ is constant. Hence, $a(x), b(x)$ are not units in $F[x]$ so this factorization shows $p(x)$ is reducible in $F[x]$. $\square$

Lemma 2.9.7. *Let R be a UFD and let $p(x) \in R[x]$ be irreducible. Then $p(x)$ is prime.*

Proof. Let F be the field of fractions of R.

$$\frac{R[x]}{(p(x))} \hookrightarrow \frac{F[x]}{(p(x))}.$$

$\therefore$ To show $p(x)$ $R[x]/(p(x))$ is an integral domain, it suffices to show that $F[x]/(p(x))$ is an integral domain.

$p(x)$ irreducible in $R[x] \Rightarrow p(x)$ irreducible in $F[x]$. However, $F[x]$ is a UFD (being a Euclidean Domain). So $p(x)$ is prime in $F[x]$ and thus $F[x]/(p(x))$ is an integral domain. □

Theorem 2.9.8. *R is a UFD $\iff R[x]$ is a UFD.*

Proof.

$\Leftarrow$: Suppose $R[x]$ is a UFD. Let $r \in R$. Write $r = p_1(x) \cdots p_n(x)$ as a product of primes in $R[x]$. Since $\deg r = 0$ and R is an integral domain, $\deg p_j(x) = 0\ \forall j$, ie. $p_j(x) = p_j \in R$.

$$R[x]/(p_j) = \left(\frac{R}{(p_j)}\right)[x]$$

$\therefore R/(p_j)$ is an integral domain, so p_j is prime in R.

Thus $r = p_1 \cdots p_n$ is a factorization of r into primes in R.

$\Rightarrow$: Suppose R is a UFD and let $0 \neq q(x) \in R[x]$. Let F be the field of fractions of R. Since $F[x]$ is a UFD, in $F[x]$ we can factor $q(x)$

$$q(x) = p_1(x) \cdots p_r(x)$$

where $p_j(x)$ is a prime in $F[x]$. By Gauss' lemma, in $R[x]$ we can write

$$q(x) = p_1'(x) \cdots p_n'(x)$$

where $\forall j \exists s_j \neq 0 \in F$ such that $p_j'(x) = s_j p_j(x)$.

$\therefore$ It suffices to show that $p_j'(x)$ can be factored uniquely into primes in $R[x]$, as in the following claim:

Claim. If $p(x)$ is prime in $F[x]$ and $sp(x) = p'(x) \in R[x]$ for some $0 \neq s \in F$ then $p'(x)$ can be factored uniquely into primes in $R[x]$.

Proof. Let

$$d = \gcd\{\text{coeffs. of } p'(x)\}.$$

Then $p'(x) = dp''(x)$ where

$$\gcd\{\text{coeffs. of } p''(x)\} = 1.$$

In $F[x]$, have $p''(x) = \frac{p'(x)}{d} = \frac{s}{d}p(x)$, which is prime in $F[x]$ since $p(x)$ is prime and $\frac{s}{d}$ is a unit. $\therefore$ Cor. 2.9.6$\Rightarrow$ $p''(x)$ is irreducible in $R[x]$ and thus prime in $R[x]$ by the previous lemma. Since d can be factored into primes in R and a prime in R is also a prime in $R[x]$, $p'(x) = dp''(x)$ can be factored into primes in $R[x]$.Uniqueness is easy to show. This concludes the proof of the claim and thus concludes the proof of the theorem.

$\square$

2.10 Modules over PID's

Note: In this section, and elsewhere, we will sometimes abuse notation and write R/p in place of $R/(p)$. (The notation $\mathbb{Z}/n$ is generally quite common).

Theorem 2.10.1. *Over a PID, a submodule of a free module is free.*

Proof. Let R be a PID. Let $P = \bigoplus_{j \in J} R_j$ be a free R-module with basis J ($R_j \cong R\ \forall j$), and suppose $M \subset P$ is a submodule.

Choose a well-ordering of the set J. For each $j \in J$, set $P_j = \bigoplus_{i \leq j} R_i$ and $\overline{P}_j = \bigoplus_{i<j} R_i$, so $P_j = \overline{P}_j \oplus R$.

Let f_j be the composite

$$P_j \cap M \hookrightarrow P_j = \overline{P}_j \oplus R \mapsto\!\!\!\rightarrow R.$$

Then $\ker f_j = \overline{P}_j \cap M$. $\mathrm{Im} f_j \subset R$ is an ideal, so let $\mathrm{Im} f_j = (\lambda_j)$, some $\lambda_j \in R$. Pick $c_j \in P_j \cap M$ such that $f(c_j) = \lambda_j$. Let

$$J' = \{j \in J \mid \lambda_j \neq 0\}.$$

To finish the proof we show:
Claim: $\{c_j\}_{j \in J'}$ is a basis for M.
Proof. Check $\{c_j\}_{j \in J'}$ is linearly independent:
Suppose

$$\sum_{k=1}^{n} a_k c_{j_k} = 0, \quad \text{where } j_1 < j_2 < \cdots < j_n \tag{$*$}$$

Since $j_k < j_n$ for $k < n$, $c_{j_k} \in \overline{P}_{j_n}$ for $k < n$.

$\therefore$ Applying f_{j_n} to $(*)$ gives

$$\sum_{k=1}^{n} a_k \cdot 0 + a_n \lambda_{j_n} = 0,$$

whence $a_n = 0$, since $\lambda_{j_k} \neq 0$. Inductively, $c_{j_k} = 0\ \forall k = n, n-1, \ldots, 1$.

$\therefore$ $\{c_{j_k}\}_{j \in J'}$ is linearly independent.
Check that $\{c_j\}_{j \in J'}$ spans M:
Suppose not. Then $\exists$ a least $i \in J$ such that $P_i \cap M$ contains an element a not in $\mathrm{span}\{c_j\}_{j \in J'}$. Must have $i \in J'$, since if not, $f_i(a) = 0$, so $a \in \overline{P}_i$, and thus $a \in P_k$ for some $k < i$, contradicting minimality of i.

$\therefore$ $i \in J'$. $f_i(a) \in (\lambda_i)$, so $f_i a = r\lambda_i$, for some $r \in R$. Set $b := a - rc_i$. Since $a = b + rc_i$ cannot be written as a linear combination of $\{c_i\}$, neither can b. But

$$f_i b = f(a) - rf(c_i) = r\lambda_i - r\lambda_i = 0$$

so $b \in P_k \cap M$ for some $k < i$, contradicting the minimality of i.

$\therefore \{c_j\}_{j \in J'}$ spans M. $\square$

Theorem 2.10.2. *Over a PID, a finitely generated torsion-free module is free.*

Proof. Let R be a PID and let M be a finitely generated torsion-free R-module. Let $R \hookrightarrow K$ be the inclusion of R into its field of fractions, and let

$$\tilde{M} := K \otimes_R M$$

be the extension of M to a K-vector space.

Let $x_1, \ldots, x_m \in M$ be a generating set for M. The images of $x_1, \ldots, x_m$ generate $\tilde{M}$, so $\exists$ a subset $y_1 \ldots, y_n$ whose images in $\tilde{M}$ form a basis for $\tilde{M}$. Each x_j can be written in $\tilde{M}$ as a K-linear combination of $y_1, \ldots, y_n$, so clearing denominators gives that $b_j x_j$ is an R-linear combination of $y_1, \ldots, y_n$ $\forall j$.

Set $b = b_1 \cdots b_m$, so that bx_j is an R-linear combination of $y_1, \ldots, y_n$ $\forall j$.

$\therefore bz$ is an R-linear combination of $y_1, \ldots y_n$ $\forall z \in M$, since $x_1, \ldots, x_m$ span M. Since M is torsion-free,

$$\begin{aligned} b : M &\mapsto M \\ z &\mapsto bz \end{aligned}$$

is injective. Hence,

$$M \cong M/\ker\phi \cong \mathrm{Im} b = bM.$$

However,

$$\begin{aligned} \bigoplus_{j=1}^{n} y_j &\overset{\phi}{\longmapsto} bM \\ y_j &\mapsto y_j \end{aligned}$$

is an isomorphism (onto since bz is a linear combination of $y_1, \ldots, y_n$ $\forall z \in M$, (1-1) since $y_1, \ldots y_n$ are linearly independent in $\tilde{M}$).

$\therefore M \cong bM \cong$ a free R-module. $\square$

Corollary 2.10.3. *If M is a finitely generated module over a PID then $R \cong \mathrm{Tor}(M) \oplus R^n$ for some $n \in \mathbb{N}$.*

Proof. $M/\mathrm{Tor}(M)$ is finitely generated and torsion-free. Hence,

$$M/\mathrm{Tor}(M) \cong R^n, \quad \text{for some } n.$$

R^n free $\Rightarrow M \mapsto\!\!\!\!\rightarrow M/\mathrm{Tor}(M) \cong R^n$ splits, so

$$M \cong \mathrm{Tor}(M) \oplus R^n.$$

$\square$

A torsion-free module over a PID which is not finitely generated need not be free:

Example 2.10.4. *Let $R = \mathbb{Z}$, $M = \mathbb{Q}$. Clearly $\mathbb{Q}$ is torsion-free as a $\mathbb{Z}$-module. Suppose $M \cong R^s$. Then as a vector space $/\mathbb{Q}$ we get*

$$\begin{aligned} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} &\cong M \otimes \mathbb{Q} \\ &\cong R^s \otimes \mathbb{Q} \\ &\cong (R \otimes \mathbb{Q})^s \\ &\cong \mathbb{Q}^s \end{aligned}$$

Let

$$\begin{gathered} \phi : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \mapsto \mathbb{Q} \\ x \otimes y \mapsto xy, \\ \psi : \mathbb{Q} \mapsto \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \\ x \mapsto x \otimes 1. \end{gathered}$$

Clearly $xy = 1_{\mathbb{Q}}$. $\psi\phi(x \otimes y) = (xy) \otimes 1$. Write $x = \frac{p}{q}, y = \frac{p'}{q'}$. Then in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$,

$$\begin{aligned} x \otimes y &= \frac{p}{q} \otimes \frac{p'}{q'} \\ &= q' \frac{p}{qq'} \otimes p' \frac{1}{q'} \\ &= p' \frac{p}{qq'} \otimes q' \frac{1}{q'} \\ &= \frac{pp'}{qq'} \otimes 1 \\ &= (xy) \otimes 1. \end{aligned}$$

$\therefore \psi\phi = 1_{\mathbb{Q}\otimes\mathbb{Q}}$. *Hence $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$, and thus $\mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^s$. So counting dimensions gives* $\mathrm{Card} S = 1$.

ie. If $\mathbb{Q}$ is a free R-module then its rank as a $\mathbb{Z}$-module is 1. So $\mathbb{Q} \cong \mathbb{Z}$ as a $\mathbb{Z}$-module. ie. $\exists q \in \mathbb{Q}$ s.t. $\mathbb{Q} = \mathbb{Z}q$; that is to say, $\forall x \in \mathbb{Q}\ \exists n \in \mathbb{Z}$ s.t. $x = nq$. This is a contradiction.

So $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

We now consider decompositions of finitely generated torsion modules over a PID. Let R be a PID (throughout this section). We will show that every finitely generated R-module decomposes as a direct sum of finitely many R-modules with a single generator (called cyclic modules).

First consider torsion modules.

Notation: For $r \in R$, let $\mu_r : M \mapsto M$ be multiplication by r.

Lemma 2.10.5. *Let M be a torsion R-module. Write* $\mathrm{Ann}(M) = (a)$ *and suppose $b \in R$ such that* $(a, b) = 1$. *Then multiplication by b,*

$$M \overset{\mu_b}{\longmapsto} M$$

is an isomorphism.

Proof. Since R is a PID, $\exists s, t \in R$ such that $sa + tb = 1$. Hence, for $x \in M$,

$$x = sax + tbx = tbx,$$

$\therefore bx = 0 \Rightarrow x = 0$, so μ_b is injective. Moreover,

$$x = b(tx) = \mu_b(tx)$$

so μ_b is surjective. $\square$

Let $M \neq 0$ be a torsion module. Let $\mathrm{Ann}(M) = (a)$. Suppose $a \neq 0$. (Note: if M is torsion and f.g. then $a \neq 0$ automatically.)

$M \neq 0 \Rightarrow a$ is not a unit. Write

$$a = up_1^{e_1} \cdots p_k^{e_k}$$

where u is a unit and $p_1, \ldots, p_k$ are distinct primes. Replacing a by $u^{-1}a$, may assume

$$a = p_1^{e_1} \cdots p_k^{e_k}.$$

Let

$$M_{p_j} := \{x \in M \mid p_j^e x = 0 \text{ for some } e\}.$$

Lemma 2.10.6. $M \cong M_{p_1} \oplus \cdots \oplus M_{p_k}$.

Proof. $\forall x \in M$,

$$p_1^{e_1} \mu_{p_2^{e_2} \cdots p_k^{e_k}}(x) = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} x = 0$$

so $\mathrm{Im}\mu_{p_2^{e_2} \cdots p_k^{e_k}} \subset M_{p_1}$.

Since $p_2^{e_2} \cdots p_k^{e_k}$ is coprime to $\mathrm{Ann}(M_{p_1})$, by the preceding lemma,

$$\mu_{p_2^{e_2} \cdots p_k^{e_k}}|_{M_{p_1}}$$

is an isomorphism, so it splits the inclusion $M_{p_1} \hookrightarrow M$. Hence,

$$M \cong M_{p_1} \oplus \ker \mu_{p_2^{e_2} \cdots p_k^{e_k}}.$$

$\mathrm{Ann}(\ker\mu_{p_2^{e_2}\cdots p_k^{e_k}}) = p_2^{e_2}\cdots p_k^{e_k}$. By induction,

$$\ker\mu_{p_2^{e_2}\cdots p_k^{e_k}} \cong M'_{p_2}\oplus\cdots\oplus M'_{p_k}$$

where

$$\begin{aligned} M'_{p_j} &= \{x\in\ker\mu_{p_2^{e_2}\cdots p_k^{e_k}} \mid p_j^e x = 0 \text{ for some } e\} \\ &\subset M_{p_j} = \{x\in M \mid p_j^e x = 0 \text{ for some } e\}. \end{aligned}$$

However, $M_{p_j}\subset\ker\mu_{p_2^{e_2}\cdots p_k^{e_k}}$ so $M_{p_j}\subset M'_{p_j}$ and thus $M_{p_j} = M'_{p_j}$.

Hence $M\cong M_{p_1}\oplus\cdots\oplus M_{p_k}$. □

In the finitely generated case, we now decompose M_{p_j} into cyclic summands for each p_j. ie. We have reduced to the case where $\mathrm{Ann}(M) = (p^e)$ for some prime p.

Suppose M is a f.g. R-module with $\mathrm{Ann}(M) = (p^e)$. $\exists x\in M$ such that $p^{e-1}x\neq 0$ (or else $\mathrm{Ann}(M) = p^{e-1}$ rather than p^e). Let $x, m_1,\ldots,m_k$ be a generating set for M. Let M_j be the submodule

$$M_j := \langle x, m_1,\ldots,m_j\rangle.$$

Beginning with the identity map $r_0 : M_0\mapsto Rx$, we inductively construct $r_j : M_j\mapsto Rx$ extending $r_{j-1} : M_{j-1}\mapsto Rx$ to produce a splitting $r : M\mapsto Rx$ of the inclusion $Rx\hookrightarrow M$.

Suppose by induction that $r_{j-1} : M_{j-1}\mapsto Rx$ has been defined such that $r_{j-1}|_{Rx} = 1_{Rx}$. M_j is generated by M_{j-1} and m_j. So to define r_j extending r_{j-1}, must define $r_j(m_j)\in Rx$, ie. $r_j(m_j) = \lambda x$ for the correct λ.

Let $(p^s) = \mathrm{Ann}(M_j/M_{j-1})$, so $p^s m_j\in M_{j-1}$. $r_{j-1}(p^s m_j)\in Rx$, so $r_{j-1}(p^s m_j) = \alpha x$ for some $\alpha\in R$.

$$p^{e-s}\alpha x = p^{e-s}(r_{j-1}p^s m_j) = r_{j-1}(p^e m_j) = r_{j-1}(0) = 0$$

so $p^{e-s}\alpha = \lambda p^e$ for some $\lambda\in R \implies \alpha = \lambda p^s$.

Define $r_j(m_j) = \lambda x$ and $r_j(y) = r_{j-1}(y)\forall y\in M_{j-1}$. Then

$$r_j(p^s m_j) = p^s\lambda x = \alpha x = r_{j-1}(p^s m_j)$$

so r_j is well-defined. Thus $M\cong Rx\oplus M'$.

Applying the procedure to M' gives

$$M\cong Rx\oplus Rx'\oplus M''.$$

Continuing, the procedure eventually terminates since M is Noetherian.

$\therefore M \cong Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_n$ for some $x_1, \ldots, x_n$ with $\text{Ann}x_j = (p^j)$ for some j. Notice that

$$\begin{aligned} R &\overset{\psi_j}{\longmapsto} Rx_j \\ r &\mapsto rx_j \end{aligned}$$

is surjective with $\ker \psi_j = \text{Ann}x_j$. Thus $Rx_j \cong R/(p^j)$.

Putting it all together, we get:

Theorem 2.10.7 (Structure Theorem for Finitely Generated Modules over a PID)**.** *Let M be a finitely generated module over a PID R. Then*

$$M \cong R/(p_1^{s_1}) \oplus R/(p_2^{s_2}) \oplus \cdots \oplus R/(p_n^{s_n}) \oplus R^k,$$

where $p_1, \ldots, p_n \in R$ are primes (not necessarily distinct), $s_1, \ldots, s_n \in \mathbb{N}$ and $k \geq 0$.

Note that the generator of $\text{Ann}(M)$ is $\text{lcm}\{p_1^{s_1}, \ldots, p_n^{s_n}\}$.

We now show that this decomposition is unique. k is the dimension of $M \otimes_R K$, where K is the field of fractions, so k is unique, and we need only be concerned with the torsion part of the module.

Theorem 2.10.8. *Suppose*

$$R/(p_1^{s_1}) \oplus R/(p_2^{s_2}) \oplus \cdots \oplus R/(p_n^{s_n}) \cong R/(q_1^{t_1}) \oplus R/(q_2^{t_2}) \oplus \cdots \oplus R/(q_k^{t_k}),$$

with $p_1, \ldots, p_n, q_1, \ldots q_k$ primes in R and $s_1, \ldots s_n, t_1, \ldots t_k \in \mathbb{N}$. Then $n = k$ and $\{q_1^{t_1}, \ldots, q_k^{t_k}\}$ is a permutation of (associates of) $\{p_1^{s_1}, \ldots, p_n^{s_n}\}$.

Proof. Let

$$\begin{aligned} M &= R/(p_1^{s_1}) \oplus R/(p_2^{s_2}) \oplus \cdots \oplus R/(p_n^{s_n}) \quad \text{and} \\ N &= R/(q_1^{t_1}) \oplus R/(q_2^{t_2}) \oplus \cdots \oplus R/(q_k^{t_k}). \end{aligned}$$

For any prime p, let

$$\begin{aligned} M_p &= \{x \in M \mid p^e x = 0, \text{ for some } e\}, \\ N_p &= \{x \in N \mid p^e x = 0, \text{ for some } e\}. \end{aligned}$$

If $M \cong N$ then $M_p \cong N_p$. Moreover,

$$\begin{aligned} M_p &\cong \bigoplus_{p_j \text{ assoc. to } p} R/(p_j^{s_j}), \\ N_p &\cong \bigoplus_{q_j \text{ assoc. to } p} R/(q_j^{t_j}). \end{aligned}$$

$\therefore$ It suffices to consider one prime at a time. ie. We are reduced to the case where $p_j = q_j = p\ \forall j$.

Suppose

$$M = R/(p^{s_1}) \oplus \cdots \oplus R/(p^{s_n}) \quad \text{and} \quad N = R/(p^{q_1}) \oplus \cdots \oplus R/(p^{q_k}).$$

For $Z = R/(p^s)$, $\exists$ a short exact sequence

$$0 \mapsto pZ \mapsto Z \mapsto R/p \mapsto 0,$$

ie. $Z/pZ \cong R/p$, a field.

Since $M \cong N$,

$$\bigoplus_n R/p \cong M/pM \cong N/pN \cong \bigoplus_k R/p.$$

Since the dimension of a vector space is an invariant of the isomorphism class of the vector space, $n = k$.

Also, $M \cong N \Rightarrow pM \cong pN$; that is:

$$R/p^{s_1-1} \oplus \cdots \oplus R/p^{s_n-1} \cong R/p^{t_1-1} \oplus \cdots \oplus R/p^{t_k-1}.$$

Ann(pM) has one less power of p than Ann$M$. So by induction on the size of Ann(M), the positive elts. in the list $\{t_1 - 1, \ldots, t_k - 1\}$ is a permutation of those in $\{s_1 - 1, \ldots, s_n - 1\}$. ie. Information about summands R/p has been lost, since $p(R/p) = 0$, so pM and pN have no record of how many summands R/p there were in M and N. But they see all the remaining summands, showing that entries in $\{t_1, \ldots, t_k\}$ which are at least 2 are the same (up to a permutation) as those in $\{s_1, \ldots, s_n\}$. The remaining entries on each list are 1, and there are the same number of them on each list since $n = k$ and the entries greater than 1 correspond.

$\therefore \{t_1, \ldots, t_k\}$ is a permutation of $\{s_1, \ldots, s_n\}$. □

Thus, $\{p_j^{s_j}\}$ is uniquely determined by (and uniquely determines) M. It is called the set of **elementary divisors** of M.

Example 2.10.9.

1. $R = \mathbb{Z}$. *List all non-isomorphic abelian groups of order* 16*:*

$$\mathbb{Z}/16, \quad \mathbb{Z}/8 \oplus \mathbb{Z}/2, \quad \mathbb{Z}/4 \oplus \mathbb{Z}/4 \quad \mathbb{Z}/4 \oplus \mathbb{Z}/2, \oplus\mathbb{Z}/2 \quad \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

(all non-isomorphic by the theorem).

2. *Let F be a field, V a f.d. vector space $/F$, $T : V \mapsto V$ a linear transformation. Let $R = F[x]$ (a PID) and $M = V$ with R-action*

$$f(x)(v) = f(T)(v) = \sum_{j=0}^{n} a_j T^j(v).$$

Let

$$\mathrm{Ch}(\lambda) = \det(T - \lambda I),$$

the ***characteristic polynomial*** *of* T. *Then* $\mathrm{Ch}(T) = 0$ *(Cayley-Hamilton Theorem).*

$\therefore \mathrm{Ch}(x)v = 0\ \forall v \in V$. *ie.* M *is a torsion* R*-module and* $\mathrm{Ch}(x) \in \mathrm{Ann}(M)$. *Hence*

$$M \cong F[x]/p_1(x)^{r_1} \oplus \cdots \oplus F[x]/p_k(x)^{r_k}$$

for some primes $p_1(x), \ldots, p_k(x) \in F[x]$.

Suppose F *is algebraically closed so that every poly. in* $F[x]$ *factors completely as a product of linear factors. Then the primes in* $F[x]$ *are the degree* 1 *polynomials. So mult. by a scalar to make* p_j *monic:*

$$p_j(x) = x - \lambda_j$$

for some $\lambda_j \in F$. *Then*

$$M \cong \cdots \oplus F[x]/(x - \lambda_j)^{r_j} \oplus \cdots$$

implies that $\exists v \in V$ *s.t.* $(x - \lambda_j) \in \mathrm{Ann} V$. *ie.* $(T - \lambda_j)v = 0$. *(And conversely, if* $(T - \lambda)v = 0$ *for some* v *then* $x - \lambda = p_j(x)$ *for some* j*.)*

$\therefore \{\lambda_1, \ldots, \lambda_k\}$ = *eigenvalues of* T.

Examine $F[x]/(x-\lambda_j)^{r_j}$ *more closely. Write* λ *for* λ_j *and* r *for* r_j. *As an* $F[x]$*-module,* $F[x]/(x-\lambda)^r$ *is gen. by* $(x - \lambda)$. *Elts. can be written uniquely as*

$$\sum_{k=0}^{r-1} a_k (x - \lambda)^k$$

where $a_k \in F$. *ie. Over* F, $F[x]/(x - \lambda)^r$ *has dimension* r *with basis*

$$1, x - \lambda, (x - \lambda)^2, \ldots, (x - \lambda)^{r-1}.$$

Let $B = B_j \subset V = M$ *be the image of* $F[x] = (x - \lambda_j)^{r_j}$ *under the iso.*

$$\psi : \bigoplus_i F[x]/(x - \lambda_i)^{r_i} \overset{\cong}{\longmapsto} M$$

and let $v_j = \psi((x - \lambda)^{j-1})$ *for* $j = 1, \ldots, r$ *be the* F*-basis for* B *corresponding to the basis* $\{(x - \lambda)^i\}$.

B *is a* $F[x]$*-submodule of* V *so it is closed under the action of any* $f(x) \in F[x]$. *For* $f(x) = x - \lambda$, *by construction,*

$$\begin{aligned} f(x) \cdot v_j &= v_{j+1} \quad j < r \\ f(x) \cdot v_r &= 0. \end{aligned}$$

ie. when written in the basis $v_1, \ldots, v_r$, the matrix $T - \lambda$ is

$$\begin{pmatrix} 0 & 0 & \cdots & & 0 \\ 1 & & & & \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

ie. T looks like

$$\begin{pmatrix} \lambda & 0 & \cdots & & 0 \\ 1 & \lambda & & & \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \lambda & \\ 0 & \cdots & 0 & 1 & \lambda \end{pmatrix}.$$

Therefore:

Theorem 2.10.10 (Jordan Canonical Form)**.** *Let $T : V \mapsto V$ be a linear transformation where V is a f.d. vector space over an algebraically closed field F. Then $\exists$ a basis for V in which T has the form*

$$\begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & B_k \end{pmatrix}$$

where

$$B_j = \begin{pmatrix} \lambda_j & 0 & \cdots & & 0 \\ 1 & \lambda_j & \ddots & & \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda_j & 0 \\ 0 & \cdots & 0 & 1 & \lambda_j \end{pmatrix}.$$

Note: While $\mathrm{Ch}(\lambda) \in \mathrm{Ann}(V)$, it does not necessarily generate the ideal $\mathrm{Ann}(V)$. Letting $\mathrm{Ann}(V) = (M(\lambda))$, $M(\lambda)$ is called the **minimum polynomial** of T. ie.

$$\mathrm{Ch}(x) = \prod_j (x - \lambda_j)^{r_j} \quad \text{but} \quad M(x) = \mathrm{lcm}\{(x - \lambda_j)^{r_j}\}.$$

Reformulation of the Structure Theorem for f.g. torsion modules.
Let R be a PID and let $a, b \in R$ be relatively prime. Then $Ra + Rb = 1$ so the Chinese Remainder Thm. applies:

$$R \xrightarrow{\phi} R/(a) \times R/(b)$$

and $\ker \phi = (a) \cap (b) = (a)(b)$.
Claim. R a PID and $\gcd(a, b) = 1 \Rightarrow (a)(b) = (ab)$.

Proof. $(a)(b) = (c)$ for some c. Since $ab \in (a)(b) = (c)$, $c \mid ab$.

Conversely, $(c) = (a) \cap (b) \subset (a)$ so $a \mid c$ and similarly $b \mid c$. Write $c = \lambda a$ and $c = \mu b$. $\gcd(a, b) = 1$ $\Rightarrow \exists s, t$ s.t. $sa + tb = 1$. So

$$\begin{aligned} \lambda &= \lambda sa + \lambda bt \\ &= sc + \lambda bt \\ &= s\mu b + \lambda bt \\ &= (s\mu + \lambda t)b \end{aligned}$$

$\therefore (ab) = (c)$. □

Thus

$$R/(ab) \cong R/(a) \times R/(b).$$

By continual application of this iso. we can rewrite our decomposition thm. as follows:

Theorem 2.10.11. *Let M be a f.g. R-module (R a PID). Then*

$$M \cong R^k \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n)$$

where $a_n \mid a_{n-1} \mid \cdots \mid a_1 \neq 0$.

$a_1, \ldots, a_n$ are called the **invariant factors** of M.

Example 2.10.12. *Suppose*

$$M \cong \mathbb{Z}/8 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5.$$

Then

$$M \cong \mathbb{Z}/360 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}/2$$

The number of summands required is

$$\max\{r \mid \text{some prime } p \text{ occurs } r \text{ times among the elementary divisors}\}.$$

Reformulation of Chinese Remainder Thm. over a PID. Suppose $m_1, \ldots, m_k$ satisfy $\gcd(m_i, m_j) = 1$ for $i \neq j$. Given $a_1, \ldots, a_k$, $\exists x \in R/(m_1 \cdots m_k)$ s.t. $x \equiv a_j \mod m_j \forall j = 1, \ldots, k$.

Example 2.10.13. *Find x s.t.* $x \equiv 2 \mod 9, x \equiv 3 \mod 5, x \equiv 3 \mod 7$.

Solution. $m_1 = 9, m_2 = 5, m_3 = 7, a_1 = 2, a_2 = 3, a_3 = 3$. Set $z_1 := m_2 m_3 = 35$. Then

$$\begin{aligned} y_1 &:= z_1^{-1} \mod 9 \\ &= 8^{-1} \mod 9 \\ &= 8. \end{aligned}$$

Likewise,

$$\begin{aligned} z_2 &:= m_1 m_2 = 60 \\ y_2 &:= z_2^{-1} \mod 5 \\ &= 3^{-1} \mod 5 \\ &= 2, \\ z_3 &:= m_1 m_2 = 45 \\ y_3 &:= z_3^{-1} \mod 7 \\ &= 3^{-1} \mod 7 \\ &= 5. \end{aligned}$$

Set $x := a_1 y_1 z_1 + a_2 y_2 z_2 + a_3 y_3 z_3 \mod (m_1 m_2 m_3)$. Then modulo m_1, $z_2 \equiv 0, z_3 \equiv 0, y_1 z_1 \equiv 1$, so $x \equiv a_1 \mod m_1$, etc. In our example,

$$\begin{aligned} x &= 2 \cdot 8 \cdot 35 + 3 \cdot 2 \cdot 63 + 5 \cdot 3 \cdot 45 \mod (9 \cdot 5 \cdot 7) \\ &= 1613 \mod 315 \\ &= 38 \mod 315. \end{aligned}$$

In general, $x = \sum_j a_j y_j z_j$ where $z_j = m_1 \cdots m_{j-1} m_{j+1} \cdots m_n$ and $y_j = z_j^{-1} \mod m_j$.

Chapter 3

Galois Theory

3.1 Preliminaries about Polynomials and Fields

Proposition 3.1.1. *Let $F \subset K$ be an extension of fields. Let $f(x), g(x) \in F[x]$. Then a g.c.d. of $f(x), g(x)$ within $F[x]$ is also a g.c.d. of $f(x), g(x)$ within $K[x]$.*

Proof. Let $d(x) \in F[x]$ be a g.c.d. for $f(x), g(x)$ within $F[x]$. Then $\exists s(x), t(x) \in F[x]$ s.t.

$$s(x)f(x) + t(x)g(x) = d(x) \tag{1}$$

Since $F[x] \subset K[x]$, this eqn. holds in $K[x]$ also.

$d(x) \mid f(x)$ and $d(x) \mid g(x)$ holds in $F[x]$ and thus holds in $K[x]$. If $h(x) \mid f(x)$ and $h(x) \mid g(x)$ within $K[x]$ then (1) $\Rightarrow h(x) \mid d(x)$ in $K[x]$. Hence $d(x)$ is a g.c.d. for $f(x), g(x)$ in $K[x]$. □

Proposition 3.1.2. *The ideal $(p(x))$ in $F[x]$ is maximal $\iff$ $p(x)$ is irreducible.*

Proof. $F[x]$ is a PID so in $F[x]$, prime $\iff$ irreducible $\iff$ maximal. □

Corollary 3.1.3. *$F[x]/(p(x))$ is a field $\iff$ $p(x)$ is irreducible.*

Theorem 3.1.4 (Eisenstein Irreducibility Criterion)**.** *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

where R is a UFD. Let $p \in R$ be prime. Suppose $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $K[x]$ where K is the field of fractions of R.

Proof. It suffices to consider the case where $\{a_0, \ldots, a_n\}$ has no common factor. Suppose $f(x)$ is reducible over K and thus (by Gauss' Lemma) reducible over R. Write

$$f(x) = (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots c_r x^s)$$

in $R[x]$, with $r < n, s < n$. Then $a_0 = b_0c_0$. Since $p \mid a_0$ but $p^2 \nmid a_0$, p divides one of b_0, c_0 but not both. Say $p \mid b_0, p \nmid c_0$. p can't divide every b_j since then it would divide a_n, so let k be the least integer s.t. $p \nmid b_k$. So

$$a_k = b_kc_0 + b_{k-1}c_1 + \cdots + b_1c_{k-1} + b_0c_k.$$

$p \mid b_0, \ldots, b_{k-1}$ but $p \nmid b_k$ and $p \nmid c_0 \Rightarrow p \nmid a_k$. This is a contradiction of one of the hypotheses.
$\therefore f(x)$ is irreducible. $\square$

3.2 Extension Fields

Suppose $F \subset K$, F, K fields. Then K is a vector space over F.

Definition 3.2.1. *The* ***degree*** *of K over F, written $[K : F]$ is the dimension of K as a v.s. $/F$. If $[K : F] < \infty$ we say K is a* ***finite extension*** *of F.*

Proposition 3.2.2. *Suppose $F \subset K \subset L$ finite extensions of fields. Then*

$$[L : F] = [L : K][K : F].$$

Proof. Let $[K : F] = n$, and let $w_1, \ldots, w_n \in K$ form a basis for K over F. Let $[L : K] = t$, and let $v_1, \ldots, v_t \in L$ form a basis for L over K. Check that $\{w_i v_j\}_{i=1,\ldots,n, j=1,\ldots,t}$ forms a basis for L over F:

1. Let $\ell \in L$. $v_1, \ldots, v_t$ a basis implies

   $$\ell = k_1 v_1 + k_2 v_2 + \cdots k_t v_t$$

   for some $k_1, \ldots, k_t \in K$. $w_1, \ldots, w_n$ a basis implies

   $$k_j = f_{j1} w_1 + f_{j2} w_2 + \cdots f_{jn} w_n$$

   for some $f_{j1}, \ldots, f_{jn} \in F$. Hence

   $$\begin{aligned} \ell =& f_{11}(w_1 v_1) + f_{12}(w_2 v_1) + \cdots + f_{1n}(w_n v_1) + f_{21}(w_1 v_2) + \cdots \\ &+ f_{2n}(w_n v_2) + \cdots + f_{t1}(w_1 v_t) + \cdots + f_{tn}(w_n v_t). \end{aligned}$$

   $\therefore$ ℓ is a linear comb. of $\{w_i v_j\}$ with coeffs. in F, so $\{w_i v_j\}$ spans L.

2. $\{w_i v_j\}_{i=1,\ldots,n, j=1,\ldots,t}$ is linearly independent: Suppose

   $$\begin{aligned} 0 &= f_{11} v_1 w_1 + \cdots + f_{1n} v_1 w_n + \cdots + f_{ij} v_j w_i + \cdots + f_{tn} v_t w_n \\ &= (f_{11} w_1 + f_{12} w_2 + \cdots + f_{1n} w_n) v_1 + \cdots + (f_{t1} w_1 + f_{t2} w_2 + \cdots f_{tn} w_n) v_t \end{aligned}$$

   Since $v_1, \ldots, v_t$ is a basis for L over K,

   $$f_{j1} w_1 + \cdots + f_{jn} w_n = 0 \quad \forall j = 1, \ldots, t.$$

   Since $w_1, \ldots, w_n$ is a basis for K over F, $f_{ji} = 0\ \forall j = 1, \ldots, t, i = 1, \ldots, n$.
   $\therefore$ $\{f_j w_i\}_{i=1,\ldots,n; j=1,\ldots,t}$ is linearly independent.

□

Corollary 3.2.3. *If $F \subset K \subset L$ with L a finite extension of F then* $[K : F] \mid [L : F]$.

eg. If $[L : F]$ is prime then $\nexists K$ lying strictly between F and L.
Suppose $F \subset K$ extension of fields. Let $a \in K$. Let

$$F(a) = \bigcap \{M \mid M \text{ is a field with } a \in M \text{ and } F \subset M \subset K\}.$$

Proposition 3.2.4. *$F(a)$ is a field.*

$\therefore$ $F(a)$, the field obtained from F by adjoining a, is the smallest subfield of K containing both F and a. Explicitly,

$$F(a) = \left\{ \frac{p(a)}{q(a)} \mid p(x), q(x) \in F[x], q(a) \neq 0 \text{ in } K \right\}.$$

Proof. Let

$$M = \left\{ \frac{p(a)}{q(a)} \mid p(x), q(x) \in F[x], q(a) \neq 0 \text{ in } K \right\}.$$

Let $x = \frac{p(a)}{q(a)} \in M$. Since $F(a)$ is a field and $a \in F(a)$, field axioms $\Rightarrow$ $p(a)$ and $q(a) \in F(a)$. $q(a) \neq 0$ $\Rightarrow \frac{1}{q(a)} \in F(a)$, so $x \in F(a)$. Hence $M \subset F(a)$.

It is easy to check that M is a field and clearly $a \in M$, so $F(a) \subset M$. □

Definition 3.2.5. *$a \in K$ is called* ***algebraic*** *over F if $\exists$ a polynomial $q(x) \in F[x]$ s.t. $q(a) = 0$ in K.*

We say that a **satisfies** the equation $q(x) = 0$ or say a is a **root** of $q(x)$ if $q(a) = 0$ in K.

Definition 3.2.6. *K is called* ***algebraic*** *over F if every element of K is algebraic over F.*

Definition 3.2.7. *If $a \in K$ is not algebraic over F then a is called* ***transcendental*** *over F.*

Note:

1. We will show that a algebraic $/F \Rightarrow [F(a) : F] < \infty$. However, K alg. $/F \not\Rightarrow [K : F] < \infty$.

   For example, let $K = \{x \in \mathbb{R} \mid x \text{ is algebraic over } \mathbb{Q}\}$. We will show later that K is a field, and by construction, K is alg. over $\mathbb{Q}$. But $[K : \mathbb{Q}] = \infty$.

2. Existence of elts. $x \in R$ s.t. x is transcendental over $\mathbb{Q}$ is easily established by a counting argument, because we will see that $\{x \in \mathbb{R} \mid x \text{ is algebraic over } \mathbb{Q}\}$ is countable. However, showing that any particular elt. of $\mathbb{R}$ is transcendental is not easy. eg. "π is transcendental" is true but nontrivial to prove.

Suppose a is algebraic over F. A polynomial $q(x) \in F[x]$ is called a **minimum polynomial** for a over F if $q(a) = 0$ and $\nexists q'(x)$ s.t. $q'(a) = 0$ with $\deg q' < \deg q$.

Given a min. polynomial for a over F, dividing by the lead coeff. gives a monic min. polynomial for a over F. A monic min. poly. of a over F is unique.

Proof. Suppose $q(x), r(x)$ are two monic min. polys. of a. By minimality, their degrees are equal. But then $s(x) = q(x) - r(x)$ has smaller degree and $s(a) = 0 - 0 = 0$. □

$\therefore$ We refer to "the min. polynomial of a".

Lemma 3.2.8. *The min. polynomial of a is irreducible.*

Proof. Let $p(x)$ be the min. poly. of a. If $p(x) = q(x)r(x)$ with $\deg q < \deg p$ and $\deg r < \deg p$ then since $p(a) = 0$, either $q(a) = 0$ or $r(a) = 0$. This is a contradiction. Hence $p(x)$ is irreducible. □

Theorem 3.2.9. *Suppose $F \subset K$, $a \in K$. Then a is algebraic over $F \iff [F(a) : F] < \infty$. More precisely, $[F(a) : F]$ = degree of the min. poly. of a.*

Proof.

$\Rightarrow$: Suppose $[F(a) : F] = n < \infty$. Consider

$$S = \{1, a, a^2, \ldots, a^n\}$$

$|S| = n + 1$. But $\dim F(a) = n$ as a v.s. $/F$. So the elts. of S are linearly dependent. ie. $\exists$ relation

$$c_0 + c_1 a + c_2 a^2 + \cdots c_n a^n = 0$$

where $c_j \in F$ and not all c_j are 0. Hence a satisfies $q(x) = 0$ where

$$q(x) = c_0 + c_1 x + c_2 x^2 + \cdots c_n x^n.$$

$\therefore$ a is algebraic over F.

$\Leftarrow$: Suppose a is alg. over F. Let

$$p(x) = p_0 + p_1 x + \cdots + x^n$$

be the min. poly. of a over F.

Claim. $B = \{1, a, a^2, \ldots, a^{n-1}\}$ forms a basis for $F(a)$ over F.

Proof. If B were linearly dependent then (as above) there would be a polynomial of degree $n-1$ or less satisfied by a, contradicting defn. of $p(x)$.

Show B spans $F(a)$: $p(a) = 0$ so

$$a^n = -p_0 - p_1 a - \cdots - p_{n-1} a^{n-1}$$

and thus, $a_n \in \operatorname{span} B$.

$$\begin{aligned} a^{n+1} &= a \cdot a^n \\ &= -p_0 a - p_1 a^2 - \cdots - p_{n-2} a^{n-1} - p_{n-1} a^n \\ &= -p_0 a - p_1 a^2 - \cdots - p_{n-2} a^{n-1} - p_{n-1}(-p_0 - p_1 a - \cdots - p_{n-1} a^{n-1}) \\ \in \operatorname{span} B \end{aligned}$$

etc. ie. By induction, $a^s \in \operatorname{span} B \ \forall s$, so $F[a] \subset \operatorname{span} B$.

So to finish the proof, it suffices to show:

Lemma 3.2.10. *$F(a) = F[a]$.*

Proof. $F[a] \subset F(a)$ is trivial. Conversely, let $x \in F(a)$, $x = \frac{q(a)}{r(a)}$ where $q(a), r(a) \in F[a]$ and $r(a) \neq 0$. $p(x) \nmid r(x)$ since $r(a) \neq 0$. Since $p(x)$ is irreducible, this implies $p(x), r(x)$ have no common factors, ie. $\gcd(p(x), r(x)) = 1$. So, $\exists$ polynomials $s(x), t(x)$ s.t.

$$s(x)p(x) + t(x)r(x) = 1.$$

$\therefore 1 = s(a)p(a) + t(a)r(a) = t(a)r(a)$. Thus, $\frac{1}{r(a)} = t(a)$ and

$$x = \frac{q(a)}{r(a)} = q(a)t(a) \in F[a].$$

$\therefore F(a) \subset F[a]$. ◻

Corollary 3.2.11. *Suppose $F \subset K$. Suppose $a \in K$ is algebraic over F and let $q(a) \in F[x]$ be the min. poly. of a over F. Then*

$$F(a) \cong F[x]/(q(x)).$$

Proof. Let $\phi : F[x] \mapsto F(a)$ be given by

$$\phi(p(x)) = p(a).$$

Since $F(a) = F[a]$, ϕ is onto.
Claim. $\ker \phi = (q(x))$.

Proof. Let $\ker\phi = (q'(x))$ where q' is monic. Then since $q(a) = 0$, $q'(x) \mid q(x)$. But $q(x)$ is irreducible, so either $q'(x) = 1$ or $q'(x) = q(x)$. Since $q'(a) = 0$, $q'(x) \neq 1$ so $q'(x) = q(x)$.

Thus, by 1st isomorphism theorem,

$$F(a) = \Im\phi \cong F[x]/\ker\phi = F[x]/(q(x).$$

□

Theorem 3.2.12. *Suppose $F \subset K$ are fields. Let*

$$M = \{x \in K \mid x \text{ is algebraic over } F\}.$$

Then M is a field.

Proof. Let $a, b \in M$. Must show $a \pm b, ab, a/b \in M$. Suppose $[F(a) : F] = m$ and $[F(b) : F] = n$. So b satisfies a degree n poly. $p(x)$ with coeffs in $F \subset F(a)$. $p(x)$ can be thought of as a polynomial in $F(a)[x]$, giving

$$[F(a)(b) : F(a)] \leq n.$$

Hence

$$[F(a)(b) : F] \leq nm.$$

Since $a + b \in F(a)(b)$,

$$F \subset F(a + b) \subset F(a)(b).$$

$\therefore$ $[F(a + b) : F] \leq nm$, and so $a + b$ is algebraic over F. Similarly, $a - b, ab, a/b \in F(a)(b)$ so the same argument applies. □

Notation: $F(a, b) = F(a)(b)$. Observe that $F(a, b) = F(b, a)$ is the smallest subfield of K containing F, a, b.

Corollary 3.2.13. *Suppose $F \subset K \subset L$. If K is algebraic over F and L is algebraic over K then L is algebraic over F.*

Proof. Let $z \in L$. L algebraic over $K \Rightarrow z$ satisfies $p(z) = 0$ where

$$p(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n$$

has coeffs. in K. So $F \subset F(c_1, \ldots, c_n) \subset K \subset L$. Since K is algebraic over F, each c_j is algebraic over F.

If m_j is the degree of the min. poly. of c_j over F then, as above,

$$[F(c_1, \ldots, c_n) : F] \leq m_1 \cdots m_n < \infty.$$

Since z satisfies the polynomial $p(x)$ whose coeffs. lie in $F(c_1, \ldots, c_n)$,

$$[F(c_1, \ldots, c_n, z) : F(c_1, \ldots, c_n)] < \infty.$$

$\therefore [F(c_1, \ldots, c_n, z) : F] < \infty$. But $F \subset F(z) \subset F(c_1, \ldots, c_n, z)$ so $[F(z) : F] < \infty$. Thus, z is algebraic over F.

This is true for all $z \in L$, so L is algebraic over F. $\square$

Example 3.2.14. *Let*

$$M = \{x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q}\}.$$

Our theorems show that M is a field, and by construction, it is algebraic over $\mathbb{Q}$. However, in $\mathbb{Q}[x]$, there are irreducible polynomials of arbitrarily large degree, and by definition, the roots of these polynomials are in M. So $[M : \mathbb{Q}]$ is unbounded.

3.3 Roots

Let F be a field and let $p(x) \in F[x]$. p might have no roots in F.
Question. Given $p(x) \in F[x]$, can we always find an extension field $K \supset F$ in which $p(x)$ has a root?

Theorem 3.3.1 (Remainder Theorem)**.** *Let K be a field. Let $p(x) \in K[x]$ and let $b \in K$. Then $\exists q(x)$ s.t. $p(x) = (x - b)q(x) + p(b)$, and* $\deg q(x) = (\deg p(x)) - 1$.

Proof. By division algorithm, $p(x) = (x-b)q(x)+r(x)$ where $\deg r < \deg(x-b) = 1$. ie. $r(x) = r \in K$.
Setting $x = b$,

$$p(b) = (b - b)q(b) + r = r.$$

Comparing degrees of LHS and RHS, $\deg q(x) = (\deg p(x)) - 1$. □

Corollary 3.3.2 (Factor Theorem)**.** *a is a root of $p(x) \iff (x - a) \mid p(x)$.*

Proof. $p(x) = (x - a)q(x) + p(a)$. If $p(a) = 0$ then $p(x) = (x - a)q(x)$ so $(x - a) \mid p(x)$. Conversely, if $p(x)$ is a multiple of $x - a$ then $p(a) = 0$. □

Definition 3.3.3. *The* ***multiplicity*** *of a root a of $p(x)$ is the largest power of $(x-a)$ which divides $p(x)$.*

Corollary 3.3.4. *A polynomial of degree n over a field K can have at most n roots (counted with multiplicity).*

Proof. A polynomial of degree 1 has exactly one root, so the result follows from the Factor Thm. by induction. □

Theorem 3.3.5. *Let $p(x) \in F[x]$ be a poly of degree n where F is a field. Then $\exists$ an extension field K of F with $[K : F] \leq n$ in which $p(x)$ has a root.*

Proof. Let $q(x)$ be an irred. factor of $p(x)$. Since any root of $q(x)$ is a root of $p(x)$ we will find an extension field in which $q(x)$ has a root. Let

$$K = F[x]/(q(x)).$$

$q(x)$ irreducible $\Rightarrow K$ is a field. $F \hookrightarrow K$ by $c \mapsto [c]$, so K is an extension field of F.
In K, $q([x]) = [q(x)] = 0$. So $a = [x]$ is a root of $q(x)$. Since $q(x)$ is irreducible over F, $q(x)$ is the min. poly. of a over F.
$\therefore K = F(a)$ and

$$\begin{aligned}[K : F] &= [F(a) : F] \\ &= \deg(\text{min. poly of } a) \\ &= \deg q \\ &\leq \deg p = n.\end{aligned}$$

□

Example 3.3.6. *Let $F = \mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$. (x^2+x+1) is irred. in $\mathbb{F}_2[x]$. Let*

$$K = \frac{\mathbb{F}_2[x]}{(x^2+x+1)}.$$

Let $w = [x] \in K$, so $w^2+w+1 = [x^2+x+1] = 0$.

In K we have four elements: $0, 1, w, w+1$. Multiplication is as follows:
Mult. by 0 and 1 is obvious.

$$\begin{aligned} w^2 &= -w-1 = w+1 \\ w(w-1) &= w^2+1 = w+1+w = 1 \\ (w-1)^2 &= w^2+2w+1 = w+1+1 = w \end{aligned}$$

Note $\frac{1}{w} = w-1$ and $\frac{1}{w-1} = w$ (every nonzero elt. has an inverse).

$$K = \mathbb{F}_4$$

(finite field with 4 elements).

By induction on the previous result, we get

Corollary 3.3.7. *Let $p(x) \in F[x]$ be a poly. of degree n (F a field). Then $\exists$ an extension field K of F with $[K:F] \leq n!$ in which $p(x)$ has n roots. ie. In K we can factor $p(x)$ completely as*

$$p(x) = \lambda(x-a_1)(x-a_2)\cdots(x-a_n).$$

Example 3.3.8.

1. *$F = \mathbb{Q}$, $p(x) = x^3-2$. Let $E_1 = F(2^{\frac{1}{3}})$ Then $[E_1 : F] = 3$. In E_1,*

   $$p(x) = (x-2^{\frac{1}{3}})(x^2+2^{\frac{1}{3}}x+2^{\frac{2}{3}}).$$

   Let $K = E_1(\sqrt{3}i)$. Then $[K:E_1] = 2$ so $[K:F] = 3 \cdot 2 = 6$. In K,

   $$p(x) = (x-2^{\frac{1}{3}})\left(x+\frac{2^{\frac{1}{3}}(1-\sqrt{3}i)}{2}\right)\left(x+\frac{2^{\frac{1}{3}}(1+\sqrt{3}i)}{2}\right).$$

2. *$F = \mathbb{Q}$, $p(x) = x^3-12x+8$. Let $M = -4+4\sqrt{3}i$. Let $z = M^{\frac{1}{3}}$ (that is, z is any one of the three elts. s.t. $z^3 = -4+4\sqrt{3}i$). Let $a = z+\bar{z}$.*
   So $\bar{z}^3 = \overline{M}$ and

   $$z\bar{z} = (M\overline{M})^{\frac{1}{3}} = (16+48)^{\frac{1}{3}} = 64^{\frac{1}{3}} = 4.$$

Thus

$$\begin{aligned} a^3 &= (z+\overline{z})^3 \\ &= M + \overline{M} + 3z^2\overline{z} + 3z\overline{z}^2 \\ &= M + \overline{M} + 3(z\overline{z})(z+\overline{z}) \\ &= M + \overline{M} + 3z\overline{z}a \\ &= -8 + 3\cdot 4\cdot a \\ &= -8 + 12a \end{aligned}$$

$\therefore a^3 - 12a + 8 = 0$. *Let* $E_1 = \mathbb{Q}(a)$, *so* $[E : F] = 3$. *Let* $b = \frac{a^2-8}{2} \in E_1$. *Then*

$$\begin{aligned} b^3 &= \frac{a^6 - 12a^4 + 3\cdot 64a^2 - 8^3}{8} \\ &= \frac{(12a-8)^2 - 24a(12a-8) + 3\cdot 64a^2 - 8^3}{8} \\ &= \frac{16(9a^2 - 12a + 4) - 24(12a^2 - 8a) + 3\cdot 64a^2 - 8^3}{8} \\ &= 18a^2 - 24a + 8 - 36a^2 + 24a + 24a^2 - 64 = 6a^2 - 56 \\ 12b - 8 &= 12\left(\frac{a^2-8}{2}\right) - 8 \\ &= 6(a^2 - 8) - 8 \\ &= 6a^2 - 48 - 8 \\ &= 6a^2 - 56 \end{aligned}$$

$\therefore b^3 - 12b + 8 = 0$. *Note that this second root is already in* E_1. *Let* c *be the third root. Then*

$$a + b + c = \text{coeff. of } x^2 \text{ in } p(x) = 0.$$

$\therefore c = -a - b \in E_1$. *So all* 3 *roots lie in* E_1. *In* E_1, $x^3 - 12x + 8$ *factors as* $(x-a)(x-b)(x-c)$.

Definition 3.3.9. *Let* $p(x) \in F[x]$. *An extension field* K *of* F *is called a* ***splitting field*** *for* $p(x)$ *over* F *if* $p(x)$ *factors completely in* K *into linear factors*

$$p(x) = \lambda(x-a_1)(x-a_2)\cdots(x-a_n)$$

and $p(x)$ *does not factor completely in any proper subfield of* K.

ie. K is a minimal extension of F containing all roots of $p(x)$. By an earlier theorem, a poly. of degree n in $F[x]$ has a splitting field K s.t. $[K : F] \leq n!$.

Proposition 3.3.10. *Suppose $F \subset M \subset K$. Let $p(x) \in F[x]$ and suppose that K is a splitting field of $f(x)$ over F. Then regarding $p(x)$ as an elt. of $M[x]$, K is also a splitting field of $p(x)$ over M.*

Proof. Trivial. □

Example 3.3.11.

1. *$p(x) = x^3 - 2$, $F = \mathbb{Q}$. $2^{\frac{1}{3}}$ is a root of $p(x)$ but $\mathbb{Q}(2^{\frac{1}{3}})$ is not a splitting field for $p(x)$. $K = \mathbb{Q}(2^{\frac{1}{3}}, \sqrt{3}i)$ is a splitting field for $p(x)$, and $[K : \mathbb{Q}] = 6$.*

2. *$p(x) = x^3 - 12x + 8$, $F = \mathbb{Q}$. $a = z + \bar{z}$ where $z^3 = -4 + 4\sqrt{3}i$. a is a root of $p(x)$ and $K = \mathbb{Q}(a)$ is a splitting field for $p(x)$. In this case, $[K : \mathbb{Q}] = 3$.*

Proposition 3.3.12. *Let $K \supset F$ be a splitting field for $p(x) \in F[x]$. Suppose that in K,*

$$p(x) = \lambda(x - a_1)(x - a_2) \cdots (x - a_n),$$

where $\lambda \in K$. Then

$$K = F(a_1, \ldots, a_n).$$

Proof. By defn of $a_1, \ldots, a_n$ they lie in K so $F(a_1, \ldots, a_n) \subset K$. However, if all of $a_1, \ldots, a_n$ lay in some proper subfield of K then the factorization

$$p(x) = \lambda(x - a_1)(x - a_2) \cdots (x - a_n)$$

would be valid in that subfield, contradicting the minimality of K. □

Recall that if $a \in K$ is a root of an irreducible poly. $p(x) \in F[x]$ then

$$F(a) \cong F[x]/(p(x))$$

where the isomorphism $\psi : F[x]/(p(x)) \overset{\cong}{\longmapsto} F(a)$ is given by $\psi(x) = a$. Suppose $\tau : F \overset{\cong}{\longmapsto} F'$. τ extends to

$$\begin{aligned} \tilde{\tau} : F[x] &\overset{\cong}{\longmapsto} F'[x] \\ x &\longmapsto x \\ f &\longmapsto \tau(f) \quad \forall f \in F. \end{aligned}$$

Theorem 3.3.13. *Let $p(x) \in F[x]$ be irreducible. Let $p' = \tilde{\tau}(p) \in F'[x]$. Let a, a' be roots of $p(x), p'(x)$ lying in extension fields of F, F' respectively. Then τ can be extended to an isomorphism*

$$\phi : F(a) \overset{\cong}{\longmapsto} F(a')$$

s.t. $\phi(a) = a'$.

Proof. We have

$$F(a) \overset{\cong}{\longleftarrow} \psi \frac{F[x]}{(p(x))} \overset{\cong}{\longrightarrow} \tilde{\tau} \frac{F'[x]}{(p'(x))} \overset{\cong}{\longrightarrow} \psi' F'(a')$$

Let $\phi = \psi' \circ \tilde{\tau} \circ \psi^{-1}$. □

Example 3.3.14. *$F = F' = \mathbb{Q}$, $\tau = 1_{\mathbb{Q}}$, $p(x) = p'(x) = x^3 - 2$. $a = 2^{\frac{1}{3}}, a' = 2^{\frac{1}{3}}\left(\frac{1-\sqrt{3}i}{2}\right)$. Using $a^3 = 2$, elts. of $\mathbb{Q}(a)$ can be expressed in the form $\alpha + \beta a + \gamma a^2$, $\alpha, \beta, \gamma \in \mathbb{Q}$. $\phi : \mathbb{Q}(a) \overset{\cong}{\longmapsto} \mathbb{Q}(a')$ is given by*

$$\phi(\alpha + \beta a + \gamma a^2) = \alpha + \beta a' + \gamma (a')^2.$$

Theorem 3.3.15. *Let $p(x) \in F[x]$. Let $p' = \tilde{\tau}(p) \in F'[x]$. Let E, E' be splitting fields of $p(x), p'(x)$ respectively. Then τ can be extended to an isomorphism $\phi : E \overset{\cong}{\longmapsto} E'$.*

In particular, letting $F' = F$ and $\tau = 1_F$ shows that any two splitting fields of $p(x)$ are isomorphic, by an isomorphism which fixes F.

Proof. Use induction on $[E : F]$. If $[E : F] = 1$ then $E = F$ so $p(x)$ splits into linear factors in F. But then $p'(x)$ splits into linear factors in F' so $E' = F'$, and use $\phi = \tau$.

Now let $[E : F] = n > 1$. Assume by induction that the theorem holds whenever $[E : F] < n$. More precisely, assume that the following statement holds: let $q(x) \in M[x]$ be a poly. over a field M, $\sigma : M \overset{\cong}{\longmapsto} M'$, $q' = \tilde{\sigma}(q)$. Let N, N' be splitting fields of q, q' respectively. If $[N : M] < n$ then σ can be extended to an iso. $\phi : N \overset{\cong}{\longmapsto} N'$.

Let $s(x)$ be a non-linear irreducible factor of $p(x)$ in $F[x]$. Let $\deg s(x) = r > 1$. Let $v \in E$ be a root of $s(x)$. Let $w \in E'$ be a root of $\tilde{\tau}(s)$. By prev. thm. $\exists$ iso. $\sigma : F(v) \overset{\cong}{\longmapsto} F'(w)$ s.t. $\sigma|_F = \tau$ and $\sigma(v) = w$. Since $\deg s(x) = r$, $[F(v) : F] = r$, so

$$[E : F(v)] = \frac{[E : F]}{[F(v) : F]} = \frac{n}{r} < n.$$

From an earlier proposition, E is a splitting field for $p(x)$ considered as a poly. in $F(v)[x]$, and likewise, E' is a splitting field for $p'(x)$ considered as a poly. in $F'(w)[x]$. So by the induction hypothesis, $\exists$ iso. $\phi : E \overset{\cong}{\longmapsto} E'$ s.t. $\phi|_{F(v)} = \sigma$. Thus $\phi|_F = \sigma|_F = \tau$ as required. □

3.4 Characteristic

Theorem 3.4.1. *Let R be an integral domain. Let H be the additive subgroup of R generated by* 1. *Then either $H \cong \mathbb{Z}$ or $H \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Proof. Define $\phi : \mathbb{Z} \mapsto F$ to be the group homomorphism determined by $\phi(1) = 1$. Then

$$H = \mathrm{Im}\phi \cong \mathbb{Z}/\ker\phi.$$

$\ker\phi$ is an ideal in $\mathbb{Z}$ so $\ker\phi = (n)$ for some n. If $n = 0$ then $H \cong \mathbb{Z}$. Otherwise, $H \cong \mathbb{Z}/n\mathbb{Z}$ (as groups), and by replacing n by $-n$ if necessary, we may assume $n > 0$.

If $a, b \in \mathbb{Z}, a, b > 0$ then in R,

$$\phi(a)\phi(b) = \overbrace{(1 + \cdots + 1)}^{a \text{ times}}\overbrace{(1 + \cdots + 1)}^{b \text{ times}} = \overbrace{(1 + \cdots + 1)}^{ab \text{ times}} = \phi(ab).$$

So $H \cong \mathbb{Z}/nZ$ as rings, and R is an integral domain, so p must be prime. $\square$

Definition 3.4.2. *If the additive subgroup of an integral domain R generated by* 1 *is $\mathbb{Z}/p\mathbb{Z}$, we say that R has **characteristic** p, and denote* $\mathrm{char}\, R = p$. *If this subgroup is $\mathbb{Z}$, we say* $\mathrm{char}\, R = 0$.

If F is a field with $\mathrm{char}\, F = p$, we can define

$$\begin{aligned} \theta : \mathbb{Z}/p\mathbb{Z} &\mapsto F \\ 1 &\mapsto 1 \end{aligned}$$

as an inclusion of fields. If $\mathrm{char}\, F = 0$, we can define

$$\begin{aligned} \theta : \mathbb{Q} &\mapsto F \\ 1 &\mapsto 1 \\ \frac{s}{t} &\mapsto \overbrace{(1 + \cdots + 1)}^{s \text{ times}} / \overbrace{(1 + \cdots + 1)}^{t \text{ times}} \end{aligned}$$

The image of θ is a subfield of F (isomorphic to either $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ or $\mathbb{Q}$), called the **prime field** of F.

Proposition 3.4.3. *If* $\mathrm{char}\, F = p$ *then in F,*

$$(a + b)^{p^k} = a^{p^k} + b^{p^k}.$$

Proof.

$$(a+b)^{p^k} = \sum_{i=0}^{p^k} \left(\begin{array}{c} p^k \\ i \end{array} \right) a^i b^{p^k-i} = a^{p^k} + b^{p^k} + \sum_{i=1}^{p^k-1} \left(\begin{array}{c} p^k \\ i \end{array} \right) a^i b^{p^k-i}.$$

If $1 \le i \le p^k - 1$ then

$$\begin{aligned} \left(\begin{array}{c} p^k \\ i \end{array} \right) &= \frac{p^k!}{i!(p^k-i)!} \\ &= \frac{p^k(p^k-1)\cdots(p^k-i+1)}{1\cdot 2\cdot 3\cdots i} \\ &= \left(\frac{p^k}{i}\right)\left(\frac{p^k-1}{1}\right)\left(\frac{p^k-2}{2}\right)\cdots\left(\frac{p^k-i+1}{i-1}\right). \end{aligned}$$

For $1 \le j < p^k$, the number of factors of p in j = the number of factors of p in $p^k - j$. However, since $i < p^k$, p^k has more factors of p than i does. Hence, the numerator has more factors of p than the denominator. ie. $p \,\Big|\, \left(\begin{array}{c} p^k \\ i \end{array} \right)$ for $0 < i < p^k$. Since char $F = p$,

$$\sum_{i=1}^{p^k-1} \left(\begin{array}{c} p^k \\ i \end{array} \right) a^i b^{p^k-i} = 0.$$

□

3.5 Repeated Roots

Notation: For $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, set

$$f'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-1} + \cdots + a_1.$$

$f'(x)$ is called the **derivative** of $f(x)$.
Note: If char $F = p \neq 0$ then $f'(x) = 0 \not\Rightarrow f(x)$ is constant. For example, $f(x) = x^p$ has $f'(x) = 0$.

Theorem 3.5.1. *$f(x)$ has a repeated root (in some extension field of F) $\iff f(x), f'(x)$ have a common factor.*

Proof. Let K be the splitting field of f.

Note that $f(x), f'(x)$ have a common factor $\iff \gcd(f, f') \neq 1$. Moreover, as seen before, the g.c.d. is the same whether taken in $F[x]$ or $K[x]$.

$\Rightarrow$: Suppose $f(x)$ has a repeated root. In $K[x]$, $f(x) = (x-\alpha)^2 q(x)$, so

$$f'(x) = 2(x-\alpha)q(x) + (x-\alpha)^2 q'(x) = (x-\alpha)(2q(x) + (x-\alpha)q'(x)).$$

$\therefore \gcd(f, f') \neq 1$ in K and thus in F.

$\Leftarrow$: Suppose $f(x), f'(x)$ have a common factor. If $f(x)$ has no repeated root then by (WLOG) taking $f(x)$ to be monic, in $K[x]$,

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

where $\alpha_j \neq \alpha_k$ for $j \neq k$. So

$$f'(x) = \sum_{i=1}^{n} (x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_r).$$

If $(x-\alpha_j)$ is also a factor of $f'(x)$ then α_j would be a root of $f'(x)$ giving

$$0 = \prod_{j\neq i}(\alpha_j - \alpha_i).$$

But then $\alpha_j - \alpha_i = 0$ for some i, which is a contradiction. Thus, $f(x)$ has a repeated root.

□

Corollary 3.5.2. *Let $f(x) \in F[x]$ be irreducible. Then*

1. *If* char $F = 0$ *then* $f(x)$ *has no repeated roots.*

2. *If* char $F = p > 0$ *then* $f(x)$ *has a repeated root* $\iff f(x) = g(x^p)$ *for some* g.

Proof. If $f(x)$ has a repeated root then $f(x), f'(x)$ have a common factor. But $f(x)$ is irreducible and $\deg f'(x) < \deg f(x)$. Thus $f'(x) = 0$.

If char $F = 0$ then $f'(x) = 0 \Rightarrow f(x)$ is constant, in which case, $f(x)$ does not have a repeated root after all.

If char $F = p$, let

$$f(x) = a_0 + a_1 x + \cdots + a_p x^p + a_{p+1} x^{p+1} + \cdots + a_n x^n.$$

Since $f'(x) = 0$, $a_k = 0$ for every k which is not a multiple of p. So

$$f(x) = a_p x^p + a_{2p} x^{2p} + \cdots = g(x^p).$$

□

3.6 Finite Fields

Proposition 3.6.1. *Let F be a field with q elements. Suppose $F \subset K$ is a finite extension with $[K : F] = n$. Then K has q^n elements.*

Proof. As a vector space, $K \cong F^n$, so $|K| = |F|^n = q^n$. □

Corollary 3.6.2. *Let K be a finite field. Then K has p^m elements for some m where $p = \operatorname{char} F$.*

Proof. Let F be the prime field of K. Since K is finite, F cannot be $\mathbb{Q}$, so $\operatorname{char} F = p$, a prime. Hence K has p^m elements where $m = [K : F]$. □

Corollary 3.6.3 (Fermat)**.** *Let F be a finite field with p^m elements. Then $a^{p^m} = a$ for all $a \in F$.*

Proof. If $a = 0$ then $a^{p^m} = 0$. If $a \neq 0$ then $a \in F - \{0\}$, which forms a group under multiplication, and

$$|F - \{0\}| = p^m - 1.$$

By Lagrange, $a^{p^m - 1} = 1$, so $a^{p^m} = a$. □

Theorem 3.6.4. *Let F be a finite field with p^n elements. Then in $F[x]$, $x^{p^n} - x$ factors as*

$$x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha).$$

Proof. By the previous corollary, every elt. of F is a root of $x^{p^n} - x$. Since $\deg(x^{p^n} - x) = p^n$, and F has p^n elements, we have all the roots. □

Corollary 3.6.5. *If F has p^n elements then F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.*

Corollary 3.6.6. *Any two finite fields with the same number of elts. are isomorphic.*

Proof. Any two splitting fields of the same polynomial are isomorphic. □

Theorem 3.6.7. *For every prime p and every positive integer n, $\exists!$ a field with p^n elts.*

Proof. We have already shown that $\exists$ at most one field with p^n elts. So, show that one exists.

Let K be the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. Let

$$F = \{a \in K \mid a^{p^n} = a\}.$$

$f'(x) = -1$, which is relatively prime to $f(x)$. So the roots of $f(x)$ are distinct, ie. F has p^n elts., and it suffices to show that F is a field.

Suppose $a, b \in F$. Then

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$$

so $a + b \in F$. Similarly, $(a-b)^{p^n} = a - b$.

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab$$

and similarly, $(\frac{a}{b})^{p^n} = \frac{a}{b}$. Hence F is a field. $\square$

Theorem 3.6.8. *Let G be a finite abelian group s.t. $\forall n \in \mathbb{Z}$, there are at most n elts. of G satisfying $g^n = e$. Then G is a cyclic group.*

Proof. By the structure theorem for finitely generated abelian groups, we can write

$$G \cong G_1 \times G_2 \times \cdots \times G_k$$

where $|G_j| = p_j^{t_j}$ for some p_j with $p_j \neq p_{j'}$ if $j \neq j'$. Since $C_n \times C_m \cong C_{nm}$ when $\gcd(n, m) = 1$, it suffices to show that each G_j is a cyclic group.

Pick j and write p for p_j and t for t_j. Let $a \in G_j$ be an elt. whose order is maximal. Then

$$|a| \,\Big|\, |G_j| = p^t$$

so $|a| = p^r$ for some $r \leq t$. Within G_j,

$$S = \{a, a^2, \cdots, a^{p^r - 1}, e\}$$

are the distinct roots of $g^{p^r} = e$, by construction of a. Since there are p^r of them, by the hypothesis, g^{p^r} has no other solutions in G, and in particular, no other solutions in G_j.

Now let $b \in G_j$. Then $|b| = p^s$ for some $s \leq r$.

$$b^{p^r} = \left(b^{p^s}\right)^{p^{r-s}} = e^{p^{r-s}} = e.$$

Thus, $b \in S$, ie. $b = a^i$ for some i.

Hence G_j is cyclic, so G is cyclic. $\square$

Corollary 3.6.9. *Let F be a field. Then any finite subgroup of the multiplicative group of $F - \{0\}$ is cyclic.*

Proof. Since F is a field, a polynomial of degree n in $F[x]$ has at most n roots in F. $\square$

Corollary 3.6.10. *If F is a finite field then the multiplicative group $F - \{0\}$ is cyclic.*

3.7 Separable Extensions

Definition 3.7.1. *Suppose $F \subset K$ is a finite extension. Then $\alpha \in K$ is called **separable** over F if its irreducible polynomial over F has no repeated roots. K is called separable over F if α is separable over F $\forall \alpha \in K$.*

Proposition 3.7.2. *If* $\operatorname{char} F = 0$ *then every finite extension of F is separable over F.*

Example 3.7.3. *Let E be any field with* $\operatorname{char} E = p$. *Let $F = E(z)$, the field of fractions of $E[z]$. Let $K = F(z^{\frac{1}{p}})$, and let $a = z^{\frac{1}{p}} \in K$. Then the min. poly. of a over F is $x^p - z = (x-a)^p$. Hence, $z^{\frac{1}{p}}$ is not separable over F.*

Theorem 3.7.4. *Suppose $F \subset K$ is separable. Then $\exists \gamma \in K$ s.t. $K = F(\gamma)$.*

Proof.

Case 1: F is finite.

Since $F \subset K$ is a finite extension, K is also a finite field. Let c be a generator for the cyclic group $K - \{0\}$.

$$\text{ie.} \quad K - \{0\} = \{c, c^2, \cdots, c^{p^m-1}, e\}.$$

$\therefore$ Any field containing c contains all of $K - \{0\}$. $\therefore K = F(c)$.

Case 2: $|F| = \infty$.

Since $[K : F] < \infty$, let $K = F(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n$. Using induction, it suffices to consider the case $n = 2$. ie. Suppose $K = F(a, b)$ and show that $\exists c$ s.t. $F(a, b) = F(c)$.

Let $f(x), g(x)$ be the min. polynomials of a, b respectively. Let M be the splitting field of $f(x)g(x)$. In M,

$$f(x) = (x - a_1) \cdots (x - a_m) \quad \text{where } a_1 = a$$
$$g(x) = (x - b_1) \cdots (x - b_n) \quad \text{where } b_1 = b.$$

Since K is separable, $a_i \neq a_j$ for $i \neq j$ and $b_i \neq b_j$ for $i \neq j$. Consider the equation

$$a_i + \lambda b_j = a_1 + \lambda b_1$$

where $j > 1$ and $\lambda \in F$. The solution for λ is

$$\lambda = \frac{a_i - a_1}{b_1 - b_j}$$

Since F is finite, choose $\gamma \in F$ s.t. $\gamma \neq \frac{a_i - a_1}{b_1 - b_j}$ and $\gamma \neq \frac{b_j - b_1}{a_1 - a_j}$ for any i and j. So $a_i + \gamma b_j \neq a + \gamma b$ unless $i = j = 1$. Set $c := a + \gamma b$.

Claim. $F(a, b) = F(c)$.

Proof. $c \in F(a,b)$ so $F(c) \subset F(a,b)$. So show $F(a,b) \subset F(c)$, ie. show $a \in F(c)$ and $b \in F(c)$.

Let $h(x) = f(c - \gamma x) \in F(c)[x]$. Then

$$h(b) = f(c - \gamma b) = f(a) = 0.$$

By construction, $c - \gamma b_j \neq a_i$ unless $i = j = 1$. So if $j > 1$ then $c - \gamma b_j \neq a_i$ for any i and so $c - \gamma b_j$ is not a root of $f(x)$.

$\therefore$ If $j > 1$ then $h(b_j) = f(c - \gamma b_j) \neq 0$. Hence $b = b_1$ is the only common root of $g(x)$ and $h(x)$. ie. In $K[x]$,

$$\gcd(g(x), h(x)) = x - b.$$

But $g(x) \in F[x] \subset F(c)[x]$ and $h(x) \in F(c)[x]$, so by an earlier proposition,

$$x - b = \gcd(g(x), h(x)) \in F(c)[x].$$

In particular, $x - b \in F(c)[x]$; that is, its coefficients lie in $F(c)$. So $b \in F(c)$.

Similarly, using $\gamma \neq \frac{b_j - b_1}{a_1 - a_i}$ for any i and j gives $a \in F(c)$. Thus $F(a,b) \subset F(c)$ as required.

$\square$

3.8 Automorphism Groups

Definition 3.8.1. *An isomorphism from a field to itself is called an* ***automorphism***. *Explicitly, an automorphism* $\sigma : F \overset{\cong}{\longmapsto} F$ *must satisfy:*

1. *σ is a bijection,*
2. *$\sigma(a + b) = \sigma(a) + \sigma(b)$, and*
3. *$\sigma(ab) = \sigma(a)\sigma(b)$.*

Let $\mathrm{Aut}(F)$ *denote the set of all automorphisms of F. This forms a group under composition.*

Theorem 3.8.2. *Let $\sigma_1, \dots, \sigma_n$ be distinct automorphisms of F. Then $\sigma_1, \dots, \sigma_n$ are linearly independent in the vector space* $\hom_{abel.\ grps.}(F, F)$.

ie. If $a_1, \dots, a_n \in F$ such that

$$a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0 \quad \forall u \in F$$

then $a_1 = a_2 = \cdots = a_n = 0$.
Note: This proof works equally well to show that distinct homomorphisms from a ring A to a field F are linearly independent in the F-vector space $\hom_{\text{abel. grps.}}(A, F)$.

Proof. Suppose $\sigma_1, \dots, \sigma_n$ are not linearly independent in $\hom_{\text{abel. grps.}}(F, F)$. Find a relation having as few terms as possible. Renumber the σ's so that the terms appearing in the relation come first. So the relation is

$$a_1\sigma_1 + \cdots + a_k\sigma_k = 0$$

with $a_j \neq 0$ for $j = 1, \dots, k$, and no relation exists involving fewer than k terms. That is, for all $u \in F$,

$$a_1\sigma_1(u) + \cdots + a_k\sigma_k(u) = 0 \tag{1}$$

If $k = 1$ then $a_1\sigma(u) = 0$ $\forall u \in K$, so $a_1 = 0$ (since $\sigma_1(u) \neq 0$ unless $u = 0$), which is a contradiction. Since $\sigma_1 \neq \sigma_k$, $\exists c \in F$ s.t. $\sigma_1(c) \neq \sigma_k(c)$. Then for all $u \in F$,

$$\begin{aligned} 0 &= a_1\sigma_1(cu) + \cdots + a_k\sigma_k(cu) \\ &= a_1\sigma_1(c)\sigma_1(u) + \cdots + a_k\sigma_k(c)\sigma_k(u) \end{aligned} \tag{2}$$

Combining (1) and (2), for all $u \in F$,

$$a_2(\sigma_2(c) - \sigma_1(c))\sigma_2(u) + \cdots + a_k(\sigma_k(c) - \sigma_1(c))\sigma_k(u) = 0$$

$a_k \neq 0$ and $\sigma_k(c) - \sigma_1(c) \neq 0$ so the last coefficient is nonzero. So this is a relation among $\sigma_1, \dots, \sigma_n$ having fewer than k terms, which is a contradiction. Thus, $\sigma_1, \dots, \sigma_k$ are lin. indep. $\square$

Theorem 3.8.3. *Let K be a field. Let $S = \{\sigma_\alpha\}$ be a set of automorphisms of K. Let*

$$F = \{x \in K \mid \sigma(x) = x \ \forall \sigma \in S\}.$$

Then F is a field.

F is called the **fixed field** of S in K, written $F = K^S$.

Proof. Suppose $a, b \in F$. Then $\forall \sigma \in S$,

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b.$$

$\therefore a + b \in F$. Similarly, $a - b, ab \in F$ and if $b \neq 0$, $\frac{a}{b} \in F$. ◻

Notation: Suppose $F \subset K$. Set

$$G(K, F) := \{\sigma \in \mathrm{Aut}(K) \mid \sigma(\alpha) = \alpha \ \forall \alpha \in F\}.$$

$G(K, F)$ forms a subgroup of $\mathrm{Aut}(K)$.

This gives us two functors:

$$\begin{aligned} \text{Extension of fields} &\rightsquigarrow \text{Subgroup of automorphisms of larger field} \\ F \subset K &\rightsquigarrow G(K, F) \end{aligned}$$

and

$$\begin{aligned} \text{Field, subgroup of its automorphisms} &\rightsquigarrow \text{Extension of fields} \\ K, G &\rightsquigarrow K^G \subset K \end{aligned}$$

Are these inverse processes? In general, no. Given $F \subset K$,

$$G(K, F) = \{\sigma \in K \mid \sigma(x) = x \forall x \in F\}$$

$\therefore K^{G(K,F)} = \{x \in K \mid \sigma(x) = x \forall \sigma \in G(K, F)\} \supset F$. But $K^{G(K,F)}$ can be strictly larger than F.

Example 3.8.4.

1. *$K = \mathbb{C}$, $F = \mathbb{R}$. Let $\sigma \in G(\mathbb{C}, \mathbb{R})$. $\sigma(x) = x \ \forall x \in \mathbb{R}$. So σ is determined by $\sigma(i)$.*

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1.$$

   $\therefore \sigma(i) = \pm i$. So there are two elts. in $G(\mathbb{C}, \mathbb{R})$:

$$\begin{aligned} \sigma_1(i) = i \Rightarrow \ & \sigma_1(a + bi) = a + bi \quad \textit{identity of } G(\mathbb{C}, \mathbb{R}), \\ \sigma_2(i) = -i \Rightarrow \ & \sigma_2(a + bi) = a - bi \quad \textit{complex conjugation.} \end{aligned}$$

$\therefore G(\mathbb{C}, \mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Conversely,

$$\begin{aligned}\mathbb{C}^{G(\mathbb{C},\mathbb{R})} &= \{z \in \mathbb{C} \mid \sigma(z) = z\ \forall \sigma \in G(\mathbb{C}, \mathbb{R})\} \\ &= \{z \in \mathbb{C} \mid z = \sigma_1(z) = z \textit{ and } \overline{z} = \sigma_2(z) = z\} \\ &= \mathbb{R}\end{aligned}$$

In this case, we get our starting field back.

2. $F = \mathbb{Q}$, $K = \mathbb{Q}(a)$ *where* $a = 2^{\frac{1}{3}}$. *Let* $\sigma \in G(K, F)$. *Since* $\sigma(x) = x\ \forall x \in \mathbb{Q}$, σ *is determined by* $\sigma(a)$.

$$\sigma(a)^3 = \sigma(a^3) = \sigma(2) = 2,$$

so $\sigma(a)$ *is a cube root of* 2. *Since* $\mathbb{Q}(a)$ *contains only real numbers, it contains only one cube root of* 2, *namely* a. *So* $\sigma(a) = a$ *and* σ *is the identity. Thus,*

$$G(\mathbb{Q}(2^{\frac{1}{3}}), \mathbb{Q}) = 1.$$

$\therefore \mathbb{Q}(2^{\frac{1}{3}})^{G(\mathbb{Q}(2^{\frac{1}{3}}),\mathbb{Q})} = \mathbb{Q}(2^{\frac{1}{3}})$, *which is strictly larger than* $\mathbb{Q}$.

Let $f(x) \in F[x]$ and let $G = G(K, F)$ where K is the splitting field of $f(x)$. Let $\alpha_1, \ldots, \alpha_n \in K$ be the roots of

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n \quad (c_j \in F).$$

Let $\sigma \in G(K, F)$, so $\sigma(c_j) = c_j$. Then

$$\begin{aligned}f(\sigma(\alpha_i)) &= c_0 + c_1\sigma(\alpha_i) + \cdots + c_n(\sigma(\alpha_i))^n \\ &= \sigma(c_0 + c_1 x + \cdots + c_n x^n) \\ &= \sigma(f(\alpha_i)) = \sigma(0) = 0.\end{aligned}$$

$\therefore \sigma(\alpha_i)$ is also a root of $f(x)$, ie. $\sigma(\alpha_i) = \alpha_{i'}$ for some $i' = 1, \ldots, n$. If $i \neq j$ then $\sigma(\alpha_i) \neq \sigma(\alpha_j)$, since σ is (1-1). So σ permutes the roots of $f(x)$. This map

$$\sigma \mapsto \sigma|_{\{\alpha_1,\ldots,\alpha_n\}}$$

is a group homomorphism $G \hookrightarrow S_n$.

Theorem 3.8.5. $|G(K, F)| \leq [K : F]$.

Proof. Let $[K : F] = n$ and let $u_1, \ldots, u_n$ be a basis for K over F. Suppose $G(K, F)$ has $n+1$ elements $\sigma_1, \ldots, \sigma_{n+1}$. Consider the system of equations

$$\begin{aligned}
\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \cdots + \sigma_{n+1}(u_1)x_{n+1} &= 0 \\
\sigma_1(u_2)x_1 + \sigma_2(u_2)x_2 + \cdots + \sigma_{n+1}(u_2)x_{n+1} &= 0 \\
&\vdots \\
\sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \cdots + \sigma_{n+1}(u_n)x_{n+1} &= 0.
\end{aligned}$$

This consists of n equations and $n+1$ variables, so $\exists$ a solution

$$x_1 = a_1,\ x_2 = a_2,\ \ldots,\ x_{n+1} = a_{n+1},$$

with not all $a_j = 0$. So, for all $j = 1, \ldots, n$,

$$a_1\sigma_1(u_j) + a_2\sigma_2(u_j) + \cdots + a_{n+1}\sigma_{n+1}(u_j) = 0.$$

Since $u_1, \ldots, u_n$ form a basis,

$$(a_1\sigma_1 + \cdots + a_{n+1}\sigma_{n+1})(t) = 0 \quad \forall t \in K.$$

But then $\sigma_1, \ldots, \sigma_{n+1}$ are linearly dependent in $\hom_{\text{abel. grps.}}(F, F)$, contradicting an earlier theorem.

Hence, $G(K, F)$ does not have $n+1$ elements, ie. $|G(K, F)| \leq [K : F]$. $\square$

3.9 Elementary Symmetric Polynomials

Let F be a field.
Notation:

$$\begin{aligned} F(x_1, \ldots, x_n) &:= \text{ field of fractions of } F[x_1, \ldots, x_n] \\ &= \left\{ \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} \mid p, q \in F[x_1, \ldots, x_n], q \neq 0 \right\} \end{aligned}$$

This is called the field of **rational functions** in n variables over F.

Let $K = F(x_1, \ldots, x_n)$. Given $\sigma \in S_n$, setting $\tilde{\sigma}(x_j) = x_{\sigma(j)}$ and $\tilde{\sigma}(a) = a\ \forall a \in F$ determines an automorphism of K s.t.

$$\sigma \in G(K, F) \subset \mathrm{Aut}(K).$$

In this way, S_n becomes a subgroup of $\mathrm{Aut}(K)$.

Let $S = K^{S_n}$. S is called the field of **symmetric rational functions** in n variables over F, and $S \cap F[x_1, \ldots, x_n]$ is called the ring of **symmetric polynomials** in n variables over F.

Definition 3.9.1. *Let*

$$s(t) = (t + x_1)(t + x_2) \cdots (t + x_n) \in F[x_1, \ldots, x_n][t].$$

*For $k = 1, \ldots, n$, the coefficient of t^{n-k} in $s(t)$ is called the k^{th} **elementary symmetric polynomial** in n variables, denoted $s_k(x_1, \ldots, x_n)$.*

For example:

$$\begin{aligned} s_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n \\ s_2(x_1, \ldots, x_n) &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots x_{n-1}x_n \\ s_3(x_1, \ldots, x_n) &= x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n \\ s_n(x_1, \ldots, x_n) &= x_1 \cdots x_n \end{aligned}$$

In general,

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Theorem 3.9.2.

1. $S = F(s_1, \ldots, s_n)$.

2. $[F(x_1, \ldots, x_n) : S] = n!$.

3. $G(F(x_1, \ldots, x_n), S) = S_n$.

4. $F(x_1, \ldots, x_n)$ *is the splitting field of* $s(t)$ *over* S.

Proof. $\sigma(s_k) = s_k\ \forall\sigma \in S_n$, so $F(s_1, \ldots, s_n) \subset S$. Conversely, $S_n \subset G(F(x_1, \ldots, x_n), S)$, so

$$[F(x_1, \ldots, x_n) : S] \geq |G(F(x_1, \ldots, x_n), S)| \geq |S_n| = n!.$$

$\therefore$ To show 1, 2 and 3, it suffices to show

$$[F(x_1, \ldots, x_n) : F(s_1, \ldots s_n)] \leq n!$$

since this simultaneously shows

$$[S : F(s_1, \ldots s_n)] = 1 \Rightarrow 1.$$

and

$$[F(x_1, \ldots, x_n) : S] = n! \Rightarrow 2.$$

and

$$|G(F(x_1, \ldots, x_n), S)| = n! \Rightarrow 3.$$

The polynomial

$$s(t) = (t + x_1)(t + x_2) \cdots (t + x_n)$$

factors linearly as shown in $F(x_1, \ldots, x_n)$. But its coefficients are $s_1, \ldots, s_n$, which lie in S. $s(t)$ cannot split in any proper subfield of $F(x_1, \ldots, x_n)$ since its roots are $-x_1, \ldots, -x_n$.

So $F(x_1, \ldots, x_n)$ is the splitting field of $s(t)$ over $F(s_1, \ldots, s_n)$. By an earlier corollary, the degree fo a splitting field extension of a polynomial of degree n is at most $n!$. Hence,

$$[F(x_1, \ldots, x_n) : F(s_1, \ldots, s_n)] \leq n!.$$

$\square$

3.10 The Galois Group

Let $F \subset K$ be a separable finite extension of fields. We observed earlier that $F \subset K^{G(K,F)}$.

Definition 3.10.1. *K is called a* ***normal extension*** *(or* ***Galois extension****) of F if $F = K^{G(K,F)}$.*

eg. $\mathbb{R} \subset \mathbb{C}$ is normal, $\mathbb{Q} \subset \mathbb{Q}(2^{\frac{1}{3}})$ is not.

Theorem 3.10.2. *Let $F \subset K$ be a normal extension and let H be a subgroup of $G(K,F)$. Then*

1. $[K : K^H] = |H|$.
2. $H = G(K, K^H)$.

Corollary 3.10.3. *If $F \subset K$ is normal then $[K : F] = |G(K,F)|$.*

Proof of corollary. Let $H = G(K,F)$. Then

$$[K : F] = [K : K^{G(K,F)}] = |G(K,F)|.$$

□

Proof of theorem. $\forall \sigma \in H, x \in K^H$, $\sigma(x) = x$. So $H \subset G(K, K^H)$. Thus

$$[K : K^H] \geq |G(K, K^H)| \geq |H|.$$

Since $F \subset K$ is separable, so is $K^H \subset K$. Hence, $\exists a \in K$ s.t. $K = K^H(a)$.

By an earlier theorem, the min. poly. of a has degree $[K : K^H]$. Let

$$H = \{\sigma_1, \ldots, \sigma_h\},$$

where $\sigma_1 = 1$. Let

$$s_1(x_1, \ldots, x_h), \ldots, s_h(x_1, \ldots, x_h)$$

be the elementary symmetric polynomials in h variables. Let

$$\alpha_j = s_j(\sigma_1(a), \sigma_2(a), \ldots, \sigma_h(a)) \in K.$$

Let

$$p(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \ldots (x - \sigma_h(a)) = x^h - \alpha_1 x^{h-1} + \alpha_2 x^{h-2} + \cdots + (-1)^h \alpha_h \in K[x].$$

In any group, left multiplication by any element permutes the elements of the group. By construction, each α_j is invariant under permutations of the σ's. So for all j, $\sigma(\alpha_j) = \alpha_j$ $\forall \sigma \in H$, so $\alpha_j \in K^H$. Hence $p(x) \in K^H[x]$. Since $a = \sigma_1(a)$ is a root of $p(x)$,

$$|H| = h = \deg p(x) \geq \deg(\text{min. poly. of } a \text{ over } K^H) = [K : K^H].$$

$\therefore |H| = |G(K, K^H)| = [K : K^H]$, showing 1, and also $H \subset G(K, K^H)$, showing 2. □

Theorem 3.10.4. *Suppose K is separable over F. Then $F \subset K$ is a normal extension $\iff$ K is the splitting field of some polynomial in F.*

Proof.

$\Rightarrow$: Suppose $F \subset K$ is a normal extension. $K = F(a)$ for some $a \in K$. Let

$$G(K, F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\},$$

where $\sigma_1 = 1$. Let

$$\begin{aligned} p(x) &= (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a)) \\ &= x^n - \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + (-1)^n \alpha_n, \end{aligned}$$

where $\alpha_j = s_j(\sigma_1(a), \ldots, \sigma_n(j)) \in K$. As in the preceding proof, $\sigma(\alpha_j) = \alpha_j \ \forall \sigma \in G(K, F)$, so

$$\alpha_j \in K^{G(K,F)} = F,$$

by normality.

So $p(x) \in F[x]$ and $p(x)$ splits in K. $a = \sigma_1(a)$ is a root of $p(x)$. By defn. of $F(a)$, a lies in no proper subfield of $K = F(a)$ which contains F. So $p(x)$ does not split in any subfield of K. Thus, K is the splitting field of $p(x)$.

$\Leftarrow$: Let K be the splitting field of some $f(x) \in F[x]$.

Lemma 3.10.5. *Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ and let $\alpha_1, \ldots, \alpha_r \in K$ be the roots of $p(x)$. Then $\forall j = 1, \ldots, r$, $\exists \sigma_j \in G(K, F)$ s.t. $\sigma_j(\alpha_1) = \alpha_j$.*

Proof of lemma. By Theorem 3.3.13, $\exists$ an isomorphism

$$\tau_j : F(\alpha_1) \overset{\cong}{\longmapsto} F(\alpha_j)$$

s.t. $\tau_j(\alpha_1) = \alpha_j$ and $\tau_j(z) = z \ \forall z \in F$. Hence, $\tau_j(f(x)) = f(x)$.

K can be regarded as the splitting field of $f(x)$ over both $F(\alpha_1)$ and $F(\alpha_j)$. So by Theorem 3.3.15, τ_j can be extended to

$$\sigma_j : K \overset{\cong}{\longmapsto} K.$$

Since σ_j extends τ_j, $\sigma_j \in G(K, F)$ and $\sigma_j(\alpha_1) = \alpha_j$, as required. $\square$

Proof of theorem (continued). Assume by induction that if K_1 is the splitting field of some polynomial $f_1 \in F_1[x]$ and $[K_1 : F_1] < [K : F]$ then K_1 is normal over F_1. If $[K_1 : F_1] = 1$ then $K_1 = F_1$ is normal over F_1, to start induction.

So suppose $[K : F] > 1$. Then $f(x)$ has a non-linear irreducible factor $p(x)$. Let

$$\deg p(x) = r > 1.$$

Let $\alpha_1, \ldots, \alpha_r \in K$ be the roots of $p(x)$. Regarding K as the splitting field of $f(x)$ over $F(\alpha_1)$, induction implies that K is a normal extension of $F(\alpha_1)$. Show $K^{G(K,F)} = F$.

$F \subset F(\alpha_1)$, so $G(K, F(\alpha_1)) \subset G(K, F)$. ie. $\sigma \in G(K, F(\alpha_1)) \Rightarrow \sigma(z) = z \; \forall z \in F(\alpha_1)$, and in particular, $\sigma(z) = z \; \forall z \in F$. Thus,

$$K^{G(K,F)} \subset K^{G(K,F(\alpha_1))} = F(\alpha_1),$$

because $F(\alpha_1) \in K$ is normal.

Let $z \in K^{G(K,F)}$. We must show $z \in F$. Since $z \in F(\alpha_1)$,

$$z = \lambda_0 + \lambda_1\alpha_1 + \cdots + \lambda_{r-1}\alpha^{r-1},$$

for some $\lambda_0, \ldots, \lambda_{r-1} \in F$. For $j = 1, \ldots, r$, choose $\sigma_j \in G(K, F)$ s.t. $\sigma(\alpha_1) = \alpha_j$. Then

$$z = \sigma_j(z) = \lambda_0 + \lambda_1\alpha_j + \cdots + \lambda_{r-1}\alpha_j^{r-1}$$

Let

$$q(x) = \lambda_{r-1}x^{r-1} + \cdots + \lambda_1 x + (\lambda_0 - z) \in K[x]$$

Then α_j is a root of $q(x) \; \forall j = 1, \ldots, r$. But $\deg q(x) \leq r - 1$ and $\alpha_1, \ldots, \alpha_r$ are distinct. This is a contradiction unless all coefficients of $q(x)$ are zero. In particular, $z = \lambda_0 \in F$.

□

Definition 3.10.6. *Let $f(x) \in F[x]$. Let K be the splitting field of f over F and suppose that K is separable over F. The **Galois group** of $f(x)$ over F is $G(K, F)$. This will sometimes be denoted* $\mathrm{Gal}(f(x))$.

Theorem 3.10.7 (Fundamental Theorem of Galois Theory)**.** *Let $f(x) \in F$. Let $K \supset F$ be the splitting field of $f(x)$ over F. Suppose K is separable over F and let $G = G(K, F)$ be the Galois group of $f(x)$ over F. Then the associations*

$$M \rightsquigarrow G(K, M)$$
$$K^H \leftsquigarrow H$$

set up a bijection between fields M s.t. $F \subset M \subset K$ and subgroups of G. It has the following properties:

1. $M = K^{G(K,M)}$.
2. $H = G(K, K^H)$.
3. $[K : M] = |G(K, M)|$, *and* $[M : F] = G : G(K, M)$ *(the index of the subgroup* $G(K, M)$ *in* G*).*
4. M *is a normal extension of* $F \iff G(K, M)$ *is a normal subgroup of* G.
5. *If* M *is a normal extension of* F *then* $G(M, F) \cong G/G(K, M)$.

Proof.

1. K is the splitting field of $f(x)$ over F, so F can be regarded as the splitting field of $f(x)$ over M. So $M \subset K$ is normal, ie. $M = K^{G(K,M)}$.

2. This is just Theorem 3.10.2. 1 and 2 say that the associations are inverse bijections.

3.
$$\begin{aligned} |G(K, M)| &= [K : K^{G(K,M)}] \quad \text{by Theorem 3.10.2} \\ &= [K : M] \quad \text{by 1.} \end{aligned}$$
and
$$[M : F] = \frac{[K : F]}{[K : M]} = \frac{|G(K, F)|}{|G(K, M)|} = G : G(K, M).$$

4.
Lemma 3.10.8. *M is normal $\iff \sigma(M) \subset M \ \forall \sigma \in G$.*

Proof of lemma.

$\Rightarrow$: Suppose M is normal. Let $\sigma \in G$. Let $q(x) \in F[x]$ be a polynomial whose splitting field is M. So in M,
$$q(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r).$$
By an earlier proposition, $M = F(\alpha_1, \alpha_2, \ldots, \alpha_r)$. Since $\sigma \in G$,
$$q(\sigma(\alpha_j)) = \sigma(q(\alpha_j)) = \sigma(0) = 0.$$
$\therefore \sigma(\alpha_j)$ is a root of $q(x)$. But M contains the full set of roots of $q(x)$, so $\sigma(\alpha_j) \in M$. Thus, $\sigma(M) \subset M$.

$\Leftarrow$: Suppose $\sigma(M) \subset M\ \forall \sigma \in G$. Let $z \in M^{G(M,F)}$, and check that $z \in F$. Let $\sigma \in G$. Since $\sigma(M) \subset M$, $\sigma|_M \in G(M, F)$. So,

$$\sigma(z) = \sigma|_M(z) = z,$$

since $z \in M^{G(M,F)}$. So $z \in M^G \subset K^G = F$.

$\square$

Proof of 4.

$\Rightarrow$: Suppose M is a normal extension of F. Let $\sigma \in G, \tau \in G(K, M)$. Then $\forall m \in M$,

$$\begin{aligned} \sigma^{-1}\tau\sigma(m) &= \sigma^{-1}\tau(\sigma(m)) \\ &= \sigma^{-1}\sigma(m), \quad \text{since } \sigma(m) \in M \text{ and } \tau|_M = \mathrm{id} \\ &= m. \end{aligned}$$

$\therefore \sigma^{-1}\tau\sigma \in G(K, M)$. Hence $G(K, M)$ is a normal subgroup of G.

$\Leftarrow$: Suppose $G(K, M)$ is a normal subgroup of G. Let $\sigma \in G, z \in M$. Then $\forall \tau \in G(K, M)$, $\sigma^{-1}\tau\sigma \in G(K, M)$, so

$$\sigma^{-1}\tau\sigma(z) = z.$$

$\therefore \tau\sigma(z) = \sigma(z)$. Thus $\sigma(z) \in K^{G(K,M)} = M$ (by 1). So $\sigma(M) \subset M$ and M is normal over F by the lemma.

5. Suppose M is normal over F. Given $\sigma \in G(K, F)$, define $\psi(\sigma) = \sigma|_M$. By the lemma,

$$\sigma(M) \subset M,$$

so $\psi(\sigma) \in G(M, F)$. If $\sigma \in \ker\psi$ then $\sigma|_M = \mathrm{id}_M$, ie. $\sigma \in G(K, M)$. Hence, $\ker\psi = G(K, M)$. So by 1st isomorphism theorem,

$$G/G(K, M) = G/\ker\psi \cong \mathrm{Im}\psi \subset G(M, F).$$

But $|G/G(K, M)| = [M : F] = |G(M, F)|$, so

$$G/G(K, M) \cong G(M, F).$$

$\square$

Theorem 3.10.9. *Let $F \subset K$ be an extension field. Let $f(x) \in F[x]$. Then the Galois group of $f(x)$ over K is isomorphic to a subgroup of the Galois group of $f(x)$ over F.*

Proof. Let L be the splitting field of $f(x)$ over K and E the splitting field of $f(x)$ over F. Since $f(x)$ splits in L, $E \subset L$. Let $r_1, \ldots, r_n \in E$ be the roots of $f(x)$.

For $\sigma \in G(L, K)$, σ is determined by its action on $r_1, \ldots, r_k$. Define $\psi : G(L, K) \mapsto G(E, F)$ by $\psi(\sigma) = \sigma|_E$. If $\psi(\sigma) = \psi(\tau)$ then $\sigma|_E = \tau|_E$, so

$$\sigma(r_j) = \tau(r_j) \quad \forall j.$$

$\therefore \sigma = \tau$. Hence ψ is a monomorphism. □

Example 3.10.10. *Let E be the finite field with p^n elements, which was shown to be the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Define $\phi \in \mathrm{Aut}(E)$ by*

$$\phi(x) = x^p.$$

Then it is clear that the automorphisms $\phi, \phi^2, \ldots, \phi^n = \mathrm{id}$ are distinct. But $|G(E, \mathbb{F}_p)| = [E : \mathbb{F}_p] = n$, and thus,

$$G(E, \mathbb{F}_p) = \{\phi, \phi^2, \ldots, \phi^n\}.$$

In particular, this shows that $G(E, \mathbb{F}_p)$ is cyclic.

3.11 Constructions with Ruler and Compass

Let $S \subset \mathbb{C} \cong \mathbb{R}^2$ be a finite subset. Let

$$S' := \{z \in \mathbb{C} \mid z \text{ can be constructed from the points of } S \text{ using a ruler and compass}\}.$$

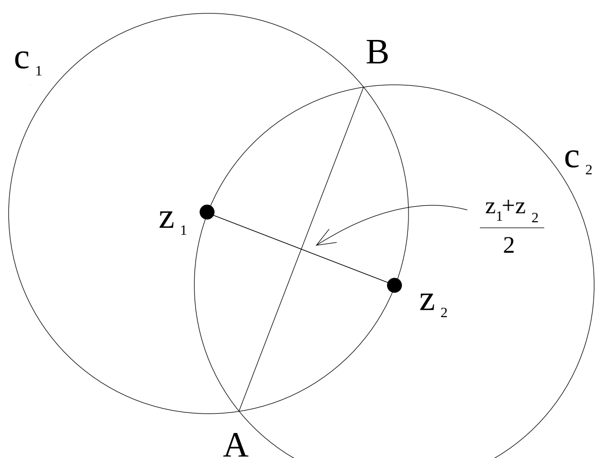
More precisely:
Let $S_0 = S$. Using a ruler and compass, we can join pts. in S_0 with lines or can construct circles centred at a point in S_0 and passing through another point in S_0. Let $\tilde{S}_0$ be the set of points which are the intersections of these lines and circles.
Let $S_1 = S_0 \cup \tilde{S}_0, S_2 = S_1 \cup \tilde{S}_1, \ldots, S_n = S_{n-1} \cup \tilde{S}_{n-1}$. Then let

$$S' = \bigcup_n S_n.$$

Let $P_0 = 0 = (0,0), P_1 = 1 = (1,0)$. Let $F = \{P_0, P_1\}'$. We say z is **constructible** if $z \in F$. Show F is a field.

Proposition 3.11.1. *If $z_1, z_2 \in S'$ then $\frac{z_1+z_2}{2} \in S'$.*

Proof.



Let $c_1 := C_{z_1}(z_2)$, the circle centred at z_1 through z_2, and let $c_2 := C_{z_2}(z_1)$. Let A, B be the two intersection points of c_1 and c_2. Then $L(A, B)$, the line through A and B, intersects $L(z_1, z_2)$ at $\frac{z_1+z_2}{2}$. □

Proposition 3.11.2. *If $z_1, z_2 \in F$ then $z_1 + z_2 \in F$.*

Proof. $C_{\frac{z_1+z_2}{2}}(0)$ meets $L\left(0, \frac{z_1+z_2}{2}\right)$ at $z_1 + z_2$ (and 0). □

Proposition 3.11.3. *If $z \in F$ then $-z \in F$.*

Proof. Intersect $L(0,z)$ with $C_0(z)$. ◻

Proposition 3.11.4. $z = (x,y) \in F \iff (x,0) \in F$ *and* $(0,y) \in F$.

Proof.

⇒: Suppose $z = (x,y) \in F$. $C_z(0)$ meets $L(0,P_1)$ at $(2x,0)$, so $(2x,0) \in F$. By Prop. 3.11.1, $(x,0) \in F$. Hence also,
$$(0,y) = (x,y) - (x,0) \in F.$$

⇐: If $(x,0),(0,y) \in F$ then by Prop. 3.11.2,
$$(x,y) = (x,0) + (0,y) \in F.$$

◻

Let
$$\mathcal{L} := \{\text{lines joining two points in } F\}.$$

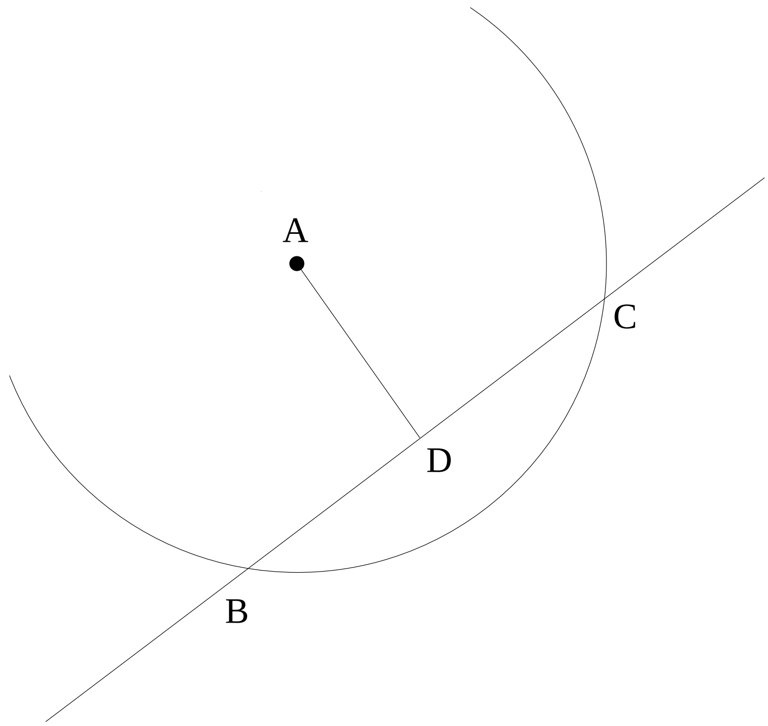
Proposition 3.11.5. *Let $L \in \mathcal{L}, A \in F$. Then the line parallel to L through A lies in $\mathcal{L}$.*

Proof. Let $P, Q \in F$ be distinct points lying on L. Let
$$R = P - Q + A \in F.$$
Then the line parallel to L through A is $L(A,R)$. ◻

Proposition 3.11.6. *Let $L \in \mathcal{L}, A \in F$. Then the line through A perpendicular to L lies in $\mathcal{L}$.*

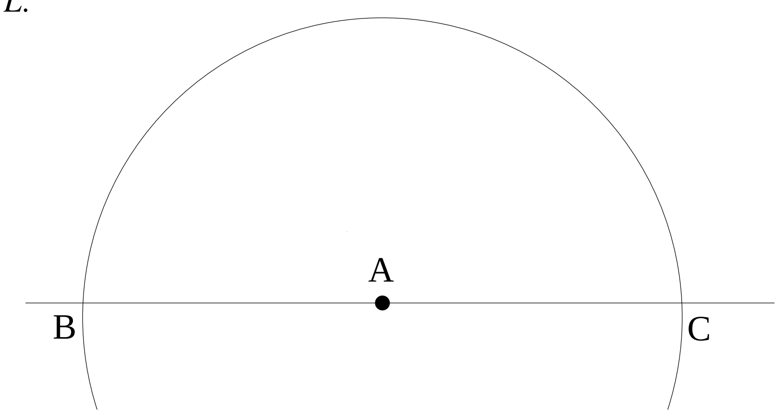
Proof.

Case 1: $A \notin L$. Let C be the other point where $C_A(B)$ meets L and let $D = \frac{B+C}{2}$. (If $C_A(B)$ happens to be tangent to L at B then let $D = B$).



Then $D \in F$ and $L(A, D)$ is the line perependicular to BC through A.

Case 2: $A \in L$. Since L has at least two points of F, let $A \neq B \in L$. Let C be the other point where $C_A(B)$ meets L.



Then $A = \frac{B+C}{2}$ and the construction of Prop. 3.11.1 produces the line through A perpendicular to L.

$\square$

Proposition 3.11.7. *Let $z = re^{i\theta}$. Then $z \in F \iff r \in F$ and $e^{i\theta} \in F$.*

Proof.

⇒: Suppose $z \in F$. $C_0(z)$ meets $L(0, P_1)$ at $(r, 0)$, ie. $r \in F$. $e^{i\theta}$ is the point where $L(0, re^{i\theta})$ crosses $C_0(P_1)$. Hence $e^{i\theta} \in F$.

⇐: Let $r \in F$ and $e^{i\theta} \in F$. Then $re^{i\theta}$ is the point where $L(0, e^{i\theta})$ meets the circle centred at 0 through $(r, 0)$.

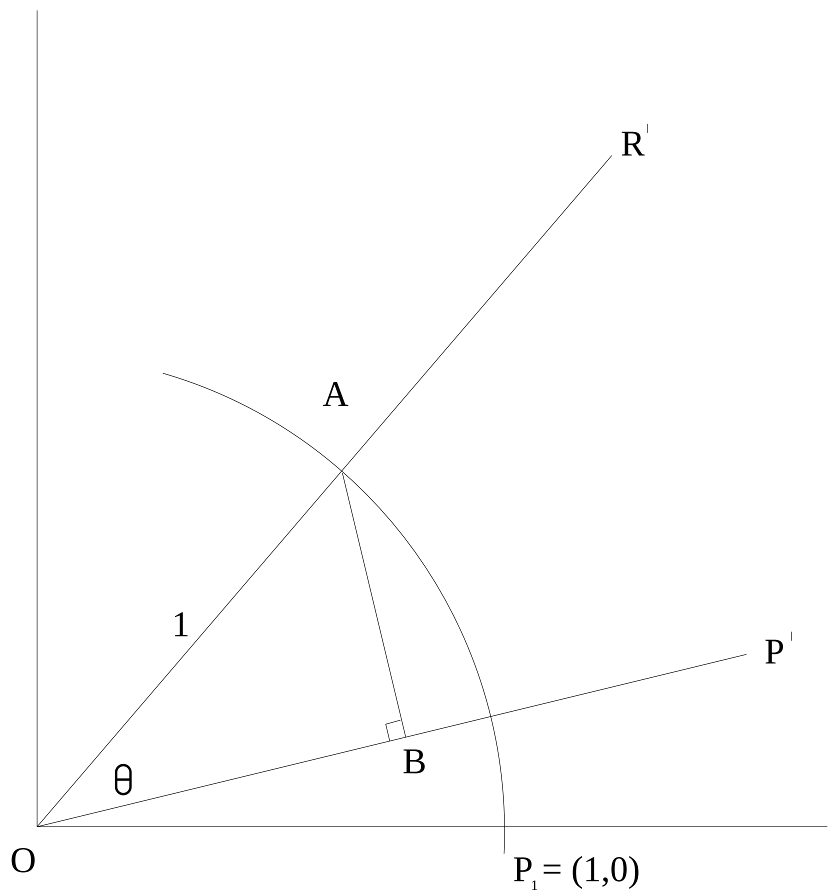
□

Proposition 3.11.8. $\exists P, Q, R \in F$ *s.t.* $\angle PQR = \theta \iff e^{i\theta} \in F$.

Proof.

⇒: Suppose $P, Q, R \in F$ s.t. $\angle PQR = \theta$. Let

$$P' = P - Q, R' = R - Q \in F.$$



Let A be the point where $C_0(P_1)$ meets $L(0, R')$. Let B be the point where the perpendicular to $L(0, P')$ through A meets $L(O, P')$. Then

$$\cos\theta = |0B| \in F.$$

Also, letting $z = A - B$,

$$\sin\theta = |AB| = |z| \in F.$$

Then the y-axis is in $\mathcal{L}$ by Prop. 3.11.6, and $i\sin\theta$ is the point where $C_0(\sin\theta)$ meets the y-axis, whence $i\sin\theta \in F$. So

$$e^{i\theta} = \cos\theta + i\sin\theta \in F.$$

$\Leftarrow$: Suppose $e^{i\theta} \in F$. Let

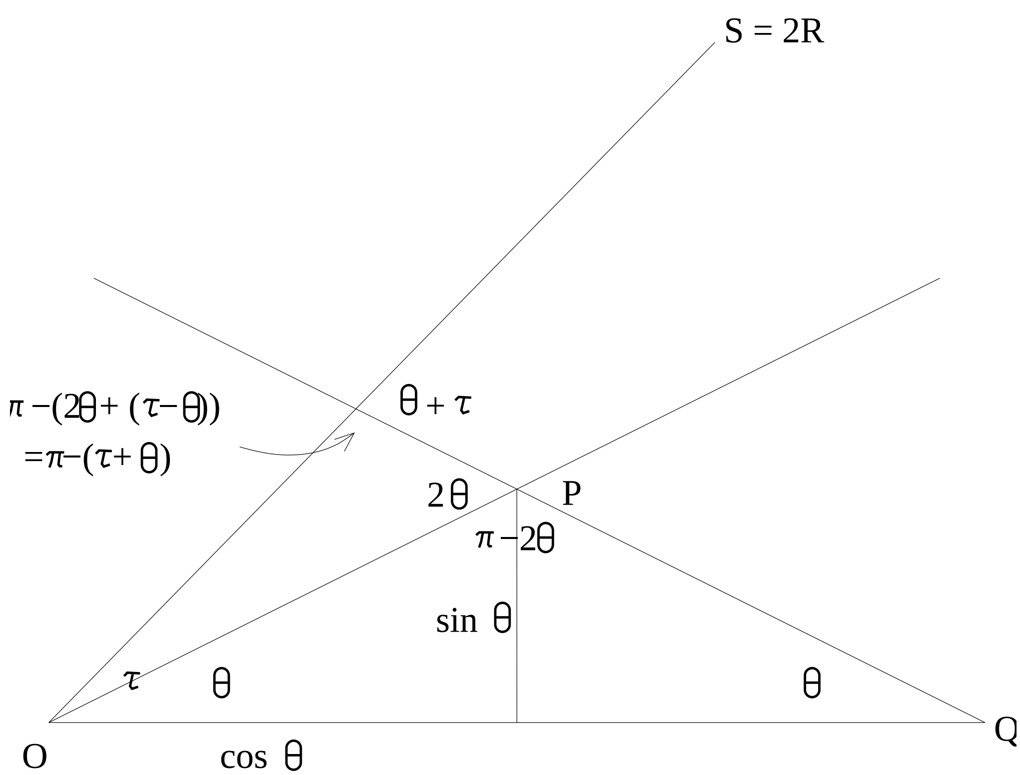
$$P = (0, 1), \quad Q = 0, \quad R = e^{i\theta} = (\cos\theta, \sin\theta).$$

Then $\angle PQR = \theta$.

□

Proposition 3.11.9. *Let* $(\cos\theta, \sin\theta) \in F$ *and* $(\cos\tau, \sin\tau) \in F$. *Then* $(\cos(\theta+\tau), \sin(\theta+\tau)) \in F$.

Proof.



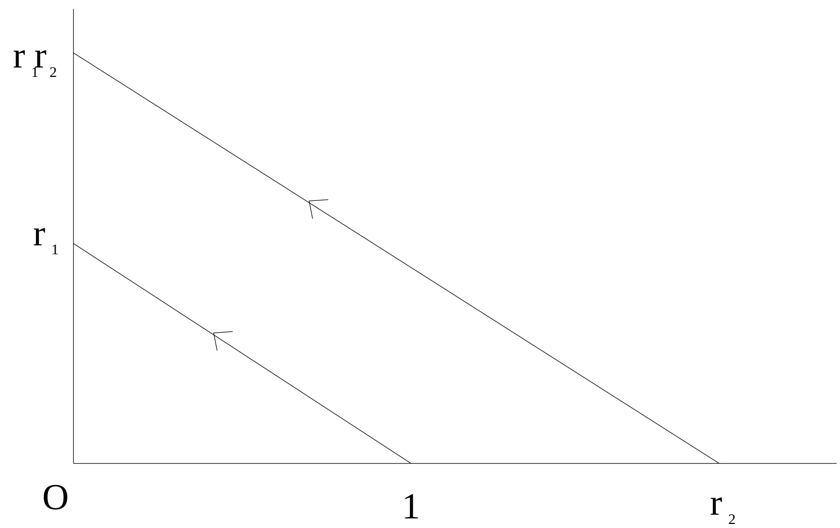
Let $P = (\cos\theta, \sin\theta)$, so $(\cos\theta, 0) \in F$. Let $Q = (2\cos\theta, 0) \in F$. Let R be the point where $L(Q, P)$ meets the line joining 0 to $(\cos\tau, \sin\tau)$. Let $S = 2R$. Then $Q, R, S \in F$ and $\angle QRS = \theta + \tau$. So

$$(\cos(\theta + \tau), \sin(\theta + \tau)) \in F.$$

□

Proposition 3.11.10. *If $z_1, z_2 \in F$ then $z_1 z_2 \in F$.*

Proof. Let $z_1 = r_1 e^{i\theta_1}$, z_2 $r_2 e^{i\theta_2}$. Then $z_1 \in F \Rightarrow (r_1, 0) \in F$ and $z_2 \in F \Rightarrow (r_2, 0) \in F$.



The line joining $(r_1, 0)$ to $(0, r_1 r_2)$ is parallel to that joining $(1, 0)$ to $(0, r_2)$, so it lies in $\mathcal{L}$. Hence, its intersection with the y-axis lies in F, ie. $(0, r_1 r_2) \in F$.

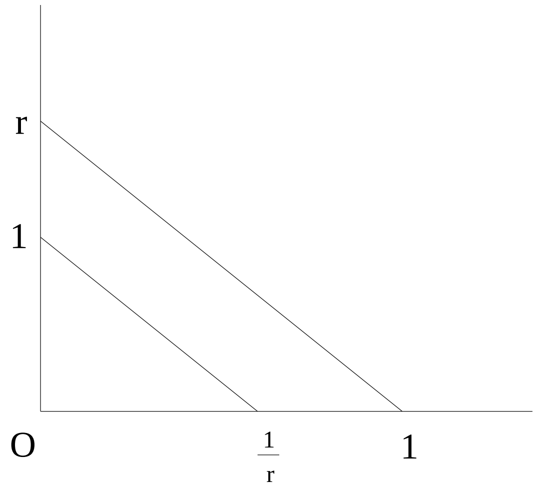
$z_1 \in F \Rightarrow (\cos\theta_1, \sin\theta_1) \in F$ and $z_2 \in F \Rightarrow (\cos\theta_2, \sin\theta_2) \in F$ by Prop. 3.11.7. So by Prop. 3.11.9,

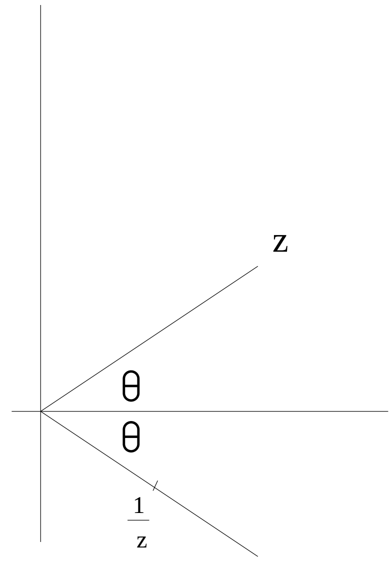
$$P = (\cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2)) \in F.$$

$L(0, P)$ meets the circle centred at 0 through $(0, r_1 r_2)$ at $z_1 z_2$. □

Proposition 3.11.11. *If $z \in F$ then $\frac{1}{z} \in F$.*

Proof. Let $z = re^{i\theta}$.





As above, $z \in F \Rightarrow\ (0, r) \in F \Rightarrow$ the line joining $(1, 0)$ to $(0, r)$ lies in $\mathcal{L}$. So the line joining $(\frac{1}{r}, 0)$ to $(0, 1)$ lies in $\mathcal{L}$, and thus, $(\frac{1}{r}, 0) \in F$.

$e^{i\theta} \in F$, so by Props. 3.11.3 and 3.11.4, $e^{-i\theta} \in F$. By Prop. 3.11.10,

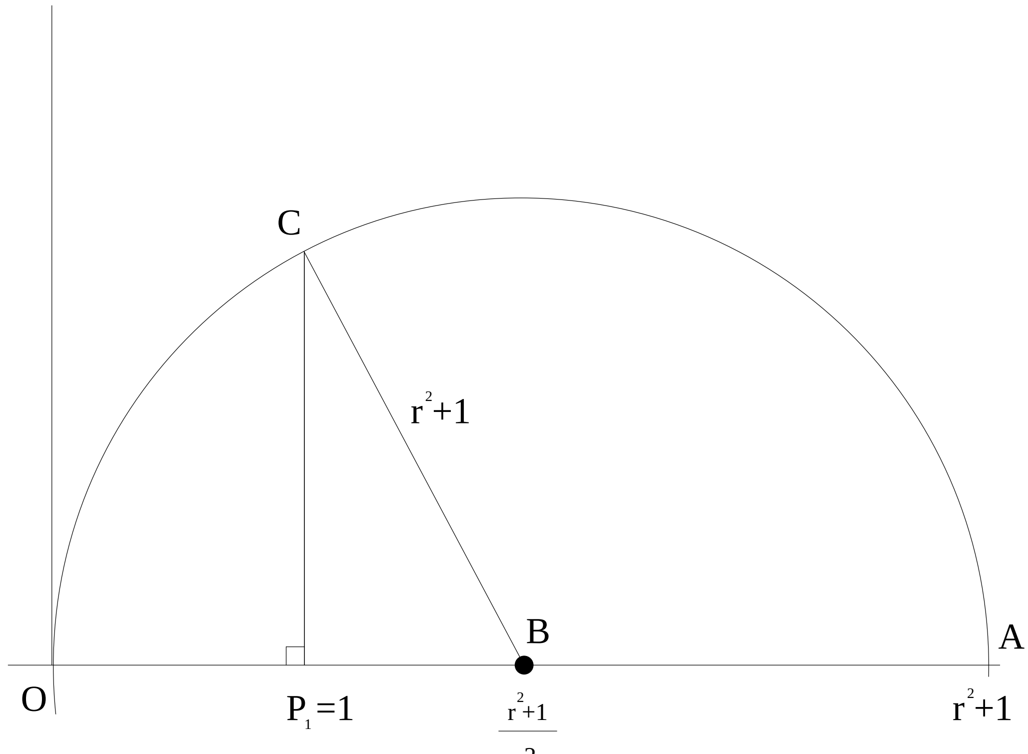
$$\frac{1}{z} = \frac{1}{r}e^{-i\theta} \in F.$$

□

Thus, F is a field.

Proposition 3.11.12. *If $z^2 \in F$ then $z \in F$.*

Proof. $z = \left(\frac{z+1}{2}\right)^2 - \left(\frac{z-1}{2}\right)^2$.



Let $z = re^{i\tau}$, so $z^2 = r^2 e^{i2\tau} \in F$. Then $(r^2, 0) \in F$ so $A = (r^2, 0) + (1, 0) \in F$. Let $B = \frac{A}{2} \in F$. Let C be the point where $C_B(A)$ meets the perpendicular to $L(0, A)$ through $(1, 0)$. By Pythagoras,

$$|P_1C|^2 = |BC|^2 - |P_1B|^2 = \left(\frac{r+1}{2}\right)^2 - \left(\frac{r-1}{2}\right)^2.$$

$\therefore C = (1, r)$ so $r \in F$.

Let $\theta = 2\tau$. $r^2 e^{2i\tau} \in F \Rightarrow e^{i2\tau} \in F$, ie. $Q = (\cos\theta, \sin\theta) \in F$. Let

$$\begin{aligned} S &= Q - P_1 \\ &= (\cos 2\tau - 1, \sin 2\tau) \\ &= (2\cos^2\tau, 2\cos\tau\sin\tau) \\ &= 2\cos\tau(\cos\tau, \sin\tau). \end{aligned}$$

So, if $\cos\tau \neq 0$ then $\angle P_1 0 S = \tau$, ie. $L(0, S)$ bisects $\angle P_1 0 Q$. If $\cos\tau = 0$ then $\tau = \pm\frac{\pi}{2}$ and it is obvious that a line with angle τ is in $\mathcal{L}$. The circle centred at 0 passing through $(r, 0)$ meets this line at $re^{i\tau} \in F$. $\square$

Theorem 3.11.13. *F is the smallest subfield of $\mathbb{C}$ which is closed under square roots and complex conjugation.*

Proof. By earlier propositions, F is closed under square roots and complex conjugation. Conversely, let K be a subfield of $\mathbb{C}$ closed under square roots and complex conjugation. Since $S_0 = \{0, 1\} \in K$, if we can show that $K' = K$, it will follow that $F \subset K$.

Lemma 3.11.14. *The equation of a line joining two points in K can be written in the form*

$$ax + by = c$$

where $a, b, c \in K \cap \mathbb{R}$.

Proof. Let L join $P = (p_1, p_2)$ to $Q = (q_1, q_2)$, where $p_1, p_2, q_1, q_2 \in K \cap \mathbb{R}$. (Since K is closed under complex conjugation, it is clear that this can be done for any elements $P, Q \in K$). Then L has the equation

$$(q_1 - p_1)(y - p_2) = (q_2 - p_2)(x - p_1),$$

which has the desired form. □

Lemma 3.11.15. *The equation for a circle centred at a point of K passing through another point of K can be written in the form*

$$x^2 + y^2 + ax + by + c = 0$$

where $a, b, c \in K \cap \mathbb{R}$.

Proof. Let C be the circle centered at $P = (p_1, p_2)$ passing through $Q = (q_1, q_2)$., where $p_1, p_2, q_1, q_2 \in K \cap \mathbb{R}$. Then the radius of C is

$$r = \sqrt{(q_2 - p_q)^2 + (q_1 - p_1)^2} \in K \cap \mathbb{R}.$$

So C has the equation

$$(x - p_1)^2 + (y - p_2)^2 = r^2,$$

which has the desired form. □

Proof of Theorem (continued).

1. The intersection of $ax + by = c, a'x + b'y = c'$ is the solution of the simultaneous equations, which is given by a quotient of determinants involving a, b, c, a', b', c'. So the intersection is $z = (p, q)$ where $p, q \in K \cap \mathbb{R}$. Hence $z = p + iq \in K$.

2. The intersection(s) of $ax + by = c$ and $x^2 + y^2 + a'x + b'y + c' = 0$:

$$x^2 + \left(\frac{c - ax}{b}\right)^2 + a'x + b'\left(\frac{c - ax}{b}\right) + c' = 0.$$

(consider $b = 0$ separately: exercise). This is a quadratic, so if there is a solution then by quadratic formula, it lies in $K \cap \mathbb{R}$. Similarly, the solution for y lies in $K \cap \mathbb{R}$.

3. Intersection(s) of $x^2 + y^2 + ax + by + c = 0$ and $x^2 + y^2 + a'x + b'y + c' = 0$:
   By subtracting the equations, get
$$(a - a')x + (b - b')y + c - c' = 0$$
   so the intersection pts. are the same as that of the line $(a - a')x + (b - b')y + c - c' = 0$ and the circle $x^2 + y^2 + ax + by + c = 0$, which transposes into case 2.

□

Theorem 3.11.16. *If $z \in F$ then z is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of* 2.

Proof. By the last theorem, if $z \in F$ then we can create a field K s.t. $z \in K$ by a finite number of extensions, each of which adjoins the square root of some element. That is,
$$\mathbb{Q} \subset \mathbb{Q}(z) \subset K$$
where $\mathbb{Q} \subset K$ is a composition of some sequence of degree 2 extensions. So
$$[K : \mathbb{Q}] = 2^t$$
for some t, and $[\mathbb{Q}(z) : \mathbb{Q}]$ divides 2^t, so it is a power of 2. □

Example 3.11.17. *It is impossible by ruler and compass to trisect* $60°$.

Proof. Using earlier techniques, we can construct equilateral triangles and thus $\cos 60°, \sin 60° \in F$. If $60°$ could be trisected, then $\alpha = \cos 20°$ would be in F.

In general,
$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$
For $\theta = 20°$, $\cos 3\theta = \cos 60 = \frac{1}{2}$. So
$$\frac{1}{2} = 4\alpha^3 - 3\alpha$$
or
$$8\alpha^3 - 6\alpha - 1 = 0.$$
But $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$, so
$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3,$$
which is not a power of 2. Hence $\alpha \notin F$. So $60°$ cannot be trisected using ruler and compass. □

Example 3.11.18. *It is impossible by ruler and compass to "double" the cube (ie. to construct a cube whose volume is twice that of a given cube). (Historically, this was called "duplicating" the cube).*

Proof. Suppose the volume of the original cube is 1. Then the length of the edge of the new cube is $2^{\frac{1}{3}}$, whose min. poly. is $x^3 - 2$. Since 3 is not a power of 2, $2^{\frac{1}{3}}$ is not constructible, so we cannot duplicate the cube. □

3.12 Solvability by Radicals

$g(x) = x^2 + bx + c \Rightarrow x = \frac{-b \pm \sqrt{b^2-4c}}{2}$. So if $b, c \in \mathbb{Q}$, then we can form the splitting field of $f(x)$ by adjoining to $\mathbb{Q}$ the square root of some elt. of $\mathbb{Q}$.

$g(x) = x^3 + ax^2 + bx + c$. We shall see, $\exists$ a formula where, by successively adding roots (cube roots and square roots) to our field, we can produce the splitting field of $g(x)$. $\exists$ a similar formula for quartics.

Given a field F and a polynomial $p(x) \in F[x]$, we say that $p(x)$ is **solvable by radicals** over F if we can find a sequence of fields satisfying:

$$\begin{aligned} F_0 &= F \\ F_1 &= F_0(w_1) \quad \text{where } w_1^{r_1} \in F_0 \text{ for some } r_1 \\ F_2 &= F_1(w_2) \quad \text{where } w_2^{r_2} \in F_1 \text{ for some } r_2 \\ &\vdots \\ F_n &= F_{n-1}(w_n) \quad \text{where } w_n^{r_n} \in F_{n-1} \text{ for some } r_n \end{aligned}$$

such that $p(x)$ splits in F_n. (We do not require that F_n be the splitting field of $p(x)$; it could be larger. Thus, F_n might not be normal.)

Let $F = K(a_1, \ldots, a_n)$ be the field of fractions in n variables. The general polynomial of degree n over K,

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

can be regarded as an elements of $F[x]$. Finding a "formula" involving roots for the general polynomial of degree n over K means showing that $p(x) \in F[x]$ is solvable by radicals. We shall show that that this is not true if $n \geq 5$.

Note: This does not mean that it is impossible for some specific 5^{th} degree polys. in $K[x]$ to be solvable by radicals.

Theorem 3.12.1. *Suppose* char $F = 0$. *Let* $p(x) = x^n - 1 \in F[x]$. *Then* $F\left(e^{\frac{2\pi i}{n}}\right)$ *is the splitting field of* $p(x)$ *over* F, *and the Galois group of* $p(x)$ *over* F *is abelian.*

Proof. Let $w = e^{\frac{2\pi i}{n}}$. Then all roots of $p(x)$ are powers of w, so $F(w)$ is the splitting field for $p(x)$ over F.

Let $\sigma, \tau \in G = G(F(w), F)$. σ is determined by $\sigma(w)$, since $\sigma(f) = f \; \forall f \in F$. $\sigma(w)$ is a root of $x^n - 1$, so let

$$\sigma(w) = w^j, \quad \text{for some } j.$$

Similarly,

$$\tau(w) = w^k, \quad \text{for some } k.$$

So

$$\sigma\tau(w) = \sigma(w^k) = (\sigma(w))^k = (w^j)^k = w^{jk} = \tau\sigma(w).$$

ie. $\sigma\tau = \tau\sigma$. So G is abelian. $\square$

Theorem 3.12.2. *Suppose* char $F = 0$ *and suppose* $w = e^{\frac{2\pi i}{n}} \in F$. *Let* u *be a root of* $p(x) = x^n - a$ *lying in an extension field of* F. *Then* $F(u)$ *is the splitting field of* $p(x)$ *over* F *and the Galois group of* $x^n - a$ *over* F *is cyclic, with order dividing* n.

Proof. Let $F \subset K$ be an extension s.t. $u \in K$. Then the n roots of $x^n - a$ are

$$u, wu, w^2u, \ldots, w^{n-1}u,$$

which all lie in $F(u)$. So $F(u)$ is the splitting field of $p(x)$ over F.

Let $G = G(F(u), F)$. Let $\sigma \in G$. Then $\sigma(u)$ is a root of $p(x)$, so $\sigma(u) = w^j u$ for some j, and σ is determined by $\sigma(u)$. Define $\psi : G \mapsto \mathbb{Z}/n\mathbb{Z}$ by

$$\psi(\sigma) = j \quad \text{where } \sigma(u) = w^j u.$$

If $\psi(\tau) = k$ then

$$\sigma\tau(u) = \sigma(w^k u) = \sigma(w^k)\sigma(u) = w^k w^j u = w^{j+k}u.$$

$\therefore \psi(\sigma\tau) = j + k = \psi(\sigma) + \psi(\tau)$, so ψ is a group homomorphism. If $\psi(\sigma) = \psi(\tau)$ then $\sigma(u) = \sigma(\tau)$ and thus $\sigma = \tau$. Hence ψ is a monomorphism. Thus,

$$G \cong \text{subgroup of a cyclic group of order } n,$$

so G is cyclic with order dividing n. $\square$

Theorem 3.12.3. *Let* p *be prime. Suppose* $\exists p$ *distinct elts.* $z_1, \ldots, z_n \in F$ *s.t.*

$$z_j^p = 1 \quad \forall j.$$

Let $F \subset E$ *be normal s.t.* $G = G(E, F)$ *is cyclic of order* p. *Then* $E = F(u)$ *where* $u^p \in F$.

Proof. Let $c \in E - F$. Since $[E : F] = |G| = p$, there are no fields lying strictly between F and E, so $E = F(c)$. Let σ be a generator of G. Let

$$c_1 = c, c_2 = \sigma(c), c_3 = \sigma(c_2), \ldots, c_j = \sigma(c_{j-1}).$$

Let

$$a_j = c_1 + c_2 z_j + c_3 z_j^2 + \cdots + c_p z_j^{p-1}.$$

Then, using the fact that $z_j^p = 1$,

$$\sigma(a_j) = c_2 + c_3 z_j + \cdots + c_p z_j^{p-2} + c_1 z_j^{p-1} = \frac{a_j}{z_j}.$$

So $\sigma(a_j^p) = (\sigma(a_j))^p = \frac{a_j^p}{z_j^p} = a_j^p$. Thus, $g(a_j^p) = a_j^p\ \forall g \in G$, ie. $a_j^p \in F$. Letting

$$M = \begin{pmatrix} 1 & z_1 & z_1^2 & \cdots & z_1^{p-1} \\ 1 & z_2 & z_2^2 & \cdots & z_2^{p-1} \\ & & \vdots & & \\ 1 & z_p & z_p^2 & \cdots & z_p^{p-1} \end{pmatrix},$$

we have

$$M \begin{pmatrix} c_1 \\ \vdots \\ c_p \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_p \end{pmatrix}.$$

Since M has entries in F and

$$\det M = \prod_{i<j} (z_i - z_j) \neq 0,$$

we can write $c = c_1$ as an F-linear combination of $a_1, \ldots, a_p$. Since $c \notin F$, not all a_j are in F.

Let $u = a_j$ s.t. $a_j \notin F$. Then $E = F(u)$ (by the same reasoning that showed $E = F(c)$) and $u^p = a_j^p \in F$. □

Theorem 3.12.4. *Let $p(x) \in F[x]$ be solvable by radicals over F, where* $\operatorname{char} F = 0$. *Then $\exists$ a sequence of field extensions*

$$F = L_0 \subset L_1 \subset \cdots \subset L_k = L$$

where $L_\lambda = L_{\lambda-1}(\alpha_\lambda)$, s.t. $\alpha_\lambda^{s_\lambda} \in L_{\lambda-1}$ for some s_λ and L is normal over F and contains the splitting field of $p(x)$.

Proof. By definition, $\exists$ a sequence

$$F = K_0 \subset K_1 \subset \cdots \subset K_m = K$$

where $K_j = K_{j-1}(w_j)$ with $w_j^{r_j} \in K_{j-1}$ for some r_j, and $p(x)$ splits in K.

Write $K = F(a)$ and let L be the splitting field of the min. poly. of a over F. Thus L is normal over F. Let

$$G = G(L, F) = \{\sigma_0, \ldots, \sigma_{t-1}\}, \quad \text{where } |G| = t.$$

Since $K = F(w_1, w_2, \ldots, w_m)$,

$$L = F(\sigma_0 w_1, \sigma_1 w_1, \ldots, \sigma_{t-1} w_1, \sigma_0 w_2, \ldots, \sigma_{t-1} w_2, \ldots, \sigma_0 w_m, \ldots, \sigma_{t-1} w_m).$$

Label these generators α_λ, ie. let $\alpha_\lambda = \sigma_i w_{j+1}$ where

$$\lambda - 1 = i + tj, \quad 0 \leq i \leq t-1, \quad 0 \leq j \leq m-1.$$

Inductively define $L_0 := F, L_\lambda = L_{\lambda-1}(\alpha_\lambda)$ for $1 \leq \lambda \leq tm$.

Given λ, write $\lambda - 1 = i + tj$ where $0 \leq i \leq t-1, 0 \leq j \leq m-1$. Then

$$\alpha_\lambda^{r_{j+1}} = (\sigma_i w_{j+1})^{r_{j+1}} = \sigma_i \left(w_{j+1}^{r_{j+1}} \right) \in \sigma_i(K_j) = F(\sigma_i w_1, \ldots, \sigma_i w_j) \subset L_{\lambda-1}.$$

Thus, setting $s_\lambda = r_{j+1}$ satisfies the statement of the theorem. □

Theorem 3.12.5. *Let F be a field with $\operatorname{char} F = 0$ and let $f(x) \in F[x]$. Then $f(x)$ is solvable by radicals $\iff$ the Galois group of $f(x)$ over F is a solvable group.*

Proof.

$\Rightarrow$: Suppose $f(x)$ is solvable by radicals. Then $\exists$ a sequence of field extensions

$$F = L_0 \subset L_1 \subset \cdots \subset L_k = L$$

where $L_j = L_{j-1}(\alpha_j)$, s.t. $\alpha_j^{r_j} \in L_{j-1}$ and L is normal over F and $f(x)$ splits in L. Since L is normal, L is the splitting field of some $g(x) \in F[x]$. Let $n = \operatorname{lcm}\{r_1, \ldots, r_j\}$ and let

$$w = e^{\frac{2\pi i}{n}}.$$

Let $G = G(L, F)$ and $H = G(L(w), F)$. L is normal over F, so by the Fund. Thm. (part 5),

$$G \cong H / G(L(w), L).$$

$G(L(w), L)$ is abelian, so to show G is solvable, it suffices to show that H is solvable.

Let

$$H_0 = G(L(w), F)$$

and for $i \geq 1$,

$$H_i = G(L(w), L_{i-1}(w)).$$

Then $H_0 = H$ and $H_{k+1} = \{e\}$. $F(w)$ is normal over F, and by Theorem 3.12.2, $L_i(w)$ is normal over $L_{i-1}(w)$ for each i. So by the Fund. Thm. (parts 4 and 5), $H_{i+1} \lhd H_i$ and

$$H_i / H_{i+1} \cong G(L_i(w), L_{i-1}(w)),$$

for $i \geq 1$, whereas

$$H_0/H_1 \cong G(F(w), F).$$

By Theorem 3.12.2, $G(L_i(w), L_{i-1}(w))$ is cyclic and thus abelian. $G(F(w), F)$ is also abelian. Hence, H is solvable, and so G is solvable.

$\Leftarrow$: Suppose that the Galois group of $f(x)$ over F is a solvable group. Let E be the splitting field of $f(x)$ over F. Let $G = G(E, F)$ and let $n = |G|$. Let $F_0 = F$ and $F_1 = F_0(w)$ where $w = e^{\frac{2\pi i}{n}}$. Let $K = E(w)$. By the Fund. Thm. (part 5),

$$G(K, F)/G \cong G(E(w), E),$$

which is abelian, so $G(K, F)$ is solvable. By Theorem 3.10.9, $G(K, F_1)$ is isomorphic to a subgroup H of $G(K, F)$, so it too is solvable.

So $\exists$ subgroups

$$\{e\} = H_{r+1} \lhd H_r \lhd \cdots \lhd H_2 \lhd H_1 = H$$

s.t. H_j/H_{j+1} is cyclic of prime order.

By the Fund. Thm., corresponding to this is a sequence of fields

$$F_1 \subset F_2 \subset \cdots \subset F_{r+1}$$

where $F_j = K^{H_j}$, so that $H_j = G(K, F_j)$. F_j is normal over F_{j+1} with cyclic Galois group of prime order p_j. Since $p_j \mid |G| = n$ and $e^{\frac{2\pi i}{n}} \in F_j$, F_j contains all the p_j^{th} roots of 1. By Theorem 3.12.3, this implies that

$$F_{j+1} = F_j(\alpha_j)$$

where $\alpha_j^{p_j} \in F_j$. Since $F_{r+1} = K$ contains the splitting field of $f(x)$, $f(x)$ is solvable by radicals over F.

$\square$

Theorem 3.12.6. *The Galois group of $p(x) = x^n + a_1 x^{n+1} + \cdots + a_{n-1}x + a_n$ over $K(a_1, \ldots, a_n)[x]$ is S_n.*

Proof. Let $r_1, \ldots, r_n$ be the roots of $p(x)$ in some extension field M of $K(a_1, \ldots, a_n)$. Then the splitting field of $p(x)$ is $K(r_1, \ldots, r_n)$, and

$$a_j = \pm s_j(r_1, \ldots, r_n) \quad \text{(the } j^{\text{th}} \text{ symmetric poly.).}$$

$\therefore$ The Galois group of $p(x)$ is S_n by Theorem 3.9.2. $\square$

Corollary 3.12.7. *The general n^{th} order polynomial is not solvable by radicals if $n \geq 5$.*

3.13 Calculation of Galois Groups: Cubics and Quartics

Let $f(x) \in F[x]$. Let E be the splitting field of $f(x)$ over F. Suppose E is separable over F. Let $G = G(E, F)$ be the Galois group of $f(x)$ over F and let $\alpha_1, \ldots, \alpha_n \in E$ be the roots of $f(x)$.

As noted earlier, each $\sigma \in G$ permutes $\alpha_1, \ldots, \alpha_n$, and this association yields a homo.

$$G \subset S_n.$$

What properties must this subgroup have?

Definition 3.13.1. *A subgroup $G \subset S_n$ is called **transitive** if $\forall i, j\ \exists \sigma \in G$ s.t. $\sigma(i) = j$.*

Example 3.13.2. $\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\} \subset S_4$ *is transitive.*
$\{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \subset S_4$ *is not transitive.*

If $k < n$ then $S_k \subset S_n$ cannot be transitive. So, to have a chance for G to be transitive in $S_{\deg f(x)}$, $f(x)$ must have distinct roots.

Theorem 3.13.3. *Let $n = \deg f(x)$. Then $G \subset S_n$ is transitive $\iff$ $f(x)$ is irreducible in $F[x]$.*

Proof.

$\Leftarrow$: Suppose $f(x)$ is irreducible. Then by Theorem 3.3.15, for any pair of roots α, β of $f(x)$, $\exists \sigma \in G$ s.t. $\sigma(\alpha) = \beta$. So G is transitive.

$\Rightarrow$: Suppose G is transitive. If $f(x)$ is reducible, write

$$f(x) = g(x)h(x)$$

where $g(x)$ is irreducible. Let α be a root of $g(x)$. If β is any root of $f(x)$, then find $\sigma \in G$ s.t. $\sigma(\alpha) = \beta$. Since $g \in F[x]$ and σ fixes F, this means that β is also a root of $g(x)$. This shows that every root of $f(x)$ is a root of $g(x)$. But G transitive $\Rightarrow$ the roots of $f(x)$ are distinct, so roots of $h(x)$ are not roots of $g(x)$, which is a contradiction. Hence $f(x)$ is irreducible.

$\square$

Let $h(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$. Let

$$H = \{\sigma \in S_n \mid \sigma h = h\}$$

where σ acts by permuting the variables, ie.

$$h \cdot \sigma = (\sigma^{-1} h)(y_1, \ldots, y_n) := h(y_{\sigma(1)}, \ldots, y_{\sigma(n)}).$$

$H \leq S_n$ is called the **isotropy subgroup** of h.

Example 3.13.4. *$n = 4$, $h = y_1 + y_2$. Then $H = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.*

Let $\delta = h(\alpha_1, \ldots, \alpha_n) \in E$. If $\sigma \in G \cap H$ then $\sigma(\delta) = \delta$, so

$$\sigma \in G(E, F(\delta)).$$

When is $G(E, F(\delta)) = G \cap H$?

Example 3.13.5.

1. *$n = 3$,*
$$h(y_1, y_2, y_3) = (y_1 - y_2)(y_1 - y_3)(y_2 - y_3).$$
Then $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} = A_3$. Let $f(x)$ be an irreducible cubic over F with roots $\alpha_1, \alpha_2, \alpha_3$. Assume char $F \neq 2$. *Let*
$$\Delta = h(\alpha_1, \alpha_2, \alpha_3).$$
For $\sigma \in G$, if $\sigma \in H$ then $\sigma(\Delta) = \Delta$. If $\sigma \notin H$ then $\sigma(\Delta) = -\Delta \neq \Delta$. So
$$\sigma(\Delta) = \Delta \iff \sigma \in G \cap H.$$
$\therefore G \cap H = G(E, F(\Delta))$.

2. *$n = 4, h = y_1 + y_4$. Let $f(x) = x^4 - x^2 + 1$ over $F = \mathbb{Q}$. Then*
$$H = \{e, (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}.$$
Also,
$$f(x) = x^4 - x^2 + 1 = (x^2+1)^2 - 3x^2 = (x^2+1+\sqrt{3}x)(x^2+1-\sqrt{3}x) = (x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1).$$
So the roots are
$$\frac{-\sqrt{3} \pm \sqrt{3-4}}{2}, \quad \frac{\sqrt{3} \pm \sqrt{3-4}}{2}.$$
Let
$$\alpha_1 = \frac{-\sqrt{3}+i}{2},\ \alpha_2 = \frac{-\sqrt{3}-i}{2},\ \alpha_3 = \frac{\sqrt{3}+i}{2},\ \alpha_4 = \frac{\sqrt{3}-i}{2},$$
and with this numbering of the roots, $H \subset G$. So
$$\delta = h(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha_1 + \alpha_4 = 0.$$
Consider complex conjugation σ. $\sigma \in G$ and acts on the roots as $\sigma = (1\ 2)(3\ 4)$, so $\sigma \notin H$. But $\sigma(0) = 0$. So in this case,
$$H = G \cap H \subsetneq G(E, F(\delta)) = G(E, F(0)) = G(E, F).$$

More generally, suppose

$$\delta_j = h_j(\alpha_1, \ldots, \alpha_n) \in E$$

for $j = 1, \ldots, k$, where $h_j \in F[y_1, \ldots, y_n]$. Define the isotropy subgroup by

$$H = \{\sigma \in S_n \mid \sigma h_j = h_j \ \forall j = 1, \ldots, k\}.$$

In general:

Theorem 3.13.6. *Let*

$$\delta_j = h_j(\alpha_1, \ldots, \alpha_n) \in E$$

where $h_j(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$. Let $H \subset S_n$ be the isotropy subgroup of $\{h_j\}$. Suppose that for all $\sigma \in G - H$, $\exists j$ s.t. $\sigma(\delta_j) \neq \delta_j$. Then

$$G(E, F(\delta_1, \ldots, \delta_n)) = G \cap H.$$

Proof. $G \cap H \subset G(E, F(\delta_1, \ldots, \delta_n))$ in general. Suppose $\sigma \in G(E, F(\delta_1, \ldots, \delta_n)) \subset G(E, F) = G$. Then $\sigma(\delta_j) = \delta_j \ \forall j$ so $\sigma \in H$, since if $\sigma \notin H$ then $\exists j$ s.t. $\sigma(\delta_j) \neq \delta_j$. $\square$

Note: It is often not so easy to check whether or not the condition $\sigma(\delta) \neq \delta \ \forall \sigma \in G - H$ is satisfied.

3.14 Cubics

3.14.1 Galois Theory of Cubics

Let

$$k(z) = z^3 + az^2 + bz + c$$

be irreducible, $a, b, c \in F$. Assume char $F \neq 2, 3$. Let $z = x - \frac{a}{3}$ to get

$$f(x) = x^3 + px + q$$

where $p = \frac{3b-a^2}{3}, q = \frac{2a^3-9ab+27c}{27}$. This adds $\frac{a}{3}$ to each root, but does not affect the Galois group since $\frac{a}{3} \in F$.

Let E be the splitting field of f and let $G = G(E, F)$ be the Galois group of f. Since $G \subset S_3$, and G is transitive, there are only 2 possibilities: $G = S_3$ or $G = A_3$.

Either
$$\begin{tikzcd}[arrows=dash]
F(\alpha_1,\alpha_2) = E \arrow[d, "2"'] \\
F(\alpha_1) \arrow[d, "3"'] \\
F
\end{tikzcd}$$
$G=S_3$

or
$$\begin{tikzcd}[arrows=dash]
F(\alpha_1) = E \arrow[d, "3"'] \\
F
\end{tikzcd}$$
$G=A_3$

ie. Depending on a, b, c, either $F(\alpha_1)$ already contains α_2 and α_3 so that $E = F(\alpha_1)$ and $G = A_3$ or it does not and we have a further degree 2 extension. How do we tell which?

Let
$$\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$
$f(x)$ is irreducible and char $F \neq 3 \Rightarrow$ the roots are distinct $\Rightarrow \Delta \neq 0$.
$$H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} = A_3 \subset G.$$
If $\sigma \notin H$ then $\sigma(\Delta) = -\Delta \neq \Delta$.. The theorem implies $G(E, F(\Delta)) = G \cap H = A_3$. So in either case we have:
$$\begin{tikzcd}[arrows=dash]
E \arrow[d, "3"'] \\
F(\Delta) \arrow[d, "?"'] \\
F
\end{tikzcd}$$

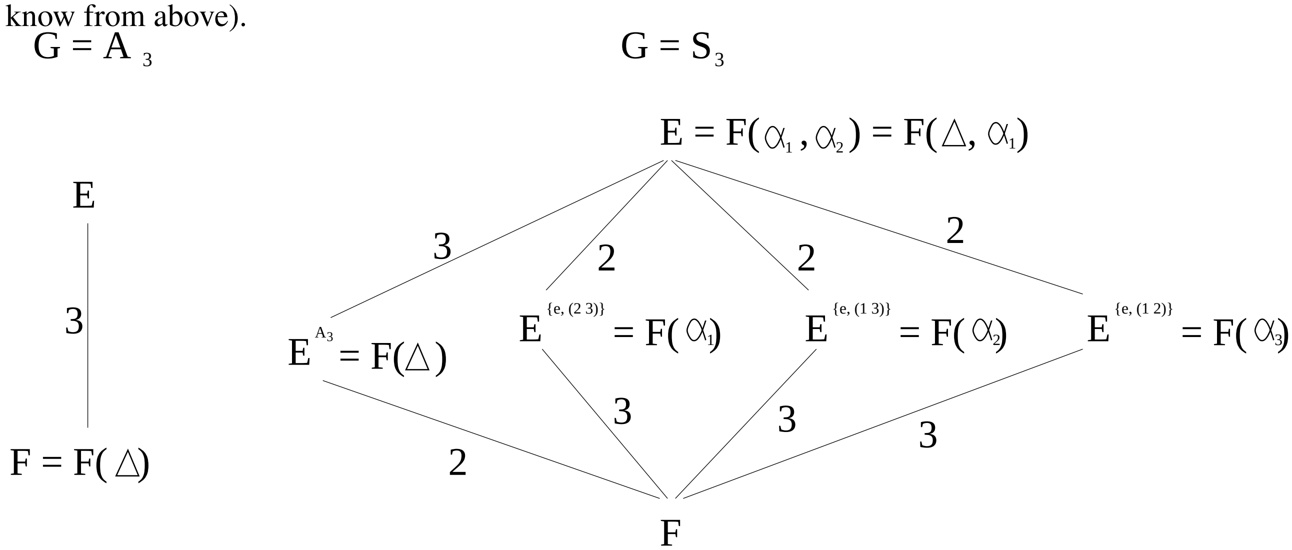
If $\Delta \in F$ then $F(\Delta) = F$ so

$$G(E, F) = G(E, F(\Delta)) = A_3.$$

If $\Delta \notin F$ then $[F(\Delta) : F] > 1$ so $[E : F] > 3$, so $G = S_3$.
Note: $\sigma(\Delta) = \pm\Delta \ \forall \sigma \in G$ so

$$\sigma(\Delta^2) = \Delta^2 \ \forall \sigma \in G.$$

$\therefore \Delta^2 \in F$ in any case. (This also shows that if $\Delta \notin F$ then $[F(\Delta) : F] = 2$, confirming what we already know from above).



So, how to tell if $\Delta \in F$? For a general polynomial $f(x) \in F[x]$, let it factor in its splitting field as

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i).$$

Let

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j).$$

The sign of Δ depends on our choice of the order of the roots. Set $D = \Delta^2$. Then D is fixed by all permutations of $\{\alpha_j\}$, (since for each permutation σ, $\sigma(\Delta) = \pm\Delta$). So $D \in F$. D is called the **discriminant** of $f(x)$.

$n = 2$: $f(x) = x^2 + bx + c$;

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4c}}{2}, \quad \alpha_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

$\therefore \Delta = \alpha_1 - \alpha_2 = \sqrt{b^2 - 4c}$ and $D = b^2 - 4c$.

$n = 3$: $f(x) = x^3 + ax^2 + bx + c$. As before, let $x = y - \frac{a}{3}$ to get

$$g(y) = y^3 + py + q$$

where $p = \frac{1}{3}(3b - a^2)$ and $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.

$$g(y) = (y - \alpha)(y - \beta)(y - \gamma)$$

in an extension field.

$$\begin{aligned} s_1 &= \alpha + \beta + \gamma = 0, \\ s_2 &= \alpha\beta + \beta\gamma + \alpha\gamma = p, \\ s_3 &= \alpha\beta\gamma = -q. \end{aligned}$$

Then

$$\begin{aligned} 3y^2 + p &= g'(y) \\ &= (y - \alpha)(y - \beta) + (y - \alpha)(y - \gamma) + (y - \beta)(y - \gamma) \\ \therefore \quad g'(\alpha) &= (\alpha - \beta)(\alpha - \gamma) \\ g'(\beta) &= (\beta - \alpha)(\beta - \gamma) \\ g'(\gamma) &= (\gamma - \alpha)(\gamma - \beta) \end{aligned}$$

$$\therefore \ D = -g'(\alpha)g'(\beta)g'(\gamma).$$

That is,

$$\begin{aligned} D &= -(3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) \\ &= -27\alpha^2\beta^2\gamma^2 - 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) - 3p^2(\alpha^2 + \beta^2 + \gamma^2) - p^3 \\ &= -27s_3^2 - 9p(s_2^2 - 2s_1s_3) - 3p^2(s_1^2 - 2s_2) - p^3 \\ &= -27q^2 - 9p(p^2 - 0) - 3p^2(-2p) - p^3 \\ &= -4p^3 - 27q^2 \\ &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2. \end{aligned}$$

3.14.2 Solution of Cubics

$$0 = x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

That is,

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= p \\ \alpha_1\alpha_2\alpha_3 &= -q \end{aligned}$$

Find $\alpha_1, \alpha_2, \alpha_3$.

Let

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \sqrt{-4p^3 - 27q^2}.$$

Let $\omega = e^{\frac{2\pi i}{3}}$ so that $\omega^3 = e^{2\pi i} = 1$, ie. ω satisfies

$$0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1).$$

Explicitly,

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

Let

$$\begin{aligned} z_1 &= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \\ z_2 &= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \\ z_3 &= \alpha_1 + \alpha_2 + \alpha_3 = 0 \end{aligned}$$

ie.

$$\begin{pmatrix} z_1 \\ z_2 \\ 0 \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \quad \text{where } A = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \\ 1 & 1 & 1 \end{pmatrix}.$$

If we can find z_1, z_2 then $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = A^{-1} \begin{pmatrix} z_1 \\ z_2 \\ 0 \end{pmatrix}$. Explicitly,

$$\begin{aligned} \alpha_1 &= \frac{1}{3}(z_1 + z_2) \\ \alpha_2 &= \frac{1}{3}(\omega^2 z_1 + \omega z_2) \\ \alpha_3 &= \frac{1}{3}(\omega z_1 + \omega^2 z_2). \end{aligned}$$

To find z_1, z_2:

$$\begin{aligned}
z_1^3 =& \alpha_1^3 + \omega^3\alpha_2^3 + \omega^6\alpha_3^3 + 3\omega\alpha_1\alpha_2 + 3\alpha_1\omega^2\alpha_2^2 \\
&+ 3\omega^2\alpha_1^2\alpha_3 + 3\omega^4\alpha_1\alpha_3^2 + 3\omega^4\alpha_2^2\alpha_3 + 3\omega^5\alpha_2\alpha_3^2 + 6\omega^3\alpha_1\alpha_2\alpha_3.
\end{aligned}$$

Using the facts that $\alpha_j^3 = -p\alpha_j - q$, $\omega^3 = 1$, and $\omega^2 = -\omega - 1$, this becomes

$$\begin{aligned}
z_1^3 &= -p\alpha_1 - q - p\alpha_2 - q - p\alpha_3 - q \\
&\quad + 3\omega(\alpha_1^2\alpha_2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_3^2) + 6\alpha_1\alpha_2\alpha_3 \\
&= -p(\alpha_1 + \alpha_2 + \alpha_3) - 3q - 3\omega(\alpha_1^2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_3^2) - 6q \\
&= -9q + 3\omega u + 3\omega^2 v
\end{aligned}$$

where

$$\begin{aligned}
u &= \alpha_1^2\alpha_2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3 \quad \text{and} \\
v &= \alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_3^2.
\end{aligned}$$

Now,

$$\begin{aligned}
0 &= (\alpha_1 + \alpha_2 + \alpha_3)^3 \\
&= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\alpha_1^2\alpha_2 + 3\alpha_1^2\alpha_3 + 3\alpha_2^2\alpha_3 + 3\alpha_1\alpha_2^2 + 3\alpha_1\alpha_3^2 + 3\alpha_2\alpha_3^2 + 6\alpha_1\alpha_2\alpha_3 \\
&= -p\alpha_1 - q - p\alpha_2 - q - p\alpha_3 - q + 3u + 3v - 6q \\
&= -9q + 3u + 3v.
\end{aligned}$$

$\therefore u + v = 3q$. Also,

$$\begin{aligned}
\Delta &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\
&= \alpha_1^2\alpha_2 - \alpha_1^2\alpha_3 - \alpha_1\alpha_2^2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3 - \alpha_2\alpha_3^2 \\
&= u - v.
\end{aligned}$$

Using the equations $u + v = 3q$ and $u - v = \Delta$, get

$$\begin{aligned}
u &= \frac{3}{2}q + \frac{\Delta}{2} \\
v &= \frac{3}{2}q - \frac{\Delta}{2}.
\end{aligned}$$

So

$$\begin{aligned}
z_1^3 &= -9q + 3\omega u + 3\omega^2 v \\
&= -9q + \omega\frac{9}{2}q + \omega\frac{3}{2}\Delta + \omega^2\frac{9}{2}q - \omega^2\frac{3}{2}\Delta \\
&= -9q + \omega\frac{9}{2}q + \omega\frac{3}{2}\Delta - \omega\frac{9}{2}q - \frac{9}{2}q - \omega\frac{3}{2}\Delta + \frac{3}{2}\Delta \\
&= -\frac{27q}{2} + 3\omega\Delta + \frac{3}{2}\Delta \\
&= -\frac{27q}{2} + \frac{3}{2}\Delta(2\omega + 1) \\
&= -\frac{27q}{2} + \frac{3\sqrt{3}i}{2}\Delta.
\end{aligned}$$

Similarly, we find

$$z_2^3 = \overline{z_1}^3 = -\frac{27q}{2} - \frac{3\sqrt{3}i}{2}\Delta.$$

$\therefore z_1 = (-\frac{27q}{2} + \frac{3\sqrt{3}i}{2}\Delta)^{\frac{1}{3}}$ and $z_2 = (-\frac{27q}{2} - \frac{3\sqrt{3}i}{2}\Delta)^{\frac{1}{3}}$. This determines $\alpha_1, \alpha_2, \alpha_3$ in terms of p and q.

To illustrate the Galois theory, we now find a formula for α_2 in terms of α_1, that makes is obvious that $\alpha_2 \in F(\alpha_1) \iff \Delta \in F$.

$$\begin{aligned}
\Delta &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\
&= (\alpha_1 - \alpha_2)(2\alpha_1 + \alpha_2)(\alpha_1 + 2\alpha_2), \quad \text{since } \alpha_1 + \alpha_2 + \alpha_3 = 0 \\
&= 2\alpha_1^3 + 5\alpha_1^2\alpha_2 + 2\alpha_1\alpha_2^2 - 2\alpha_1^2\alpha_2 - 5\alpha_1\alpha_2^2 - 2\alpha_2^3 \\
&= -2\alpha_1 p - 2q + 3\alpha_1^2\alpha_2 - 3\alpha_1\alpha_2^2 + 2\alpha_2 p + 2q \\
&= -2\alpha_1 p + 3\alpha_1^2\alpha_2 - 3\alpha_1\alpha_2^2 + 2\alpha_2 p.
\end{aligned}$$

Also,

$$q = -\alpha_1\alpha_2\alpha_3 = \alpha_1\alpha_2(\alpha_1 + \alpha_2) = \alpha_1^2\alpha_2 + \alpha_1\alpha_2^2 \Rightarrow \alpha_1\alpha_2^2 = q - \alpha_1^2\alpha_2.$$

So,

$$\begin{aligned}
\Delta &= -2\alpha_1 p + 3\alpha_1^2\alpha_2 - 3q + 3\alpha_1^2\alpha_2 + 2\alpha_2 p \\
&= -2\alpha_1 p + 6\alpha_1^2\alpha_2 - 3q + 2\alpha_2 p.
\end{aligned}$$

$\therefore 6\alpha_1^2\alpha_2 + 2\alpha_2 p = \Delta + 2\alpha_1 p + 3q$. This gives

$$\alpha_2 = \frac{\Delta + 2\alpha_1 p + 3q}{2(3\alpha_1^2 + p)}. \tag{*}$$

Thus, if $\Delta \in F$ then $\alpha_2 \in F(\alpha_1)$. Conversely, if $\alpha_2 \in F(\alpha_1)$ then (*) $\Rightarrow \Delta \in F(\alpha_1)$. But

$$[F(\alpha_1) : F] = 3$$

and $\Delta^2 \in F$, so this implies that $\Delta \in F$.

3.15 Quartics

3.15.1 Solution of Quartics

We want to solve

$$z^4 + a_1 z^3 + a_2 z^2 + a_3 z + a_4 = 0.$$

Let $z = x - \frac{a}{4}$ to get the form

$$x^4 + px^2 + qx + r = 0.$$

Let the roots be r_1, r_2, r_3, r_4, so

$$\begin{aligned}
s_1 &= r_1 + r_2 + r_3 + r_4 = 0 \\
s_2 &= r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4 = p \\
s_3 &= r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4 = -q \\
s_4 &= r_1r_2r_3r_4 = r.
\end{aligned}$$

Suppose we can determine

$$\begin{aligned}
(r_1 + r_2)(r_3 + r_4) &= \theta_1 \\
(r_1 + r_3)(r_2 + r_4) &= \theta_2 \\
(r_1 + r_4)(r_2 + r_3) &= \theta_3.
\end{aligned}$$

Then letting $a = r_1 + r_2, b = r_3 + r_4$, get $ab = \theta_1$ and $a + b = 0$. So $-a^2 = ab = \theta_1$, so

$$a = \sqrt{-\theta_1}, \quad b = -\sqrt{-\theta_1},$$

where $\sqrt{-\theta_1}$ is one of the square roots of $-\theta_1$ in $\mathbb{C}$.

Similarly,

$$\begin{aligned}
r_1 + r_3 &= \sqrt{-\theta_2}, \quad r_2 + r_4 = -\sqrt{-\theta_2}, \\
r_1 + r_4 &= \sqrt{-\theta_3}, \quad r_2 + r_3 = -\sqrt{-\theta_3},
\end{aligned}$$

for choices of $\sqrt{-\theta_2}$, $\sqrt{-\theta_3}$. So

$$\begin{aligned}\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3} &= r_1+r_2+r_1+r_3+r_1+r_4\\ &= 2r_1+r_1+r_2+r_3+r_4\\ &= 2r_1.\\ \therefore\ r_1 &= \frac{\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3}}{2}.\end{aligned}$$

Similarly, we can solve for r_2, r_3, r_4 if we know $\theta_1, \theta_2, \theta_3$. So it suffices to find $\theta_1, \theta_2, \theta_3$.

Consider the cubic equation

$$f(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3) = 0.$$

If we can write the coefficients of this eqn. in terms of p, q, r, then we can use the soln. of cubics to determine $\theta_1, \theta_2, \theta_3$ in terms of p, q, r and thus write r_1, r_2, r_3, r_4 in terms of p, q, r.

Consider the action of S_4 as permutations of r_1, r_2, r_3, r_4. Consider first the transposition σ which interchanges r_1 and r_2:

$$\sigma(\theta_1) = \theta_1 \quad \sigma(\theta_2) = \theta_3 \quad \sigma(\theta_3) = \theta_2.$$

$\therefore \sigma(f(x)) = f(x)$.

Similarly, $\sigma(f(x)) = f(x)$ for every transposition in S_4. Since S_4 is generated by transpositions, $\sigma(f(x)) = f(x)\ \forall \sigma \in S_4$. That is, the coeffs. of $f(x)$ are left fixed by all permutations of r_1, r_2, r_3, r_4. So the coeffs. of $f(x)$ are symmetric polynomials in r_1, r_2, r_3, r_4, and so can be expressed in terms of p, q, r. This gives:

Theorem 3.15.1. *The coefficients of $f(x)$ are polynomials in p, q, r.*

To find the coefficients:

Method 1: Expand

$$\begin{aligned}f(x) &= (x-(r_1+r_2)(r_3+r_4))(x-(r_1+r_3)(r_2+r_4))(x-(r_1+r_4)(r_2+r_3))\\ &= \text{big mess}\\ &= \text{poly. in } p, q, r, x.\end{aligned}$$

Or

Method 2: Geometric method using conics.

3.15.2 Conics (over $\mathbb{R}$)

Definition 3.15.2. *A **conic** is a polynomial of degree ≤ 2 in two variables (over $\mathbb{R}$),*

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f.$$

To conic $q(x, y)$, associate the 3-variable quadratic form:

$$Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + cYZ + fZ^2.$$

ie. $Q(X, Y, Z) = Z^2 q(\frac{X}{Z}, \frac{Y}{Z})$. The **associated matrix** to q is

$$M_q = \begin{pmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{pmatrix},$$

and this gives

$$Q(X, Y, Z) = \begin{pmatrix} X & Y & Z \end{pmatrix} M_q \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

M_q is symmetric, so it is diagonalizable. ie. $\exists U$ s.t.

$$U^{-1} M_q U = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}.$$

This corresponds to change of variables

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = U \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix}.$$

In the new basis,

$$Q'(X', Y', Z') = \lambda_1 X'^2 + \lambda_2 Y'^2 + \lambda_3 Z'^2.$$

$\det M_q = \lambda_1\lambda_2\lambda_3$. If $\det M_q = 0$ then $Q = 0$ degenerates into a product of lines.

e.g. Suppose $\lambda_3 = 0$. If λ_1, λ_2 have the same sign then $Q' = 0 \iff X' = 0, Y' = 0$, giving one line. If λ_1, λ_2 have different signs then

$$0 = Q' = \lambda_1 X'^2 + \lambda_2 Y'^2$$

factors into linear factors, giving two planes. So $q(x, y)$ degenerates when $\det M_q = 0$.

Conversely, if $q(x, y)$ factors as a product

$$q(x, y) = (\alpha x + \beta y + \gamma)(\delta x + \epsilon y + \varphi)$$

then Q factors as

$$(\alpha X + \beta Y + \gamma Z)(\delta X + \epsilon Y + \varphi Z),$$

and by inspection, this can only happen when one of the λ_i's is 0. So $q(x, y)$ is degenerate $\iff$ $\det M_q = 0$.

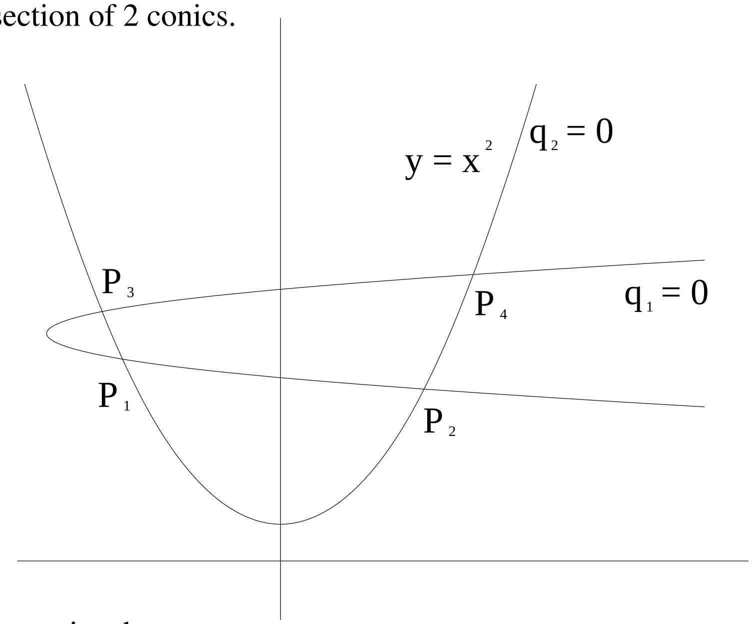
Consider the quartic

$$x^4 + px^2 + qx + r = 0.$$

Let $y = x^2$. Then solving $x^4 + px^2 + qx + r = 0$ is equivalent to solving the system

$$\begin{aligned} q_1 &= y^2 + py + qx + r = 0, \\ q_2 &= y - x^2 = 0. \end{aligned}$$

$\therefore$ Look for the intersection of 2 conics.



Let the intersection points be

$$P_1 = (r_1, r_1^2), \quad P_2 = (r_2, r_2^2), \quad P_3 = (r_3, r_3^2), \quad P_4 = (r_4, r_4^2).$$

Consider the family of conics $q_t = q_1 - tq_2$. Then $q_t(P_j) = 0$ regardless of t. Since M_{q_t} is a 3×3 matrix, $\det M_{q_t} = 0$ is a cubic eqn. in t. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $\det M_{q_t}$. We will show that $\alpha_1, \alpha_2, \alpha_3$ are $\theta_1, \theta_2, \theta_3$.

For $j = 1, 2, 3$, $\det M_{q_{\alpha_j}} = 0$, so q_{α_j} is a product of lines. We know that P_1, P_2, P_3, P_4 satisfy $q_t = 0\ \forall t$ so they must lie on the lines. So the lines have to be those joining the points P_j. Let $L_{ij} = 0$ be the line joining P_i to P_j. Then (upon renumbering if necessary),

$$q_{\alpha_1} = L_{12}L_{34}, \quad q_{\alpha_2} = L_{13}L_{24}, \quad q_{\alpha_3} = L_{14}L_{23}.$$

L_{12} is

$$y - r_1^2 = \left(\frac{r_2^2 - r_1^2}{r_2 - r_1}\right)(x - r_1) = (r_2 + r_1)(x - r_1) = (r_1 + r_2)x - r_1 r_2 - r_1^2$$

That is, L_{12} is $y - (r_1 + r_2)x + r_1 r_2 = 0$. Similarly, L_{34} is $y - (r_3 + r_4)x + r_3 r_4 = 0$.

To show $\alpha_1 = \theta_1$:

$$\begin{aligned}
q_1 - \alpha_1 q_2 = q_{\alpha_1}& \\
&= (y - (r_1 + r_2)x + r_1 r_2)(y - (r_3 + r_4)x + r_3 r_4) \\
&= y^2 - (r_1 + r_2 + r_3 + r_4)xy + (r_1 + r_2)(r_3 + r_4)x^2 - (r_1 r_2 r_3 + r_1 r_2 r_4 + r_1 r_3 r_4 + r_2 r_3 r_4)x \\
&\quad + (r_1 r_2 + r_3 r_4)y + r_1 r_2 r_3 r_4 \\
&= y^2 + \theta_1 x^2 + qx + (p - r_1 r_3 - r_1 r_4 - r_2 r_3 - r_2 r_4)y + r \\
&= y^2 + \theta_1 x^2 + qx + py - (r_1 + r_2)(r_3 + r_4)y + r \\
&= y^2 + \theta_1 x^2 + qx + py - \theta_1 y + r \\
&= q_1 - \theta_1 q_2.
\end{aligned}$$

$\therefore \alpha_1 = \theta_1$. Similarly, $\alpha_2 = \theta_2$ and $\alpha_3 = \theta_3$. So to find $\theta_1, \theta_2, \theta_3$, we must solve $\det M_{q_t} = 0$

$$q_t = q_1 - tq_2 = y^2 + py + qx + r - t(y - x^2) = y^2 + tx^2 + qx + (p - t)y + r.$$

So

$$\begin{aligned}
\det M_{q_t} &= \begin{vmatrix} t & 0 & \frac{q}{2} \\ 0 & 1 & \frac{p-t}{2} \\ \frac{q}{2} & \frac{p-t}{2} & r \end{vmatrix} \\
&= tr - \frac{q^2}{4} - \left(\frac{p - t}{2}\right)^2 t \\
&= tr - \frac{q^2}{4} - \frac{p^2 t}{4} + \frac{2pt^2}{4} - \frac{t^3}{4} \\
&= \frac{1}{4}(t^3 - 2pt^2 + (p^2 - 4r)t + q^2)
\end{aligned}$$

So $\det M_{q_t} = 0 \iff t^3 - 2pt^2 + (p^2 - 4r)t + q^2 = 0$.

Summary: To solve

$$z^4 + a_1 z^3 + a_2 z^2 + a_3 z + a_4 = 0,$$

1. Let $z = x - \frac{a}{4}$ to get the form
$$x^4 + px^2 + qx + r = 0.$$

2. Solve the cubic
$$t^3 - 2pt^2 + (p^2 - 4r)t + q^2 = 0$$
to get $\theta_1, \theta_2, \theta_3$.

3. $r_1 = \frac{\sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}}{2}$ for some choice of square roots of $-\theta_1, -\theta_2, -\theta_3$, and similar formulae for the other roots.

Notice that

$$\begin{aligned}\theta_1 - \theta_2 &= (r_1 + r_2)(r_3 + r_4) - (r_1 + r_3)(r_2 + r_4)\\ &= r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 - r_1r_2 - r_1r_4 - r_2r_3 - r_3r_4\\ &= -(r_1 - r_4)(r_2 - r_3).\end{aligned}$$

Similarly, $\theta_1 - \theta_3 = -(r_1 - r_3)(r_2 - r_4)$ and $\theta_2 - \theta_3 = -(r_1 - r_2)(r_3 - r_4)$. So

$$D_{\text{cubic}} = \prod_{i \neq j}(\theta_i - \theta_j) = \prod_{i \neq j}(r_i - r_j) = D_{\text{original quartic}}.$$

Thus

$$\begin{aligned}D &= -4(-2p)^3q^2 + (-2p)^2(p^2 - 4r)^2 + 18(-2p)(p^2 - 4r)q^2 - 4(p^2 - 4r)^3 - 27(q^2)^2\\ &= 32p^3q^2 + 4p^4 - 32p^4r + 64p^2r^2 - 36p^3q^2 + 144pq^2r - 4p^6 + 48p^4r - 192p^2r^2 + 256r^3 - 27q^4\\ &= 16p^4r - 4p^3q^2 - 128p^2r + 144pq^2r - 27q^4 + 256r^3\\ &= -128b^2d^2 - 4a^3g^3 + 16x^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 + 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d\\ &\quad - 6a^2c^2d + 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd.\end{aligned}$$

3.15.3 Galois Theory of Quartics

Let
$$f(x) = x^4 + px^2 + qx + r$$
be irreducible, char $F \neq 2, 3$. Let E be the splitting field of $f(x)$ over F. Let $G = G(E, F)$ be the Galois group.

$G \subset S_4$ is transitive. The transitive subgroups of S_4 are:

1. S_4.

2. A_4.

3. The Sylow 2-subgroups, isomorphic to D_8:

$$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\},$$
$$\{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3), (1\ 2), (3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$
$$\{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2), (1\ 4), (2\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4)\}.$$

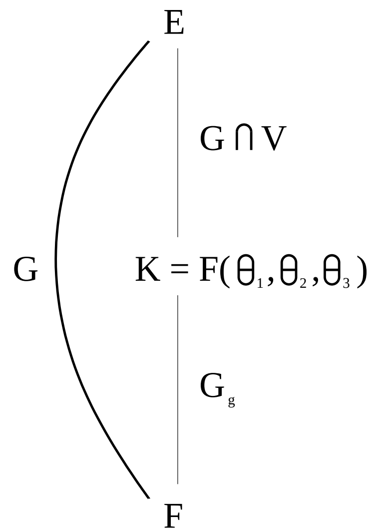
4. Groups isomorphic to C_3:

$$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}, \{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}, \{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}.$$

5. $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong C_2 \times C_2 = V$.

Let
$$g(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 - 2px^2 + (p^2 - 4r)x + q^2,$$
where
$$\begin{aligned} \theta_1 &= (r_1 + r_2)(r_3 + r_4), \\ \theta_2 &= (r_1 + r_3)(r_2 + r_4), \\ \theta_3 &= (r_1 + r_4)(r_2 + r_3). \end{aligned}$$
Let
$$\Delta = \prod_{i<j}(r_i - r_j) = -(\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3).$$
char $F \neq 2$ and f irreducible $\Rightarrow$ roots are distinct, so $\Delta \neq 0$. The discriminant is
$$D = \Delta^2 \in F.$$

Let $K = F(\theta_1, \theta_2, \theta_3)$ be the splitting field of $g(x)$. $\theta_j \in E$ for $j = 1, 2, 3$ so $K \subset E$. Notice that $V \cong C_2 \times C_2$ is the isotropy group of
$$\{\theta_1, \theta_2, \theta_3\}.$$
ie. If $\sigma \in V$ then $\sigma(\theta_j) = \theta_j$, but if $\sigma \in S_4 - V$ then for some j, $\sigma(\theta_j) \neq \theta_j$. According to Theorem 3.13.6, this implies $G(E, K) = G \cap V$.



By the Fund. Thm.,

$$G_g = G(K, F) \cong G/(G \cap V).$$

We can calculate G_g from the section on cubics. Will this determine G? By inspection:

	G	$G/(G \cap V)$
1	S_4	S_3
2	A_4	C_3
3	D_8	C_2
4	C_4	C_2
5	V	$\{e\}$

So $G_g = G/(G \cap V)$ will tell us G unless $G_g \cong C_2$, in which case it cannot distinguish between D_8 and C_4.

Study $G_g = C_2$ more closely to obtain a method of distinguishing. So assume $G_g \cong C_2$. Since $g(x)$ is a cubic and $|C_2| = 2$, this means that one root of $g(x)$, say θ_1, already lies in F. ie. In F, $g(x)$ factors as

$$g(x) = (x - \theta_1)g_1(x)$$

where $g_1(x)$ is an irreducible quadratic (with roots θ_2, θ_3, which are not in F).

Suppose $G = C_4$.

$$
\begin{tikzcd}
E \arrow[d, dash, "2"] \arrow[dd, bend right=60, dash, "C_4"'] \\
E^{C_2} = F(\theta_2) = F(\theta_1, \theta_2, \theta_3) = F(\triangle) \arrow[d, dash, "2"] \\
F = F(\theta_1)
\end{tikzcd}
$$

Recall $(r_1 + r_2)^2 = -\theta_1$ so $[F(r_1 + r_2) : F] \leq 2$. If $r_1 + r_2 \in F$ then $r_1 + r_2$ is fixed by all $\sigma \in G$. But $G = C_4$ contains a 4-cycle, and no 4-cycle fixes $r_1 + r_2$. e.g. Say $\sigma = (1\ 2\ 3\ 4)$. Then $\sigma(r_1 + r_2) = r_2 + r_3$.

Thus $r_1 + r_2 \notin F$, and so

$$[F(r_1 + r_2) : F] = 2.$$

C_4 has a unique subgroup of index 2, so E has a unique subfield of order 2 over F. So

$$F(r_1 + r_2) = E^{C_2} = F(\theta_2) = F(\Delta).$$

Hence $r_1 + r_2 = a + b\Delta$ for some $a, b \in F$.

$$-\theta_1^2 = (r_1 + r_2)^2 = a^2 + 2ab\Delta + b^2\Delta^2 = a^2 + b^2 D + 2ab\Delta$$

where $D = \Delta^2 \in F$. So

$$2ab\Delta = -\theta_1 - a^2 - b^2 D \in F.$$

But $\Delta \notin F$, so either $a = 0$ or $b = 0$. $b \neq 0$, since $b = 0$ puts $r_1 + r_2 = a \in F$, so $a = 0$. Thus

$$-\theta_1 = b^2 D$$

$\therefore \frac{-\theta_1}{D}$ is a square in F.

In conclusion, $G = C_4 \Rightarrow \frac{-\theta_1}{D}$ is a square in F.

Conversely, suppose $\frac{-\theta_1}{D} = b^2$ for some $b \in F$. Then

$$(r_1 + r_2)^2 = b^2 D = b^2 \Delta^2$$

so $r_1 + r_2 = \pm b\Delta \in F(\Delta)$.

Suppose that $G = D_8$. Then by inspection, G contains 2 disjoint transpositions. $(1\ 2) \notin G$, since this contradicts $r_1 + r_2 = \pm b\Delta$ (any transposition applied to Δ produces $-\Delta$). So, some other transposition, say $(1\ 3)$ lies is G (since G contains 2 disjoint transpositions, one of them must include 1).

$$r_3 + r_2 = (1\ 3) \cdot (r_1 + r_2) = (1\ 3)(\pm b\Delta) = \mp b\Delta.$$

So

$$-\theta_3 = (r_3 + r_2)^2 = b^2\Delta^2 = b^2 D \in F.$$

This is a contradiction, so $G \ncong D_8$, and thus, $G \cong C_4$. ie. $G \cong C_4 \iff -\frac{\theta_1}{D}$ is a square in F.
Summary: To compute G,

1. Compute
$$g(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2.$$

2. Factor $g(x)$ in F:

Case I: $g(x)$ factors completely in F. Then $G_g = \{e\}$, so $G = V$.

Case II: $g(x)$ has one linear factor in F,

$$g(x) = (x - \theta)g_1(x).$$

(a) The factorization determines $\theta \in F$.
(b) Compute $D \in F$, the discriminant of g, by earlier formula.
(c) If $-\frac{\theta}{D}$ is a square in G, then $G = C_4$; otherwise, $G = D_8$.

Case III: $g(x)$ is irreducible over F.

(a) Compute $D \in F$ as above.
(b) If D is a square in F then $G_g = C_3 = A_3$, so $G = A_4$. Otherwise, $G_g = S_3$ so $G = S_4$.

For $G = S_4$:
$r_1 + r_2 \neq 0$, since $\theta_1 \neq 0$ (g is irreducible when $G = S_4$). Similarly, $r_i + r_j \neq 0\ \forall i, j$. So

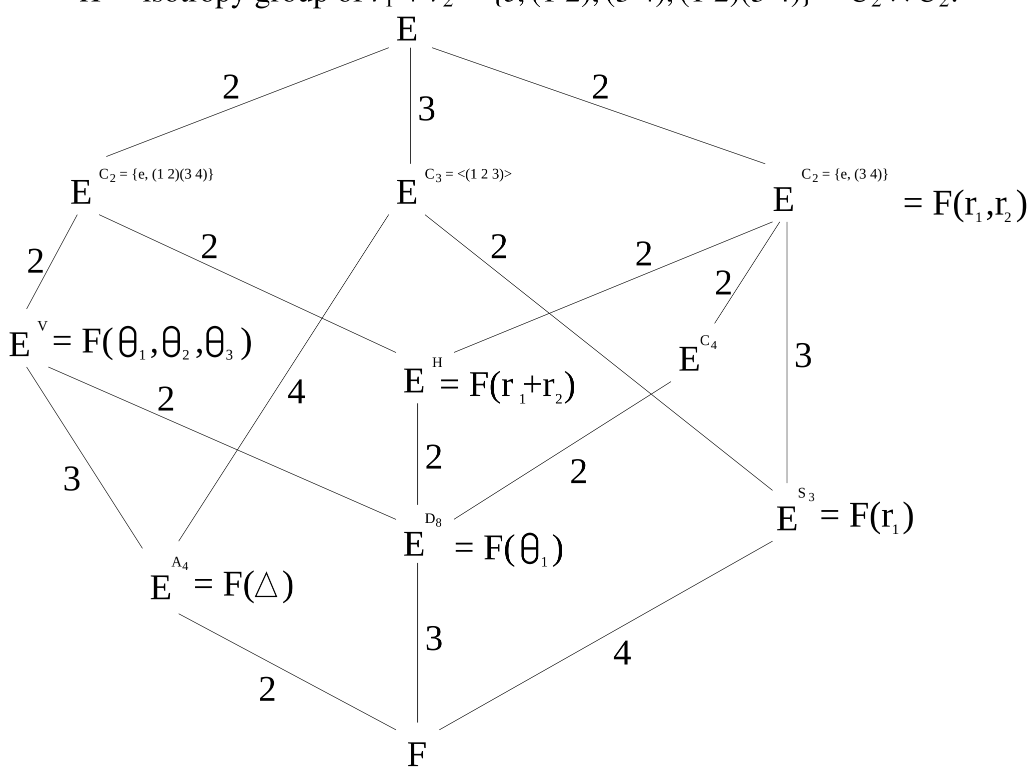
$$r_1 + r_2 \neq r_i + r_j$$

unless $i = 1$, $j = 2$ or $j = 1, i = 2$. Hence $\sigma(\theta_j) \neq \theta_j$ if $\sigma \in$ isotropy group of θ_1, which is D_8. Thus,

$$G(E, F(\theta_1)) \cong D_8.$$

Let

$$H = \text{isotropy group of } r_1 + r_2 = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \cong C_2 \times C_2.$$



For $G = A_4$:
In this case,

$$V = G(E, F(\theta_1)) = \text{isotropy group of } \theta_1.$$

$$\begin{tikzcd}
 & E \arrow[ddl, dash, "3"'] \arrow[dr, dash, "2"] & \\
 & & E^{C_2} = F(r_1+r_2) \arrow[dd, dash, "2"] \\
E^{A_3} = F(r_1) \arrow[ddr, dash, "4"'] & & \\
 & & E^{V} = F(\theta_1) \arrow[dl, dash, "3"'] \\
 & F = F(\triangle) &
\end{tikzcd}$$

For $G = D_8$:

$$\begin{tikzcd}
 & E \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] & \\
E^{\langle(3\,4)\rangle} = F(r_1) \arrow[d, dash, "2"] & E^{\langle(1\,3)(2\,4)\rangle} = F(r_1+r_3) \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
E^{\langle(1\,2),\,(3\,4)\rangle} = F(r_1+r_2) \arrow[dr, dash, "2"] & E^{C_4} \arrow[d, dash, "2"'] & E^{V} = F(\triangle) = F(\theta_2) = F(\theta_3) \arrow[dl, dash, "2"] \\
 & F = F(\theta_1) &
\end{tikzcd}$$

For $G = C_4$:

$$\begin{tikzcd}[arrows=dash]
E \arrow[d, "2"'] \\
E^{C_2} = F(\triangle) = F(r_1+r_2) = F(r_1+r_3) = F(r_1+r_4) \arrow[d, "2"'] \\
F = F(\theta_1)
\end{tikzcd}$$

For $G = C_2 \times C_2$:

$$\begin{tikzcd}[arrows=dash]
 & E \arrow[dl, "2"'] \arrow[d, "2"'] \arrow[dr, "2"] & \\
E^{\langle(1\,2)(3\,4)\rangle} = F(r_1+r_2) \arrow[dr] & E^{\langle(1\,3)(2\,4)\rangle} = F(r_1+r_3) \arrow[d, "2"'] & E^{\langle(1\,4)(2\,3)\rangle} = F(r_1+r_4) \arrow[dl] \\
 & F = F(\theta_1, \theta_2, \theta_3) = F(\triangle) &
\end{tikzcd}$$

3.16 Resultants and Discriminants

Let F be a field. Let $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ belong to $F[x]$.

Let $d(x) = \gcd(f(x), g(x))$. Suppose $\deg d(x) > 0$. Write

$$f(x) = b(x)d(x),$$
$$g(x) = a(x)d(x),$$

with $\deg b(x) < n$, $\deg a(x) < m$. Then

$$a(x)f(x) = a(x)b(x)d(x) = b(x)g(x).$$

Conversely, suppose $\exists a(x), b(x)$ s.t. $\deg a(x) < m, \deg b(x) < n$. and

$$a(x)f(x) = a(x)b(x)d(x) = b(x)g(x).$$

So $f(x) \mid b(x)g(x)$. If $\gcd(f(x), g(x)) = 1$ then $f(x) \mid b(x)$, contradicting $\deg b < \deg f$. Thus:

Proposition 3.16.1. *$f(x), g(x)$ have a common factor $\iff \exists a(x), b(x)$ s.t.*

$$a(x)f(x) = b(x)g(x),$$

with $\deg a < \deg g$ *and* $\deg b < \deg f$.

Let $a(x)f(x) = b(x)g(x)$ with

$$a(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{m-1}x^{m-1},$$
$$b(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1},$$

(coeffs. $\alpha_j, \beta_j \in F$, possibly are 0). So

$$\sum_{k=0}^{n+m-1}\left(\sum_{j=0}^{k}\alpha_{k-j}a_j\right)x^k = a(x)f(x) = b(x)g(x) = \sum_{k=0}^{n+m-1}\left(\sum_{j=0}^{k}\beta_{k-j}b_j\right)x^k.$$

That is,

$$\sum_{j=0}^{k}\alpha_{k-j}a_j - \sum_{j=0}^{k}\beta_{k-j}b_j = 0 \qquad \text{for } k = n+m-1, n+m-2, \ldots, 0.$$

Treat this as a system of $n+m$ equations in the $n+m$ variables $\{\alpha_{m-1}, \ldots, \alpha_0, \beta_{n-1}, \ldots, \beta_0\}$. Then the existence of a common factor of $f(x), g(x)$ is equivalent to the existence of a non-zero solution to this

system.
$\therefore$ Common factor exists $\iff$ determinant of this system is zero.
The determinant of the system is

$$\mathrm{Det} = \begin{vmatrix} a_n & 0 & \cdots & 0 & -b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \ddots & \vdots & -b_{m-1} & -b_m & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ a_0 & & & a_n & & & & \\ & & & & -b_0 & & & -b_m \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & -b_0 \end{vmatrix}.$$

Multiply by $(-1)^m$ and transpose to get:

Proposition 3.16.2. *$f(x), g(x)$ have a common factor* $\iff$

$$R(f,g) := \begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & & & a_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & a_n & \cdots & \cdots & & a_0 \\ b_m & b_{m-1} & \cdots & & b_0 & & & \\ & b_m & & & & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & & b_m & \cdots & \cdots & b_0 \end{vmatrix} = 0.$$

$R(f,g)$ is called the **resultant** of f and g. Denote

$$R = \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & & & a_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & a_n & \cdots & \cdots & & a_0 \\ b_m & b_{m-1} & \cdots & & b_0 & & & \\ & b_m & & & & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & & b_m & \cdots & \cdots & b_0 \end{pmatrix},$$

so that $R(f, g) = \det R$.

$$R\begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} a_n x^{n+m-1} + a_{n-1}x^{n+m-2} + \cdots + a_0 x^{m-1} \\ a_n x^{n+m-2} + a_{n-1}x^{n+m-3} + \cdots + a_0 x^{m-2} \\ \vdots \\ a_n x^n + \cdots + a_0 \\ b_m x^{n+m-1} + \cdots + b_0 x^{n-1} \\ \vdots \\ b_m x^m + \cdots + b_0 \end{pmatrix} = \begin{pmatrix} x^{m-1}f(x) \\ x^{m-2}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ \vdots \\ g(x) \end{pmatrix}. \qquad (*)$$

Let $\tilde{R}$ be the matrix of cofactors of R. That is,

$(\tilde{R})_{ij} = \det\big((n+m-1)\times(n+m-1)$ matrix formed by deleting row j and column i from $R\big)$.

So $\tilde{R}R = R\tilde{R} = (\det R)I$. Apply $\tilde{R}$ to (*) gives

$$(\det R)\begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} = \tilde{R}\begin{pmatrix} x^{m-1}f(x) \\ x^{m-2}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ \vdots \\ g(x) \end{pmatrix} = \begin{pmatrix} * \\ \vdots \\ * \\ \gamma_1 x^{m-1}f(x) + \cdots + \gamma_m f(x) + \gamma_{m+1}x^{n-1}g(x) + \cdots + \gamma_{n+m}g(x) \end{pmatrix},$$

where

$$\tilde{R} = \begin{pmatrix} * & \cdots & * \\ \vdots & & \vdots \\ * & \cdots & * \\ \gamma_1 & \cdots & \gamma_{n+m} \end{pmatrix}.$$

Equating the bottom row gives

$$\det R = r(x)f(x) + s(x)g(x)$$

for some polynomials $r(x), s(x)$.

Let $r_1, \ldots, r_n$ be the roots of $f(x)$ and let $t_1, \ldots, t_m$ be the roots of $g(x)$. If $r_i = t_j$ for any i and j then in an extension field, $f(x)$ and $g(x)$ have a common factor, so $\det R = 0$. For all i, j, $r_i - t_j$ divides $\det R$ in the splitting field of $f(x)g(x)$. By comparing degrees, up to a scalar multiple λ,

$$\det R = \lambda \prod_{i,j}(r_i - t_j).$$

By comparing the lead coefficient, find $\lambda = a_n^m b_m^n$. Thus:

Theorem 3.16.3. $R(f, g) = \det R = a_n^m b_m^n \prod_{i,j}(r_i - t_j)$.

Since $f(x) = a_n \prod_{i=1}^n (x - r_i)$ and $g(x) = b_n \prod_{j=1}^m (x - t_j)$, we get:

Corollary 3.16.4.

1. $R(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (r_i - t_j) = a_n^m \prod_{i=1}^n \left(b_m \prod_{j=1}^m (r_i - t_j)\right) = a_n^m \prod_{i=1}^n g(r_i)$*, and*

2. $R(f, g) = (-1)^{nm} b_m^n \prod_{j=1}^m \left(a_n \prod_{i=1}^n (t_j - r_i)\right) = (-1)^{nm} b_m^n \prod_{j=1}^m f(t_j)$.

Let $f(x)$ be monic and let $g(x) = f'(x)$.

$$f'(x) = \sum_{k=1}^n (x - r_1)(x - r_2) \cdots \widehat{(x - r_k)} \cdots (x - r_n).$$

So

$$f(r_i) = \prod_{\{j | j \neq i\}} (r_i - r_j).$$

Hence

$$R(f, f') = \prod_{i=1}^n f'(r_i) = \prod_i \prod_{\{j | j \neq i\}} (r_i - r_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{(i,j) | i < j} (r_i - r_j)^2 = (-1)^{\frac{n(n-1)}{2}} D,$$

where D is the discriminant. So,

$$D = (-1)^{\frac{n(n-1)}{2}} R(f, f').$$

Example 3.16.5.
$n = 2$: $f(x) = x^2 + bx + c$.

$$D = (-1) \begin{vmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2 & b \end{vmatrix} = -(b^2 + 4c - 2b^2) = b^2 - 4c.$$

$n = 3$: $f(x) = x^3 + px + q$.

$$
\begin{aligned}
D &= (-1)\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} \\
&= -\begin{vmatrix} 1 & 0 & p & q \\ 0 & p & 0 & 0 \\ 3 & 0 & p & 0 \\ 0 & 3 & 0 & p \end{vmatrix} - 3\begin{vmatrix} 0 & p & q & 0 \\ 1 & 0 & p & q \\ 3 & 0 & p & 0 \\ 0 & 3 & 0 & p \end{vmatrix} \\
&= -p\begin{vmatrix} 1 & p & q \\ 3 & p & 0 \\ 0 & 0 & p \end{vmatrix} + 3p\begin{vmatrix} 1 & p & q \\ 3 & p & 0 \\ 0 & 0 & p \end{vmatrix} - 3q\begin{vmatrix} 1 & 0 & q \\ 3 & 0 & 0 \\ 0 & 3 & p \end{vmatrix} \\
&= 2p\begin{vmatrix} 1 & p & q \\ 3 & p & 0 \\ 0 & 0 & p \end{vmatrix} - 3q\begin{vmatrix} 1 & 0 & q \\ 3 & 0 & 0 \\ 0 & 3 & p \end{vmatrix} \\
&= 2p^2\begin{vmatrix} 1 & p \\ 3 & p \end{vmatrix} + 9q\begin{vmatrix} 1 & q \\ 3 & p \end{vmatrix} \\
&= 2p^2(-2p) + 9q(-3q) \\
&= -4p^3 - 27q^2.
\end{aligned}
$$

3.17 Reduction Mod p

Theorem 3.17.1. *Let $f(x) \in \mathbb{Z}[x]$ be monic with $n = \deg f$. Let E be the splitting field of $f(x)$ over $\mathbb{Q}$. Let p be a prime not dividing the discriminant d of f. (In particular, $d \neq 0$ or no such p exists.) Let $f_p(x) \in \mathbb{F}_p[x]$ be the reduction of $f(x)$ modulo p. Let E_p be the splitting field of $f_p(x)$ over $\mathbb{F}_p$. Let R and R_p be the set of roots of $f(x), f_p(x)$ in E, E_p respectively. Let $D \subset E$ be the smallest subring of E containing R. Then*

1. *$\exists$ a ring homo. $\psi : D \twoheadrightarrow E_p$.*
2. *Any such ψ gives a bijection $R \xrightarrow{\text{1-1}} R_p$.*
3. *If ψ, ψ' are two ring homos. satisfying 1 then $\exists \sigma \in G(E, \mathbb{Q})$ s.t. $\psi' = \psi\sigma$.*

Proof. 1. In E, write

$$f(x) = (x - r_1)\cdots(x - r_n)$$

with $R = \{r_1, \ldots, r_n\}$. The r_i's are distinct since $d \neq 0$. Let

$$D = \mathbb{Z}[r_1, \ldots, r_n] = \mathbb{Z}\text{-linear span in } E \text{ of elts. } r_1^{e_1}\cdots r_n^{e_n}.$$

Since $f(r_j) = 0$, r_j^n can be expressed as a $\mathbb{Z}$-linear comb. of r_j^m with $m < n$; so we may use the span of elts. of the above form with $e_j < n\ \forall j$. D is torsion-free, since $D \subset E$, and so it is a f.g. torsion free $\mathbb{Z}$-module. So

$$D = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_N,$$

for some basis $u_1, \ldots, u_N$.

Claim. $\{u_j\}$ forms a basis for E over $\mathbb{Q}$.

Proof. Any relation over $\mathbb{Q}$ among the u_j's gives, after clearing denominators, a relation over $\mathbb{Z}$. Hence $\{u_j\}$ is linearly indep. over $\mathbb{Q}$.

Let

$$S = \mathbb{Q}u_1 \oplus \cdots \oplus \mathbb{Q}u_N.$$

S is a subring of E containing $\mathbb{Q}$, and every elt. of S is algebraic over $\mathbb{Q}$. So the inverse of each elt. is a poly. in that elt. So S is a field. Since $r_j \in S\ \forall j$, $S = E$.

Proof of theorem (cont.) By the claim, $[E : \mathbb{Q}] = N$. Let

$$pD = \mathbb{Z}(pu_1) \oplus \mathbb{Z}(pu_2) \oplus \cdots \oplus \mathbb{Z}(pu_N) \subset D,$$

so $p \in \mathrm{Ann}(D/pD)$. pD is an ideal in D and $|D/pD| = p^N$. Let M be a maximal ideal of D containing pD. Then

$$\frac{D/pD}{M/pD} \cong D/M,$$

so $|D/M|$ divides p^N, and $p \in \mathrm{Ann}(D/M)$. Thus the field D/M has characteristic p.

$$\mathbb{Z}[r_1, \ldots, r_n] = D \quad \overset{\psi}{\longmapsto\!\!\!\!\rightarrow} \quad D/M.$$

So $D/M \cong (\mathbb{Z}/p)[\overline{r_1}, \ldots, \overline{r_n}]$, where $r_j := \psi r_j$.

$$\therefore\ \psi(f(x)) = (x - \overline{r_1}) \cdots (x - \overline{r_n})$$

is a factorization of $f_p(x)$ in the extension field D/M of $\mathbb{F}_p$. Hence $D/M = E_p$.

Let $\psi : D \mapsto E_p$ be a homomorphism. $\psi|_{\mathbb{Z}}$ is reduction mod p, so

$$f_p(x) = \psi(f(x)) = (x - \psi(r_1)) \cdots (x - \psi(r_n)).$$

Hence $\{\psi(r_j)\}$ are the roots of $f_p(x)$. That is, $\{\psi(r_j)\} = R_p$, so $\psi : R \overset{1\text{-}1}{\longmapsto} R_p$.

Let $\psi : D \mapsto E_p$. Let $\sigma \in G = G(E, \mathbb{Q})$. σ permutes roots, so $\sigma : D \mapsto D$. If $\sigma \neq \sigma'$ then σ, σ' are different permutations of the roots, so since ψ is a bijection on roots, $\psi\sigma \neq \psi\sigma'$.

Let

$$G = \{\sigma_1, \ldots, \sigma_N\}.$$

Then $\psi_1 = \psi\sigma_1, \ldots, \psi_N = \psi\sigma_N$ are N distinct ring homomorphisms. Suppose

$$\psi' : D \mapsto E_p$$

is a ring homo distinct from $\psi_1, \ldots, \psi_N$. Then $\{\psi_1, \ldots, \psi_N, \psi'\}$ are linearly independent in $\hom_{\mathbb{Z}}(D, E_p)$ (by Theorem 3.8.2).

However,

$$x_1\psi_1(u_j) + x_2\psi_2(u_j) + \cdots + x_N\psi_N(u_j) + x_{N+1}\psi'(u_j) = 0 \quad 1 \leq j \leq N$$

forms a system of N equations in $N+1$ variables in E_p, so it has a nontrivial solution $(a_1, \ldots, a_{N+1})$ in E_p. For an arbitrary element $y = \eta_1 u_1 + \eta_2 u_2 + \cdots + \eta_N u_N \in D$,

$$\psi_i(y) = \overline{\eta_1}\psi_i u_1 + \overline{\eta_2}\psi_i u_2 + \cdots + \overline{\eta_N}\psi_i u_N.$$

$\therefore a_1\psi_1(y) + a_2\psi_2(y) + \cdots + a_N\psi_N(y) + a_{n+1}\psi'(y) = \sum_j \sum_i \eta_j a_i \psi_i(u_j) = \sum_j \eta_j \cdot 0 = 0$. Hence,

$$a_1\psi_1 + a_2\psi_2 + \cdots + a_N\psi_N + a_{N+1}\psi' = 0$$

in $\hom_{\mathbb{Z}}(D, E_p)$, contradicting the linear independence of $\{\psi_1, \ldots, \psi_N, \psi'\}$.

So $\psi_1, \ldots, \psi_N$ is the complete list of ring homos. from D to E_p. ie. Any ring homo. $\psi' : D \mapsto E_p$ equals $\psi\sigma$ for some $\sigma \in G$.

$\square$

Theorem 3.17.2. *Let $f(x) \in \mathbb{Z}[x]$ be monic. Let p be prime s.t. $p \nmid$ discriminant of $f(x)$. Suppose that in $(\mathbb{Z}/p)[x]$, $f_p(x)$ factors as*

$$f_p(x) = g_1 g_2 \cdots g_r,$$

where g_j is irreducible. Let $n_j = \deg g_j$, so $n = \deg f = n_1 + \cdots + n_r$. Then in $G = \mathrm{Gal}(f(x)) \subset S_n$, there is a permutation whose cycle decomposition (after suitably ordering the roots) is

$$(1\ 2\ \cdots\ n_1)(n_1+1\ \cdots\ n_1+n_2)(n_1+n_2+1\ \cdots\ n_1+n_2+n_3)\cdots(n_1+\cdots+n_{r-1}+1\ \cdots\ n_1+\cdots+n_r).$$

Example 3.17.3.

1. *Let $f(x) = x^3 - 2$. For $p = 5$,*

$$f_5(x) = (2 + x)(4 + 3x + x^2)$$

   $\therefore$ G contains (using some ordering of the roots) the permutation $(1)(2\ 3)$, usually written just $(2\ 3)$. ie. G contains a transposition.

   For $p = 7$, $f_7(x) = x^3 + 5$, which is irreducible. So G contains (using some ordering of the roots, not necessarily the same one as before) the cycle $(1\ 2\ 3)$. ie. G contains a 3-cycle.

   This identifies G as S_3 since no proper subgroup of S_3 contains both a 3-cycle and a transposition.

2. *Let $f(x) = x^3 - 12x + 8$. For all primes, either $f(x)$ is irreducible mod p (yielding a 3-cycle $(1\ 2\ 3) \in G$) or $f(x)$ splits linearly (corresponding to the identity in G). For no prime does it factor as an irreducible quadratic and a linear factor.*

Proof. Let $\phi : E_p \mapsto E_p$ be the Frobenius automorphism $\phi(x) = x^p$, as seen in Example 3.10.10. Let $\psi : D \mapsto E_p$ be a ring homomorphism. Then so is $\phi\psi$. By the preceding theorem, $\exists \sigma \in G$ s.t. $\phi\psi = \psi\sigma$.

Restricted to $R = \{\text{roots}\}$, ψ has an inverse, so we get

$$\sigma = \psi^{-1}\phi\psi,$$

when restricted to R. ie. The action of ϕ as a permutation on R corresponds to that of ϕ on R_p under the bijection ψ. So the cycle decompositions are the same. ϕ maps one root of each g_j to another root of the same g_j (and its restriction to those roots is transitive, since ϕ generates $\mathrm{Gal}(E_p, \mathbb{F}_p)$). ie. The cycle decomposition of ϕ is as shown, and therefore so is that of σ. □

Example 3.17.4. *Let $f(x) = x^5 - 5x + 12$. Since f is irreducible, G contains a 5-cycle.*

$$f_3(x) = x(2 + x + x^2)(2 + 2x + x^2).$$

$\therefore$ G contains a product of 2-cycles, $(1\ 2)(3\ 4)$ (in some ordering).

We can search for other primes which might give other decompositions, but we don't find any (except for complete factorizations into linear pieces, corresponding to $e \in G$). How do we know when to stop? According to Chebotorev Density Theorem, every decomposition that appears must appear at least once for some prime $\leq 70(\log d)^2$, where d is the discriminant. In this case, $70(\log d)^2 \approx 22616$, which by the Prime Number Thm. includes approximately the first $2256 \approx \log(22616)$ primes. In fact, the 2526^{th} prime is $22619 > 22616$. So if we haven't found any other cycle decompositions in the first 2525 primes then there aren't any others. Since the only subgroups of S_5 containing only the 5-cycles, products of two 2-cycles, and the identity are the copies of D_5, $G = D_5$ for

$$f(x) = x^5 - 5x + 12.$$

Chapter 4

Representations of Groups

4.1 Definitions and Elementary Properties

Let G be a group and K a commutative ring.
A (linear) **representation** of G consists of a K-module V and an action $G \times V \mapsto V$ satisfying

$$g \cdot (av + bw) = ag \cdot v + bg \cdot w \quad \forall g \in G,\ a, b \in K,\ v, w \in W.$$

Equivalently, a rep. is a group homomorphism $G \mapsto \mathrm{Aut}_K(V)$.

Another formulation: Define a ring $K[G]$, called the **group ring**, as follows. As an abelian group,

$$K[G] = \{\text{free } K\text{-module with basis } G\}.$$

Multiplication is determined by $g \cdot h = gh$ (the left defines multiplication in $K[G]$; the right is multiplication in G). Then a rep. of G on V is a ring homomorphism $K[G] \mapsto \mathrm{End}_K(V)$. This makes V a left $K[G]$-module.

Note that as rings,

$$K[G \times H] = K[G] \otimes_{\mathbb{Z}} K[H].$$

$K[G]$ is commutative $\iff G$ is abelian.

Let G be finite. For a conjugacy class C, let

$$N_C := \sum_{x \in C} x \in K[G].$$

Definition 4.1.1. *Let R be a ring. The **center** of R is*

$$\mathrm{Z}(R) = \{a \in R \mid ax = xa\ \forall x \in R\}.$$

Proposition 4.1.2. *If G is finite then $\mathrm{Z}(K[G])$ is the free K-module*

$$KN_{C_1} \oplus \cdots \oplus KN_{C_k},$$

where $C_1, \ldots, C_k$ are the conjugacy classes of G.

Proof. For $g \in G$, and $C = C_j$,

$$g^{-1}N_C g = \sum_{x \in C} g^{-1}xg = \sum_{y \in g^{-1}Cg} y = N_C,$$

since $g^{-1}Cg = C$. Thus,

$$\bigoplus_{j=1}^{k} KN_j \subset \mathrm{Z}(K[G]).$$

Conversely, let

$$x = \sum_{g \in G} a_g g \in \mathrm{Z}(K[G]).$$

Then for all $h \in G$,

$$\begin{aligned} \sum_{g \in G} a_g g &= x \\ &= h^{-1}xh \\ &= \sum_{g \in G} a_g h^{-1} g h \\ &= \sum_{t \in G} a_{hth^{-1}} t. \end{aligned}$$

$\therefore a_g = a_{hgh^{-1}}\ \forall h, g.$ ie. All elements of a given conjugacy class have the same coefficient in x. Thus,

$$x = \sum a_j N_{C_j}$$

where $a_j = a_g$ for any $g \in C_j$. So $x \in \bigoplus_{j=1}^{k} KN_{C_j}$. □

4.1.1 New Representations from Old

1. Direct sum of reps.
   Given reps.

$$G \times V \mapsto V \qquad G \times W \mapsto W,$$

form rep. of G on $V \oplus W$ by

$$g \cdot (v, w) = (g \cdot v, g \cdot w).$$

eg. If K is a field, $n = \dim V, m = \dim W$, then for $g \in G$, $\rho(g) \in GL_n(K), \tau(g) \in GL_m(K)$. The direct sum action is given by

$$\begin{pmatrix} \rho(g) & 0 \\ 0 & \tau(g) \end{pmatrix}.$$

Note: Sometimes write kV for $\overbrace{V \oplus \cdots \oplus V}^{k \text{ times}}$.

2. Tensor product of reps.
   Given reps.

$$G \times V \mapsto V \qquad G \times W \mapsto W,$$

form rep of G on $V \otimes_K W$ determined by

$$g \cdot (v \otimes w) = (g \cdot v) \otimes (g \cdot w).$$

This is the tensor product of V and W in the Hopf alg. sense. ie. The action is

$$K[G] \otimes V \otimes W \overset{\psi}{\longmapsto} K[G] \otimes K[G] \otimes V \otimes W \mapsto K[G] \otimes V \otimes K[G] \otimes W \overset{\mu_V \otimes \mu_W}{\longmapsto} V \otimes W,$$

where $\psi(g) = g \otimes g$ is induced by the diagonal map $G \mapsto G \times G$.

Let R be a ring. Recall that an R-module V is simple if it has no proper R-submodules except 0. In this context, such modules will often be called **irreducible**.

Definition 4.1.3. *An R-module $V \neq 0$ is called **indecomposable** if $\nexists$ R-modules $V_1 \neq 0, V_2 \neq 0$ s.t. $V \cong V_1 \oplus V_2$.*

When $R = K[G]$, we talk of "indecomposable reps." and "irreducible" (or "simple") reps.

Clearly, irreducible $\Rightarrow$ indecomposable. The reverse is not true. eg. Suppose K is a field. If the action of each elt. g of G has the form

$$\begin{pmatrix} P(g) & Q(g) \\ 0 & R(g) \end{pmatrix},$$

(where $P(g)$ is $n \times n$, $Q(g)$ is $n \times m$, $R(g)$ is $m \times m$), then $\exists$ an n-dim. subrepresentation $g \mapsto P(g)$, so not irreducible. But it might still be indecomposable if $Q(g) \neq 0$. In particular, take $G = \mathbb{Z}$, $n = m = 1$, let $P(k) = R(k) = 1$ and $Q(k) = k$ for all $k \in \mathbb{Z}$.

Goal: Let G be finite, K a field.

1. Show that there is (up to iso.) a finite list $V_1, \ldots, V_k$ of indecomposable $K[G]$-modules and find them.

2. Given a rep. V of G, show that the decomposition

$$V \cong V_1^{n_1} \oplus V_2^{n_2} \oplus \cdots \oplus V_k^{n_k}$$

into irreducible is unique, and give a method of determining the mult. n_k of each V_k.

3. In particular, find the decomposition

$$K[G] \cong V_1^{n_1} \oplus V_2^{n_2} \oplus \cdots \oplus V_k^{n_k}.$$

Question. Given G, to what extent does this answer change with K? Does it depend on more that just char K?

4.2 Semisimple Rings

Note: Unless otherwise noted, module means left module.

Definition 4.2.1. *An R-module V is called* ***semisimple*** *if it is a direct sum of simple modules. R is called a* ***semisimple ring*** *if R is semisimple as a (left) R-module.*

Proposition 4.2.2. *If V is a semisimple module and $U \subset V$ then $V \cong U \oplus W$ for some W.*

Proof. Consider

$$S = \{\text{submodules } U' \subset V \text{ s.t. } U \cap U' = 0\}.$$

By Zorn's lemma, let $W \subset V$ be maximal s.t. $U \cap W = 0$. If $U \oplus W \subsetneq V$, choose $v \notin U \oplus W$. Write $v = v_1 + \cdots + v_n$, where $v_i \in V_i$ and $V_i \subset V$ is simple. Then $v_j \notin U \oplus W$ for some j. So

$$V_j \cap (U \oplus W) \subsetneq V_j$$

and since V_j is simple,

$$V_j \cap (U \oplus W) = 0.$$

But then $U \cap (W \oplus V_j) = 0$, so W is not maximal. Thus, $V = U \oplus W$. □

Definition 4.2.3. *V is* ***completely splittable*** *if $U \subset V \Rightarrow V = U \oplus W$ for some W.*

So V is semisimple $\Rightarrow$ V is completely splittable. Recalling Proposition 2.4.6, we see that V is completely splittable $\iff$ whenever $U \subset V$, if $i : U \hookrightarrow V$ is the inclusion then $\exists \sigma : V \mapsto U$ a homo. s.t. $\sigma i = 1_U$; σ is called a splitting of i.

Example 4.2.4. *Let K be a field, $R = M_{n\times n}(K)$,*

$$V = \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \cdots & 0 \end{pmatrix}.$$

Claim. *V is a simple R-module.*

Proof of claim. Suppose $0 \subsetneq W \subset V$. Let

$$0 \neq x = \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{pmatrix} \in W,$$

and suppose $x_j \neq 0$. Then W contains

$$\begin{pmatrix} 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix} x = \begin{pmatrix} x_j & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \vdots \\ 0 & & \cdots & 0 \end{pmatrix}.$$

By dividing by x_j, W contains

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \vdots \\ 0 & & \cdots & 0 \end{pmatrix}.$$

Thus, W contains

$$\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \\ 1 & & \vdots \\ \vdots & & \\ 0 & \cdots & 0 \end{pmatrix},$$

which is a basis of V. Hence $W = V$. $\square$

Now,

$$R = \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \cdots & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & * & 0 & \cdots & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & * & 0 & \cdots & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & \cdots & 0 & * \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & * \end{pmatrix}.$$

So R is semisimple.

Proposition 4.2.5. $\mathrm{Z}(M_{n\times n}(K)) = KI$.

Proof. Exercise. $\square$

Let R be a ring, $x, y \in R$. The **commutator** of x and y is

$$[x, y] := xy - yx \in R.$$

The **commutator subspace** is

$$[R, R] = \{[x, y] \mid x, y \in R\}.$$

Note: $[R, R]$ is not an R-submodule of R, in general.

Example 4.2.6. *Let $R = M_{n\times n}(K)$. Then*

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & & \ddots & \\ 0 & \cdots & & & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & & \ddots & \\ 0 & \cdots & & & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & & \ddots & \\ 0 & \cdots & & & 0 \end{pmatrix} - \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & & \ddots & \\ 0 & \cdots & & & 0 \end{pmatrix}.$$

Similarly, denoting by e^{ij} the matrix with 1 in the $(i, j)^{th}$ position and 0 elsewhere,

$$e^{ij} \in [R, R] \quad \forall i \neq j.$$

Also,

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & & \ddots & \\ 0 & \cdots & & & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & & \vdots \\ 0 & & & \\ \vdots & & \ddots & \\ 0 & \cdots & & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & & \vdots \\ 0 & & & \\ \vdots & & \ddots & \\ 0 & \cdots & & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & & \ddots & \\ 0 & \cdots & & & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & 0 \end{pmatrix}$$

Similarly,

$$\begin{pmatrix} 1 & 0 & & & \cdots & & & 0 \\ 0 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & & & & \\ \vdots & & & & -1 & & & \vdots \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ 0 & & & & \cdots & & & 0 \end{pmatrix} \in [R, R].$$

These matrices generate $\{M \mid \mathrm{Tr} M = 0\}$ *as a vector space. That is,*

$$[R, R] = \ker \mathrm{Tr} : R \mapsto K.$$

In particular, $\dim[R, R] = n^2 - 1$ *and* $\dim(R/[R, R]) = 1$.

Lemma 4.2.7. *If* V *is completely splittable and* $U \subset V$ *then* U *is completely splittable.*

Proof. Let $T \subset U$. Then

$$\begin{tikzcd} T \arrow[r, hook, "i"] \arrow[drr, "1_T"'] & U \arrow[r, hook, "j"] & V \arrow[d, "\exists\sigma"] \\ & & T \end{tikzcd}$$

Since V is completely splittable, $\exists\sigma$ s.t. $\sigma \circ ji = 1_T$, as in the diagram. So $\sigma \circ j$ is a splitting of i. ◻

Theorem 4.2.8. *If* V *is completely splittable then every submodule of* V *is semisimple.*

Corollary 4.2.9. V *is semisimple* $\iff$ V *is completely splittable.*

Corollary 4.2.10. *If* V *is semisimple then every submodule of* V *is semisimple.*

Proof of Theorem. Let $U \subset V$. Consider sets $\{S_i\}_{i \in I}$ of simple U-submodules which are "linearly independent", ie.

$$\langle S_i \rangle_{i \in I} = \bigoplus_{i \in I} S_i.$$

By Zorn's lemma, there is a maximal such set, $\{S_i\}_{i \in I}$. Let

$$S = \bigoplus_{i \in I} S_i.$$

By the lemma, S is completely splittable, so $\exists T$ s.t. $U = S \oplus T$. If $T \neq 0$, pick $0 \neq x \in T$. By Zorn's lemma,

$$\{T' \subset T \mid x \notin T'\}$$

has a maximal element, T_0. By the lemma, let T_1 be s.t.

$$T = T_0 \oplus T_1.$$

If T_1 is not simple then let $T_1 = A \oplus B$. x can't be in both $T_0 \oplus A$ and $T_0 \oplus B$ since their intersection is T_0. This contradicts the maximality of T_0, so T_1 is simple.

But T_1 can be added to $\{S_i\}_{i \in I}$ to get a still-linearly independent set of simple submodules. This contradicts the maximality of $\{S_i\}_{i \in I}$.

So $T = 0$ and $U = S = \bigoplus_{i \in I} S_i$ is semisimple. ◻

Corollary 4.2.11. *Let*

$$0 \to U \to V \to W \to 0$$

be a short exact sequence of R-modules. If V is semisimple then U, W are semisimple.

Proof. $V \cong U \oplus W$, so $U \subset V$ and V has a submodule isomorphic to W. So by the theorem, U and W are semisimple. □

Theorem 4.2.12 (Maschke)**.** *If K is a field, G a finite group s.t.* $\operatorname{char} K \nmid |G|$ *then* $K[G]$ *is semisimple.*

Proof. Write $V = K[G]$, as a module over itself. Suppose U is a $K[G]$-submodule, and show that there exists a K-module splitting $p : V \mapsto U$.

As vector spaces, $\exists U_0$ s.t. $V \cong U \oplus U_0$ (U_0 is not necessarily a $K[G]$-module). This yields a linear map $p_0 : V \mapsto U$ (p_0 is not necessarily a $K[G]$-homomorphism).

Define $p : V \mapsto U$ by

$$p(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} p_0(gv).$$

Then for $g' \in G$,

$$\begin{aligned} p(g'v) &= \frac{1}{|G|} \sum_{g \in G} g^{-1} p_0(gg'v) \\ &= \frac{1}{|G|} \sum_{f \in G} g' f^{-1} p_0(fv) \\ &= g' \frac{1}{|G|} \sum_{f \in G} f^{-1} p_0(fv) \\ &= g' p(v). \end{aligned}$$

So p is a $K[G]$-homomorphism.

Also, if $u \in U$ then

$$\begin{aligned} p(u) &= \frac{1}{|G|} \sum_{g \in G} g^{-1} p_0(gu) \\ &= \frac{1}{|G|} \sum_{g \in G} g^{-1}(gu) \\ &= \frac{1}{|G|} \sum_{g \in G} u \\ &= u. \end{aligned}$$

$\therefore$ p is a splitting. □

Note: If K is not a field then the same proof works, provided $|G|$ is invertible in R and $\exists$ an R-module splitting $p_0 : V \mapsto U$.

Let R be a semisimple ring,

$$R \cong \bigoplus_{i \in I} V_i$$

where each V_i is simple.

Proposition 4.2.13. *Ever simple R-module appears (up to isomorphism) as V_i for some i.*

Proof. Let W be a simple R-module and $0 \neq w \in W$. Then

$$\begin{array}{ccc} R & \overset{\phi}{\longmapsto} & W \\ 1 & \longmapsto & w \end{array}$$

is not zero, so it is onto (since W is simple).

So W is a summand of R. Furthermore,

$$0 \neq \phi \in \hom_R(R, W) \cong \bigoplus_{i \in I} \hom_R(V_i, W),$$

so $\hom_R(V_i, W) \neq 0$ for some i. But any non-zero homo. between simple R-modules is an isomorphism, so W is isomorphic to some V_i. $\square$

Proposition 4.2.14. *Let R be semisimple, $I \subset R$ a left ideal. Then $\exists$ an idempotent $e \in R$ s.t. $I = Re$.*

Note: If V is a simple R-module then $Rv = V$, for any $v \in V$. Moreover, since R is semisimple, $R \mapsto\!\!\!\rightarrow Rv$ splits, so V is isomorphic to a left ideal of R.

Proof. Since R is semisimple, $\exists J$ s.t. $R = I \oplus J$. Write $1 = e + f$ where $e \in I, f \in J$.

$e \in I \Rightarrow Re \subset I$. Conversely, given $x \in I$, $x = xe + xf$. $xf = x - xe \in I$ and since $f \in J$, $xf \in J$. Thus

$$xf \in I \cap J = 0 \Rightarrow \ x = xe.$$

$\therefore I = Re$.

Now, $x = xe \ \forall x \in I$, and in particular, $e = e^2$. $\square$

4.3 Artinian Rings

Recall that an R-module V is Noetherian if for any chain

$$V_0 \subset V_1 \subset \cdots \subset V_n \subset \cdots$$

of submodules, $\exists N$ s.t. $V_n = V_N \ \forall n \geq N$. Likewise:

Definition 4.3.1. *An R-module V is* ***Artinian*** *if for any chain*

$$V_0 \supset V_1 \supset \cdots \supset V_n \supset \cdots$$

of submodules, $\exists N$ s.t. $V_n = V_N \ \forall n \geq N$. R is an ***Artinian ring*** *if R is Artinian as a (left) R-module.*

Example 4.3.2. *$\mathbb{Z}$ is Noetherian (in fact, it is a PID) but not Artinian, since we have:*

$$2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots \supset 2^n\mathbb{Z} \supset \cdots .$$

When G is finite and K is a field, $K[G]$ is both Noetherian and Artinian (by counting dimensions, can't have a strictly increasing chain longer than $|G| + 1$).

Proposition 4.3.3. *Let*

$$0 \to U \to V \to W \to 0$$

be a short exact sequence of R-modules. Then V is Noetherian (respectively Artinian) $\iff U, W$ are Noetherian (resp. Artinian).

Corollary 4.3.4. *If*

$$V = \bigoplus_{i=1}^{n} V_i$$

then V is Noetherian (resp. Artinian) $\iff V_i$ is Noetherian (resp. Artinian) $\forall i$.

Proposition 4.3.5. *If*

$$V = \bigoplus_{i \in I} V_i$$

with $V_i \neq 0$ and V is finitely generated then $|I| < \infty$.

Proof. Each generator has only finitely many non-zero components. □

Corollary 4.3.6. *If V is finitely generated and semisimple then V is both Noetherian and Artinian.*

Proof. By the hypothesis,

$$V = \bigoplus_{i=1}^{n} V_i$$

where each V_i is simple. So for each i, the only chain is $0 \subset V_i$. Thus V_i is both Noetherian and Artinian. $\square$

Corollary 4.3.7. *If R is semisimple then R is both Noetherian and Artinian.*

Proof. As an R-module, R is generated by the single element 1. $\square$

Proposition 4.3.8. *Let G be finite, K Noetherian (resp. Artinian). Then $K[G]$ is Noetherian (resp. Artinian).*

Proof. If K is Noetherian (or Artinian) then, as a K-module, so is $K^{|G|}$, which is isomorphic, as a K-module, to $K[G]$. But every $K[G]$-submodule of $K[G]$ is a K-submodule, so if $K[G]$ is Noetherian (or Artinian) as a K-module then it has the same property as a $K[G]$-module. $\square$

Lemma 4.3.9 (Schur)**.** *Let V be a simple R-module. Then:*

1. $\mathrm{End}_R(V)$ *forms a division ring.*
2. *If R is a finite dimensional algebra (eg. $R = K[G]$ with G finite) over an algebraically closed field K then* $\mathrm{End}_R(V) \cong K$.

Proof.

1. If $f : V \mapsto V$ is nonzero then $\mathrm{Im} f = V$ so V is onto. Also, since $f \neq 0$, $\ker f \neq V$, so $\ker f = 0$. Hence f is an isomorphism, so it has an inverse. ie. $\mathrm{End}_R(V)$ is a division ring.
2. Let $f \in \mathrm{End}_R(V)$, and show $f = \lambda I$ for some $\lambda \in K$. For any $0 \neq x \in V$, Rx forms a finite dimensional subspace of V (its dimension is $\leq \dim R$). Since V is simple, $Rx = V$, so V is finite dimensional.

   So $\exists$ an eigenvector $0 \neq v \in V$ for f, so that $fv = \lambda v$. Since V is simple, $Rv = V$. Hence $\forall w \in V$, $w = rv$ so
   $$f(w) = rf(v) = \lambda rv = \lambda w.$$
   ie. $f = \lambda I$.

$\square$

4.4 Wedderburn's Theorem

Let R be semisimple. Then

$$R \cong n_1 V_1 \oplus n_2 V_2 \oplus \cdots \oplus n_k V_k$$

where $V_1, \ldots, V_k$ is the list of simple R-modules (one from each isomorphism class). (This is a finite decomposition by Proposition 4.3.5)

For a ring A,

$$\begin{aligned} A &\overset{\phi}{\longmapsto} \mathrm{End}_A(A) \\ A &\longmapsto \phi_a \\ \phi_a(b) = ba \end{aligned}$$

is a bijection, since every endomorphism f is equal to $\phi_{f(1)}$. Then

$$\phi_a \phi_b(1) = \phi_a(b) = ba = \phi_{ba}(1).$$

$\therefore \phi$ is a ring isomorphism

$$\phi : A^{\mathrm{opp}} \mapsto \mathrm{End}_A(A),$$

where A^{opp} is the ring with the same group structure as A but $a(\cdot_{\mathrm{opp}})b = ba$.

Set $D_j = \mathrm{End}_R(V_j)$, a division ring. Then

$$\begin{aligned} R &\cong (\mathrm{End}_R(R))^{\mathrm{opp}} \\ &\cong \prod_{j=1}^{k} \Big(\mathrm{End}_R(n_j V_j)\Big)^{\mathrm{opp}} \\ &\cong \prod_{j=1}^{k} \Big(M_{n_j \times n_j}(\mathrm{End}_R(V_j)\Big)^{\mathrm{opp}} \\ &\cong \prod_{j=1}^{k} \Big(M_{n_j \times n_j}(D_j)\Big)^{\mathrm{opp}} \\ &\cong \prod_{j=1}^{k} M_{n_j \times n_j}(D_j^{\mathrm{opp}}) \end{aligned}$$

where on the last line, the isomorphism is given by the transpose map.

Under this isomorphism, $V_j \subset n_j V_j \subset R$ corresponds to

$$\hom_R(n_j V_j, V_j) \cong \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \cdots & 0 \end{pmatrix} \subset M_{n_j \times n_j}(D_j^{\mathrm{opp}}).$$

In particular, suppose R is an algebra over a field K and $D_j \cong K$ (eg. if K is algebraically closed). Then:

1. $\dim V_j = n_j$ for each j.
2. $\dim R = \sum_{j=1}^{k} n_j^2$.

Example 4.4.1.

1. $R = \mathbb{C}(S_2)$
By Maschke's Theorem, $\operatorname{char} K = 0 \Rightarrow K[G]$ *is semisimple. Here,*

$$2 = 1^2 + 1^2$$

and there are no other possibilities, so R has 2 *indecomposable reps., each on a* 1*-dimensional space.*

They are: Let $\dim V = 1$ *with basis v.* $S_2 = \{e, T\}$*, with* $T^2 = e$*. The trivial rep. is:*

$$e \cdot v = v,$$
$$T \cdot v = v.$$

The sign rep. is:

$$e \cdot v = v,$$
$$T \cdot v = -v.$$

2. $R = \mathbb{C}(S_3)$
Either

$$6 = 1^2 + 1^2 + \cdots + 1^2 \qquad \text{or} \qquad 6 = 1^2 + 1^2 + 2^2.$$

Easy to see that the trivial rep. and the sign rep. ($\sigma \cdot v = (-1)^{\operatorname{sgn}\sigma} v$, sgn *is the homomorphism* $\epsilon : S_n \mapsto \{1, -1\}$ *used to define* A_n *in section 1.6.2) are the only possible reps. of R on a* 1*-dim. V. Hence R has* 3 *indecomposable reps.: trivial rep., sign rep., a* 2*-dim. rep.*

The 2*-dim. rep. is:*

$$(1\ 2) \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix},$$
$$(1\ 3) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$(1\ 2\ 3) = (1\ 2)(1\ 3) \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

3. $R = \mathbb{C}(S_4)$

$$24 = 1^2 + 1^2 + (a)^2 + \cdots + (\ )^2, \quad a \geq 2.$$

Looking at congruence $\bmod 4$*, need* 3^2 *(*$2^2, 4^2$ *are divisible by* 4*, but* $24 - 1^2 - 1^2$ *is not). Hence, the only possibility is*

$$24 = 1^2 + 1^2 + 2^2 + 3^2 + 3^2.$$

ie. two 1*-dim. reps., one* 2*-dim. rep., two* 3*-dim. reps.*

Theorem 4.4.2. *Let G be a finite group, K an algebraically closed field of characteristic* 0*. Then the number of isomorphic simple $K[G]$-modules is equal to the number of conjugacy classes of G.*

Proof. As seen earlier,

$$\mathrm{Z}(K[G]) = \text{Free } K\text{-module on } \left\{ \sum_{g \in C} g \mid C \text{ a conj. class} \right\}.$$

So the number of conjugacy classes is equal to $\dim \mathrm{Z}(K[G])$. Also,

$$K[G] = \prod_{j=1}^{k} M_{n_j \times n_j}(K).$$

Now, $\mathrm{Z}(M_{n\times n}(K)) = KI$, which has dimension 1. Thus,

$$\dim \mathrm{Z}(K[G]) = k = \#\text{ nonisomorphic simple } K[G]\text{-modules}.$$

$\square$

4.5 Changing the Ground Ring

Example 4.5.1. *Let $G = C_3 = \{e, t, t^2\}$, $K = \mathbb{R}$. Then using $V = \mathbb{R}^2$,*

$$\begin{aligned} \rho : K[G] &\mapsto M_2(\mathbb{R}) \\ t &\mapsto \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix}. \end{aligned}$$

(ρ is rotation by $\frac{2\pi}{3}$.) Then ρ is indecomposable. But if we use $K = \mathbb{C}$, and $\tilde{\rho} : \mathbb{C}[G] \mapsto M_2(\mathbb{C})$ induced by the same representation, then $\tilde{\rho}$ is decomposable since over $\mathbb{C}$, we can change basis and diagonalize:

$$\tilde{\rho}(t) = \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{\frac{4\pi i}{3}} \end{pmatrix},$$

in an appropriate basis.

Given $f : R \mapsto S$ a ring homomorphism, f induces a functor

$$\begin{aligned} \{\text{(left) } R\text{-mods.}\} &\mapsto \{\text{(left) } S\text{-mods.}\} \\ V &\mapsto V_S := S \otimes_R V. \end{aligned}$$

The map f makes S a two-sided R-module (and in particular, a right module), so $S \otimes_R V$ makes sense. $S \otimes_R V$ is an S-module via the action

$$s'(s \otimes v) = (s's) \otimes v.$$

If

$$0 \to U \to V \to W \to 0$$

is a short exact sequence of left R-modules and M is a right R-module then

$$M \otimes_R U \to M \otimes_R V \to M \otimes_R W \to 0$$

is exact, although the first map may not be injective. However, if M is a free R-module, $M \cong R^n$ then $M \otimes_R N \cong N^n$, and so

$$M \otimes_R U \hookrightarrow M \otimes_R V$$

in this case.

In particular, if $f : R \hookrightarrow S$ makes S into a free R-module then when

$$0 \to U \to V \to W \to 0$$

is exact, so is

$$0 \to U_S \to V_S \to W_S \to 0,$$

ie. $(V/U)_S \cong V_S/U_S$.

In particular, if $K \subset M$ is a field extension then M is a free K-module.

$f : K \mapsto M$ induces $K[G] \mapsto M[G]$, and thus

$$K[G]\text{-mods.} \mapsto M[G]\text{-mods.}$$
$$V \mapsto V_M$$

ie. $(mg)(m' \otimes v) = (mm' \otimes gv)$, defines $M[G]$-action on V_M.
Note: If $v = kv'$ then $m' \otimes v = m' f(k) \otimes v'$, but then

$$mg(m' \otimes v) = mm' \otimes gv = mm' \otimes kgv' = mm' f(k) \otimes gv' = mg(m' f(k) \otimes v'),$$

so the action is well-defined. Also,

$$g(m(m' \otimes v)) = g(mm' \otimes v) = mm' \otimes gv = m(m' \otimes gv) = mg(m' \otimes v),$$

so the action of g is M-linear.

If $K \subset M$ is a field extension and $n = \dim V < \infty$,

$$\rho : K[G] \mapsto \mathrm{End}_K(V) \cong M_{n\times n}(K)$$

then $\dim V_M = n$ and for the induced map

$$\tilde{\rho} : M[G] \mapsto \mathrm{End}_M(V_M),$$

the matrix $\tilde{\rho}(g)$ for the action of g is just $\rho(g)$, regarded as a matrix in M (whose entries happen to lie in K).

As we have seen, V simple $\not\Rightarrow$ V_M is simple.

4.6 Composition Series

Let V be an R-module.

Definition 4.6.1. *A **composition series** for V consists of a chain of submodules*

$$0 = V_n \subset V_{n-1} \subset \cdots \subset V_1 \subset V_0 = V$$

s.t. V_{j-1}/V_j is simple $\forall j = 1, \ldots, n$.

The composition series

$$0 = V_n \subset \cdots \subset V_0 = V$$

and

$$0 = W_m \subset \cdots \subset W_0 = V$$

are called equivalent if $n = m$ and $\exists \sigma \in S_n$ s.t.

$$V_{j-1}/V_j \cong W_{\sigma(j)-1}/W_{\sigma(j)} \quad \forall j.$$

ie. the list of "composition factors" (including multiplicities) is the same, although the order may be different.

Proposition 4.6.2. *V has a composition series $\iff$ V is both Artinian and Noetherian. In this case, any series can be refined to a composition series.*

Proof.

$\Leftarrow$: Suppose V is Artinian and Noetherian. Let $V_0 = V$. Since V is Noetherian, V contains a maximal (proper) submodule, V_1 (by Theorem 2.6.2). Continuing, so long as $V_j \neq 0$, get

$$V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_j \supsetneq \cdots$$

s.t. V_{j+1} is maximal in V_j, ie. V_j/V_{j+1} is simple. Since V is Artinian, the chain must terminate.

$\Rightarrow$: Suppose

$$0 = V_n \subset \cdots \subset V_0 = V$$

is a composition series. Then we have the exact sequence

$$0 \to V_1 \to V \to V/V_1 \to 0.$$

Since V_1 is simple, V_1 is Artinian and Noetherian. V/V_1 has a composition series of length $n-1$, so by induction, V/V_1 is Artinian and Noetherian. Thus, V is Artinian and Noetherian.

Finally, given any series

$$0 = V_n \subset \cdots \subset V_0 = V,$$

each V_{i-1}/V_i is Noetherian and Artinian, so it has a composition series. Using each of these series, we may refine the given series to a composition series. □

Theorem 4.6.3. *Any two comp. series for V are equivalent.*

Proof. Let

$$0 = V_n \subset \cdots \subset V_0 = V$$

and

$$0 = W_m \subset \cdots \subset W_0 = V$$

be comp. series. For $1 \le i \le n$ and $1 \le j \le m$, set

$$V_{ij} := V_i + (V_{i-1} \cap W_j) \quad \text{and} \quad W_{ji} := W_j + (W_{j-1} \cap W_j).$$

Claim.

$$\frac{V_{i,j-1}}{V_{ij}} \cong \frac{V_{i-1} \cap W_{j-1}}{(V_i \cap W_{j-1}) + (V_{i-1} \cap W_j)} \cong \frac{W_{j,i-1}}{W_{ji}}.$$

Proof of claim. Consider

$$\phi : V_{i-1} \cap W_{j-1} \hookrightarrow V_i + (V_{i-1} \cap W_j - 1) \twoheadrightarrow \frac{V_i + (V_{i-1} \cap W_{j-i})}{V_i + (V_{i-1}} \cap W_j) = \frac{V_{i,j-i}}{V_{ij}}.$$

$V_i \subset V_{ij}$, so every element of $V_{i,j-1}$ is congruent modulo V_{ij} to one in $V_{i-1} \cap W_{j-1}$. ie. ϕ is surjective.

Clearly, $V_{i-1} \cap W_j \subset V_{ij}$, so

$$V_{i-1 \cap W_j} \subset \ker \phi.$$

Also, $V_j \cap W_{j-1} \subset V_i \subset V_{ij}$, so

$$V_i \cap W_{j-1} \subset \ker \phi.$$

Hence,

$$(V_{i-1} \cap W_j) + (V_i \cap W_{j-1}) \subset \ker \phi.$$

Conversely, suppose $x \in V_{i-1} \cap W_{j-1}$ lies in

$$\ker \phi = (V_{i-1} \cap W_{j-1}) \cap (V_i + (V_{i-1} \cap W_j)).$$

Write $x = y + z$ where $y \in V_i$ and $z \in V_{i-1} \cap W_j$. Since $x \in W_{j-1}$ and $z \in W_j \subset W_{j-1}$, it follows that $y \in W_{j-1}$. So

$$x = y + z$$

exhibits x as an elt. of $(V_i \cap W_{j-1}) + (V_{i-1} \cap W_j)$. □

Notice that since V_{i-1}/V_i and W_{j-1}/W_j are simple,

$$\frac{V_{i-1} \cap W_{j-1}}{(V_i \cap W_{j-1}) + (V_{i-1} \cap W_j)}$$

is either 0 or simple.

So we have

$$V = V_0 = V_{10} \supset V_{11} \supset \cdots \supset V_{1m} = V_1 = V_{20} \supset \cdots \supset \cdots \supset V_{n-1} = V_{n0} \supset \cdots \supset V_{nm} = 0. \qquad (*)$$

and similarly,

$$V = W_0 = W_{10} \supset W_{11} \supset \cdots \supset W_{1n} = W_1 = W_{20} \supset \cdots \supset \cdots \supset W_{m-1} = W_{m0} \supset \cdots \supset W_{mn} = 0. \qquad (**)$$

Notice that both chains have the same length, and by the claim, there is a bijection between the quotient modules, each of which is either simple or 0. So by shortening the chains by deleting entries which equal their predecessors, all the 0-quotient modules are deleted, and what is left are composition series. The number of 0-quotients deleted is the same (they are paired), so the resulting comp. series have the same length and same quotients, ie. they are equivalent.

But (*) reduces to

$$V_n \subset \cdots \subset V_0$$

and (**) reduces to

$$W_m \subset \cdots \subset W_0,$$

since they are respectively refinements of these series, and you can't refine a comp. series any further. So these two comp. series are equivalent. ◻

4.7 Characters

Let

$$\rho : K[G] \mapsto \mathrm{End}_K(V)$$

be a rep. of K on a free K-module V. Define

$$\chi_\rho : K[G] \mapsto K,$$

the **character** of ρ by $\chi_\rho = \mathrm{Tr}(\rho(x))$.

Since $\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$, χ_ρ is determined by its values on the basis G for $K[G]$, so sometimes write $\chi_\rho : G \mapsto K$.

Recall that Tr is preserved under change of basis, since

$$\mathrm{Tr}(A^{-1}BA) = \mathrm{Tr}(AA^{-1}B) = \mathrm{Tr}(B).$$

So, if $h = x^{-1}gx$ then

$$\rho(h) = \rho(x)^{-1}\rho(g)\rho(x)$$

and thus, $\chi_\rho(h) = \chi_\rho(g)$.

Proposition 4.7.1. *Let*

$$0 \to U \to V \to W \to 0$$

be a short exact sequence of $K[G]$-modules, each of which is free as a K-module. Then

$$\chi_V = \chi_U + \chi_W.$$

Proof. Since U is a $K[G]$-submodule, for all $g \in U$, the matrix for $\rho(g)$ has the form

$$\rho_V(g) = \begin{pmatrix} \rho_U(g) & * \\ 0 & \rho_W(g) \end{pmatrix}.$$

□

Proposition 4.7.2. $\chi_{V \otimes W} = \chi_V \chi_W$.

Proof. Let $\{e_i\}, \{f_j\}$ be bases for V, W respectively. Then $\{e_i \otimes f_j\}$ is a basis for $V \otimes W$, and

$$(A \otimes B)(e_i \otimes f_j) = a_{ii}b_{jj}(e_i \otimes f_j) + \text{ other terms.}$$

So,

$$\mathrm{Tr}(A \otimes B) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ii}b_{jj} = (\mathrm{Tr}A)(\mathrm{Tr}B).$$

□

Proposition 4.7.3. *Viewing $K[G]$ as a left $K[G]$-module,*

$$\chi_{K[G]}(g) = \begin{cases} |G|, & g = e, \\ 0, & g \neq e. \end{cases}$$

Proof. In the basis $\{g\}_{g \in G}$ for $K[G]$, the action of any elt. of G is given by a permutation matrix. So, by the definition of the trace,

$$\begin{aligned} \chi_{K[G]}(g) &= |\{x \in G \mid gx = x\}| \\ &= \begin{cases} |G|, & g = e, \\ 0, & g \neq e. \end{cases} \end{aligned}$$

□

Corollary 4.7.4. *Suppose*

$$K[G] \cong V_1 \oplus \cdots \oplus V_r$$

and K is a field s.t. char $K \nmid |G|$. *Thus $\chi_{K[G]} = \sum_{i=1}^{r} \chi_i$ where $\chi_i = \chi_{V_i}$.*

Let $y = \sum_{g \in G} c_g g \in K[G]$. Then for any g,

$$c_g = \frac{1}{|G|} \sum_{i=1}^{r} \chi_i(yg^{-1}).$$

Proof. Pick $g \in G$.

$$y = \sum_{h \in G} c_h h = c_g g + \sum_{h \neq g} c_h h.$$

$\therefore yg^{-1} = c_g e + \sum_{h \neq g} c_h hg^{-1}$. Applying $\chi_{K[G]} = \sum_{i=1}^{r} \chi_i$,

$$\begin{aligned} \sum_{i=1}^{r} \chi_i(yg^{-1}) &= \chi_{K[G]}(yg^{-1}) \\ &= c_g \chi_{K[G]}(e) + \sum_{h \neq g} c_h \chi_{K[G]}(hg^{-1}) \\ &= |G| c_g + 0. \end{aligned}$$

□

Set $\mathrm{CF}_K(G) := \{f : G \mapsto K \mid f(y^{-1}xy) = f(x)\ \forall x, y \in G\}$. $\mathrm{CF}_K(G)$ is a ring using addition and multiplication of functions. It is called the ring of **class functions**.

$\mathrm{R}_K(G)$ is the abelian group generated by iso. classes of f.d. reps. of G, with the relation

$$[V] = [V'] + [V'']$$

for every short exact sequence

$$0 \to V' \to V \to V'' \to 0.$$

Define multiplication on $\mathrm{R}_K(G)$ by

$$[V][W] = [V \otimes W].$$

Then the preceeding implies that

$$\begin{aligned} \theta : \mathrm{R}_K(G) &\mapsto \mathrm{CF}_K(G) \\ [\rho] &\mapsto \mathcal{X}_\rho \end{aligned}$$

is a ring homomorphism.

Set $\mathrm{Ch}_K(G) := \mathrm{Im}\theta$, the "ring of generalized K-characters of G", or simply the "character ring of G over K".

Lemma 4.7.5. *Let V, W be $K[G]$-modules and let $f \in \hom_K(V, W)$. Define $\tilde{f} : V \mapsto W$ by*

$$\tilde{f}(v) = \sum_{g \in G} g^{-1} f(gv).$$

Then $\tilde{f} \in \hom_{K[G]}(V, W)$.

If $V = W$ then $\mathrm{Tr}\tilde{f} = |G|\mathrm{Tr}(f)$.

Proof. For $x \in G$,

$$\tilde{f}(xv) = \sum_{g \in G} g^{-1} f(gxv) = \sum_{h \in G} xh^{-1} f(hv) = x\tilde{f}(v).$$

Now suppose $V = W$. Then,

$$\tilde{f} = \sum_{g \in G} M_g^{-1} f M_g$$

where M_g represents the action of g on V. Hence,

$$\begin{aligned} \mathrm{Tr}(\tilde{f}) &= \sum_{g \in G} \mathrm{Tr}(M_g^{-1} f M_g) \\ &= \sum_{g \in G} \mathrm{Tr}(f) \\ &= |G|\mathrm{Tr}(f). \end{aligned}$$

∎

Let K be a field.

Lemma 4.7.6. *Let $\alpha : G \mapsto \mathrm{Aut}_K(V)$, $\beta : G \mapsto \mathrm{Aut}_K(W)$ be non-isomorphic simple reps. Pick bases $v_1, \ldots, v_n$ and $w_1, \ldots, w_m$ for V and W. Let $[\alpha_{ij}(g)]$ and $[\beta_{ij}(g)]$ denote matrices for $\alpha(g), \beta(g)$ in these bases. Then for any i, j, k, t, $1 \le i, j \le n$, $1 \le k, t \le m$,*

$$\sum_{g \in G} \beta_{ij}(g^{-1}) \alpha_{kt}(g) = 0.$$

Proof. Let $f : V \mapsto W$ be the linear transformation which in chosen bases for V and W is given by the matrix E which is 1 in the $(j,k)^{\text{th}}$ position and 0 elsewhere. By the previous lemma, $\tilde{f} \in \hom_{K[G]}(V, W) = 0$ (since V, W are non-isomorphic and simple). The $(i,t)^{\text{th}}$ position of the matrix for $\tilde{f}$ is

$$\begin{aligned} 0 &= \sum_{g \in G} \sum_{r,s} \beta_{ir}(g^{-1}) E_{is} \alpha_{st}(g) \\ &= \sum_{g \in G} \beta_{ij}(g^{-1}) \alpha_{kt}(g), \end{aligned}$$

since $E_{rs} = 0$ except when $r = j, s = k$. □

Corollary 4.7.7. *Let V, W be non-isomorphic simple $K[G]$-modules. Then*

$$\sum_{g \in G} \chi_V(g) \chi_W(g^{-1}) = 0.$$

Proof. Let $\alpha(g), \beta(g)$ be the matrices for the reps. Then

$$\sum_{g \in G} \chi_V(g) \chi_W(g^{-1}) = \sum_g \sum_t \sum_i \alpha_{tt}(g) \beta_{ii}(g^{-1}) = 0.$$

□

Theorem 4.7.8. *Let $\alpha : G \mapsto \mathrm{Aut}_K(V)$ be a simple G-rep. If K is algebraically closed and* $\mathrm{char}\, K = 0$ *then* $\dim Z \mid |G|$ *and*

$$\sum_{g \in G} \alpha_{ij}(g^{-1}) \alpha_{kt}(g) = \delta_{jk} \delta_{it} \frac{|G|}{\dim V}.$$

Proof. Let $f : V \mapsto V$ be the linear transformation which in a chosen basis for V is given by the matrix E which is 1 in the $(j,k)^{\text{th}}$ position and 0 elsewhere. So $\tilde{f} \in \hom_{\mathbb{Z}[G]}(V, V)$. Since V is simple, $\hom_{K[G]}(V, V) = K$, and thus, $\hom_{\mathbb{Z}[G]}(V, V) = \mathbb{Z}$. That is, $\tilde{f} = cI$ for some $c \in \mathbb{Z}$.

As above, the $(i,t)^{\text{th}}$ entry of the matrix for $\tilde{f}$ is

$$\sum_{g\in G} \alpha_{ij}(g^{-1})\alpha_{ij}(g^{-1})\alpha_{kt}(g).$$

Now, $\mathrm{Tr}(\tilde{f}) = \mathrm{Tr}(cI) = c\dim V$. On the other hand, by the earlier lemma, $\mathrm{Tr}(\tilde{f}) = |G|\mathrm{Tr}(E)$. Thus,

$$\begin{aligned} c\dim V &= |G|\mathrm{Tr}(E), \\ c &= \frac{|G|\mathrm{Tr}(E)}{\dim V}. \end{aligned}$$

If $j \neq k$ then $\mathrm{Tr}(E) = 0$, so $c = 0$. Also, if $i \neq t$ then the $(i,t)^{\text{th}}$ entry of $\tilde{f}$ is 0, regardless of c. Hence,

$$\sum_{g\in G} \alpha_{ij}(g^{-1})\alpha_{kt}(g) = 0 \quad \text{unless } i = t \text{ and } j = k.$$

When $i = t$ and $j = k$, $\mathrm{Tr}(E) = 1$ so

$$\frac{|G|}{\dim V} = c = \sum_{g\in G} \alpha_{ij}(g^{-1})\alpha_{kt}(g),$$

and in particular, $\dim V \mid |G|$. □

Corollary 4.7.9. *Let V be a simple $K[G]$-module where K is algebraically closed and* $\mathrm{char}\, K = 0$. *Then*

$$\sum_{g\in G} \chi_V(g)\chi_V(g^{-1}) = |G|.$$

Proof. Let $\alpha(g)$ be the matrix for V. Set $s := \dim V$. Then

$$\begin{aligned} \sum_{g\in G} \chi_V(g)\chi_V(g^{-1}) &= \sum_{g\in G}\sum_{t=1}^{s}\sum_{i=1}^{s} \alpha_{tt}(g)\alpha_{ii}(g^{-1}) \\ &= \sum_{t=1}^{s}\sum_{i=1}^{s}\sum_{g\in G} \alpha_{tt}(g)\alpha_{ii}(g^{-1}) \\ &= \sum_{t=1}^{s}\sum_{i=1}^{s} \delta_{it}\frac{|G|}{s} \\ &= s\frac{|G|}{s} \\ &= |G|. \end{aligned}$$

□

If char $K = 0$, can define an inner product on $\mathrm{Ch}_K(G)$ via

$$\langle \chi_V, \chi_W \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \chi_W(g^{-1}).$$

If K is algebraically closed, have just shown that $\{\chi_V \mid V \text{ simple}\}$ forms an orthonormal set in $\mathrm{Ch}_K(G)$. Since $K[G]$ is semisimple, every rep. is a sum of simple ones, so this is in fact a basis.

In particular:

Corollary 4.7.10. *If* char $K = 0$ *then*

$$\mathrm{R}_K(G) \cong \mathrm{Ch}_K(G).$$

If K is algebraically closed, then

$$\mathrm{Ch}_K(G) = \mathrm{CF}_K(G).$$

Proof. We have just shown that $\{\chi_V \mid V \text{ simple}\}$ is an orthonormal set in $\mathrm{Ch}_K(G) \subset \mathrm{CF}_K(G)$ (the inner product extends in the obvious way to $\mathrm{CF}_K(G)$). Thus, this set is linearly independent, so $\theta : \mathrm{R}_K(G) \mapsto \mathrm{Ch}_K(G)$ is injective. By construction, $\mathrm{R}_K(G) \mapsto \mathrm{Ch}_K(G)$ is onto, so $\mathrm{R}_K(G) \cong \mathrm{Ch}_K(G)$.

Let $C_1, \ldots, C_r$ be the set of conj. classes of G. $\mathrm{CF}_K(G)$ has a basis $\{f_j : G \mapsto K\}$ where

$$f_j(g) = \begin{cases} 1 & g \in C_j, \\ 0 & g \notin C_j. \end{cases}$$

Hence, the dimension of $\mathrm{CF}_K(G)$ is the number of conj. classes of G, which, we have seen, is the number of simple $K[G]$-modules, ie. the dimension of $\mathrm{R}_K(G)$. □

4.8 Change of Group - Induction and Restriction

Let $H \leq G$, so $K[H] \subset K[G]$. Let N be a rep. of G, $G \times N \mapsto N$. Restricting to H produces an action $H \times N \mapsto N$. Denote the resulting rep. of H by N_H.

Conversely, let M be a rep. of G. Define the **induced** representation of G, denoted M_G, via

$$M^G := K[G] \otimes_{K[H]} M.$$

ie. M^G is generated as a K-module by

$$\{g \otimes m \mid g \in G, m \in M\}$$

where $gh \otimes m \sim g \otimes hm$. The G-action on M^G is defined by

$$g'(g \otimes m) = g'g \otimes m.$$

Let $g_1, \ldots, g_r$ be a set of representatives for the left cosets $\{gH\}$. Then $\{g_j \otimes m\}$ generates M^G. In fact, if K is a field and $m_1, \ldots, m_k$ is a basis for M then

$$\{g_j \otimes m_i \mid 1 \leq j \leq r, 1 \leq i \leq k\}$$

forms a basis for M^G. In particular,

$$\dim M^G = \frac{|G|}{|H|} \dim M,$$

whereas $\dim N_H = \dim N$.

This is a special case of a ground-ring change. A ring homo. $f : R \mapsto S$ induces

$$\begin{array}{rcl} \{S\text{-modules}\} & \overset{P}{\longmapsto} & \{R\text{-modules}\} \\ N & \longmapsto & N, \end{array}$$

where N (on the right) is regarded as an R-module via the action through f. f also induces

$$\begin{array}{rcl} \{R\text{-modules}\} & \overset{Q}{\longmapsto} & \{S\text{-modules}\} \\ M & \longmapsto & M \otimes_R M. \end{array}$$

Q and P are adjoint functors, ie.

$$\hom_S(QM, N) = \hom_R(M, PN) \quad \forall R\text{-mods. } M, S\text{-mods. } N.$$

To see this, given $\alpha : QM = S \otimes_R M \mapsto N$, define $\beta : M \mapsto PN = N$ by

$$\beta(m) = \alpha(1 \otimes m).$$

Then

$$\beta(rm) = \alpha(1 \otimes rm) = \alpha(r \otimes m) = r\alpha(1 \otimes m) = r\beta(m),$$

$\therefore \beta$ is an R-mod. homo.

Conversely, given $\beta : M \mapsto PN$, define $\alpha : QM \mapsto N$ by

$$\alpha(s \otimes m) = s\beta(m).$$

Then

$$\alpha(s'(s \otimes m)) = \alpha(ss' \otimes m) = ss'\beta(m) = s'\alpha(s \otimes m).$$

$\therefore \alpha$ is an S-mod. homo.

In our special case,

$$\hom_{K[G]}(M^G, N) = \hom_{K[H]}(M, N_H).$$

This is called Frobenius Reciprocity.

Also, if $A \leq B \leq C$ then

$$M^C \cong (M^B)^C$$

and

$$N_A \cong (N_B)_A.$$

Let $(\chi_N)_H := \chi_{N_H}$ and $(\chi_M)^G := \chi_{M^G}$ denote the characters of restricted and induced representations. $(\chi_N)_H$ is the composite function

$$H \hookrightarrow G \overset{\chi_N}{\longmapsto} K,$$

ie. $(\chi_N)_H = \chi_N|_H$. To describe $(\chi_M)^G$, let $g_1, \ldots, g_r$ be a set of left coset representatives for GH and let $m_1, \ldots, m_m$ be a basis for V, so that $\{g_i \otimes m_j\}$ is a basis for M^G.

For $g \in G$,

$$g \cdot (g_i \otimes m_j) = gg_i \otimes m_j = g_{i_g} \otimes hm_j,$$

where $gg_i = g_{i_g}h$, $h \in H, i_g = 1, \ldots, r$. Letting $\alpha_G(g)$ be the matrix representing the action of g on M^G and $\alpha_H(h)$ be the matrix for the action of h on M, the contribution to $\mathrm{Tr}\alpha_G(g)$ is:

$$\text{coeff. of } (g_i \otimes m_j) \text{ in } g(g_i \otimes m_j) = \begin{cases} 0 & i_g \neq i \\ (\alpha_H(h))_{jj} & i_g = g. \end{cases}$$

Note that if $i_g = i$ then $h = g_i^{-1} g g_i$. So

$$\begin{aligned}
\chi_M^G(g) &= \sum_{i,j} \begin{cases} 0 & g_i^{-1} g g_i \notin H \\ \alpha_H(g_i^{-1} g g_i)_{jj} & g_i^{-1} g g_i \in H \end{cases} \\
&= \sum_{i} \begin{cases} 0 & g_i^{-1} g g_i \notin H \\ \chi_M(g_i^{-1} g g_i) & g_i^{-1} g g_i \in H \end{cases} \\
&= \sum_{i} \chi_M(g_i^{-1} g g_i), \quad \text{using the convention } \chi_M(x) = 0 \text{ if } x \notin H \\
&= \frac{1}{|H|} \sum_{x \in G} \chi_M(x^{-1} g x).
\end{aligned}$$

4.9 Examples

4.9.1 $G = S_3$

We have $|G| = 6$.

Conj. class	# conjugates
$\lambda = (3), (1\ 2\ 3)$	2
$\lambda = (2,1), (1\ 2)$	3
$\lambda = (1,1,1), e$	1

We have 3 conjugacy classes, so 3 indecomposable reps. So our dimensions are determined:

$$6 = 1^2 + 1^2 + 2^2.$$

The reps. are:

1. V_1 = trivial rep., $\dim V_1 = 1, \chi_1 = (\overset{(3)}{1}, \overset{(2,1)}{1}, \overset{(3)}{1})$.

2. V_2 = sign rep., $\dim V_2 = 1, \chi_2 = (1, -1, 1)$.

3. V_3 = natural rep., $\dim V_3 = 2$. By orthogonality of characters, $\chi_2 = (2, 0, -1)$. This representation is given on the space
$$\langle x_1, x_2, x_3 \rangle / \langle x_1 + x_2 + x_3 \rangle$$
by
$$\sigma(\overline{x_i}) = \overline{x_{\sigma(i)}}.$$

Altogether, our character table is

$$\chi = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \\ 2 & 0 & -1 \end{pmatrix}.$$

4.9.2 $G = D_8 = \langle a, b \mid a^4 = b^2 = e, bab^{-1} = a^{-1} \rangle$

$|G| = 8$. We view $G \subset S_4$ via $a = (1\ 2\ 3\ 4), b = (1\ 2)$.

Conj. class	# conjugates
$a = (1\ 3\ 2\ 4)$	2
$a^2 = (1\ 2)(3\ 4)$	1
$b = (1\ 2)$	2
$ab = (1\ 3)(2\ 4)$	2
e	1

The dimensions of the irred. reps. are determined:

$$8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2.$$

The 1-dim. reps. are given by $\hom(D_8, S^1)$ where

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

We have

$$\hom(D_8, S^1) = \hom((D_8)_{ab}, S^1) = \hom(C_2 \times C_2, S^1) = \hom(C_2, S^1) \times \hom(C_2, S^1).$$

Dimension	Rep.	
1	V_1	trivial,
1	V_2	$a \cdot v = -v, b \cdot v = v$
1	V_3	$a \cdot v = v, b \cdot v = -v$
1	V_4	$a \cdot v = -v, b \cdot v = -v$
2	V_5	Find character by $\chi_{K[G]}(\sigma) = \begin{cases} \lvert G \rvert, & \sigma = e \\ 0, & \sigma \neq e. \end{cases}$

Our character table (columns indexed by e, a, a^2, b, ab) is:

$$\chi = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 \\ 2 & 0 & -2 & 0 & 0 \end{pmatrix}.$$

Set $IC_{\langle a \rangle} := (\mathrm{Triv} C_{\langle a \rangle})^{D_8}$, that is, the 2-dimensional representation of D_8 obtained by induction from the trivial representation of the cyclic subgroup generated by a. If v is a basis for the 1-dimensional vector space V for the trivial 1-dimensional vector representation of $C_{\langle a \rangle}$, then a basis for $V^{D_8} = K[D_8] \otimes_{K[\langle a \rangle} V$ is given $\langle 1 \otimes v, b \otimes v \rangle$, since 1 and b are a set of coset representatives. Since left multiplication by e, a, or a^2 preserve the cosets, in $IC_{\langle a \rangle}$ they are mapped to the identity matrix, while left multiplication by b or ab switches the cosets. Thus the traces are 2 and 0 respectively so $\chi_{IC_{\langle a \rangle}} = (2\ 2\ 2\ 0\ 0)$. Comparing this with the character table gives $IC_{\langle a \rangle} = V_1 + V_3$.

Let $\alpha^{3,1}$ denote the natural 3-dimensional representation of S_4 on $\langle x_1, x_2, x_3, x_4 \rangle / \langle x_1 + x_2 + x_3 + x_4 \rangle$. $\alpha^{3,1}|_{D_8}$ splits as $W \oplus \alpha^{3,1}|_{D_8}/W$, where $W = \langle w \rangle$ where $w = x_1 + x_2$.. Since $a \cdot w = x_3 + x_4 = -w$ and $b \cdot w = x_2 + x_1 = w$, $W \cong V_2$. and, it is easy to see (using characters or otherwise) that $W \oplus \alpha^{3,1}|_{D_8}/W \cong V_5$, so $\alpha^{3,1}|_{D_8} = V_2 + V_5$.

4.9.3 $G = \mathbb{H}_8$

$\mathbb{H}_8$ is the group of Quaternions. It consists of 8 elements,

$$\pm i, \pm j, \pm k, \pm 1$$

such that $(-1)^2 = 1$, $-1 \in Z(\mathbb{H}_8)$ and

$$i^2 = j^2 = k^2 = -1,$$
$$ij = k, \;\; jk = i, \;\; ki = j.$$

Conj. class	# conjugates
$i \sim -i$	2
$j \sim -j$	2
$k \sim -k$	2
-1	1
1	1

The dimensions of the irred. reps. are determined:

$$8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2.$$

$\mathbb{H}_8/\langle -1 \rangle \cong C_2 \times C_2$ is abelian, so $(\mathbb{H}_8)_{ab} = C_2 \times C_2$, and thus,

$$\hom(\mathbb{H}_8, S^1) = \hom(C_2, S^1) \times \hom(C_2, S^1).$$

Dimension	Rep.	
1	V_1	trivial
1	V_2	$i \cdot v = -v, j \cdot v = v$
1	V_3	$i \cdot v = v, j \cdot v = -v$
1	V_4	$i \cdot v = -v, j \cdot v = -v$
2	V_5	Find character by $\chi_{K[G]}(\sigma) = \begin{cases} \lvert G \rvert, & \sigma = e \\ 0, & \sigma \neq e. \end{cases}$

Our character table (columns indexed by $1, -1, i, j, k$) is:

$$\chi = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & -2 & 0 & 0 & 0 \end{pmatrix}.$$

The "natural" representation of $\mathbb{H}_8$ on $W = \langle x_1, x_i, x_j, x_k \rangle$ is given by $i \cdot x_1 = x_i$, $i \cdot x_i = -x_1$, $i \cdot x_j = x_k$, $i \cdot x_k = -x_j$, etc. By inspection $\chi_W = (4 \;\; -4 \; 0 \; 0 \; 0)$, which, from the character table is recognized as $2V_5$. The subspace $\langle x_1 + x_i, x_j + x_k \rangle \subset W$ is closed under the action of $\mathbb{H}_8$ and provides a natural description of V_5.

4.9.4 $G = C_7 \rtimes C_3 = \langle a, b \mid a^7 = e, b^3 = e, bab^{-1} = a^2 \rangle$

Conj. class	# conjugates
a	3
$a^3 \sim a^{-1}$	3
b	7
b^2	7
1	1

$G_{ab} = C_{\langle b \rangle} = C_3$, and thus,

$$\hom(G, S^1) = \hom(C_3, S^1).$$

yielding three 1-dimensional representatives.

The dimensions of the irred. reps. are determined:

$$21 = 1^2 + 1^2 + 1^2 + 3^2 + 3^2.$$

Let $\omega = e^{2\pi i/3}$.

Dimension	Rep.	
1	V_1	trivial
1	V_2	$a \cdot v = v, b \cdot v = \omega v$
1	V_3	$i \cdot v = v, b \cdot v = \omega^2 v$
3	V_4	
3	V_5	

Our character table (columns indexed by $1, a, a^3, b, b^2$) looks like:

$$\chi = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \omega & \omega^2 \\ 1 & 1 & 1 & \omega^2 & \omega \\ 3 & x & y & s & t \\ 3 & x' & y' & s' & t' \end{pmatrix}.$$

for some $x, y, s, t, x', y', s', t'$.

Using $\chi_{K[G]}(\sigma) = \begin{cases} |G|, & \sigma = e \\ 0, & \sigma \neq e, \end{cases}$ we find that $x' = -(x+1), y' = -(y+1), s' = -s, t' = -t$.

Orthogonality of χ_1 and χ_4 gives $7(s+t) = -3 - 3x - 3y$ while orthogonality of the pairs χ_2, χ_4 and χ_3, χ_4 give $7(\omega s + \omega^2 t) = -3 - 2x - 3y$ and $7(\omega^2 s + \omega t) = -3 - 2x - 3y$ respectively. Thus $7(s+t) = 7(\omega s + \omega^2 t) = 7(\omega^2 s + \omega t)$, from which we deduce that $s = t = 0$ and so $(x + y + 1) = -\frac{7}{3}(s+t) = 0$. The inner product of χ_4 with itself gives $|G| = 21 = 9 + 3xy + 3xy$, which combined with $x + y + 1 = 0$ gives $x^2 + x + 2 = 0$, which determines x. Notice that the solution of $x^2 + x + 2 = 0$ satisfies $x = \zeta + \zeta^2 + \zeta^4$, where $\zeta = e^{2\pi i/7}$ and $1 - x = \zeta^3 + \zeta^5 + \zeta^6$, Thus our character table is Our character table (columns indexed by $1, a, a^3, b, b^2$) looks like:

$$\chi = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \omega & \omega^2 \\ 1 & 1 & 1 & \omega^2 & \omega \\ 3 & x & y & 0 & 0 \\ 3 & y & x & 0 & 0 \end{pmatrix}.$$

where $x = \zeta + \zeta^2 + \zeta^4$ and $y = \zeta^3 + \zeta^5 + \zeta^6$.

The representation V_4 is given explicitly by $a \mapsto \begin{pmatrix} \zeta & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta^4 \end{pmatrix}$, $b \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ while V_5 is given by $a \mapsto \begin{pmatrix} \zeta^3 & 0 & 0 \\ 0 & \zeta^6 & 0 \\ 0 & 0 & \zeta^5 \end{pmatrix}$, $b \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

4.10 Symmetric Polynomials

For a free K-module V, let

$$T^K(V) := \bigoplus_{n=0}^{\infty} V^{\otimes n},$$

called the **tensor algebra** on V. Multiplication is defined on $T^K(V)$ by

$$(x_1 \otimes \cdots \otimes x_k)(x_{k+1} \otimes \cdots \otimes x_\ell) = x_1 \otimes \cdots \otimes x_k \otimes x_{k+1} \otimes \cdots \otimes x_\ell.$$

S_n acts on $V^{\otimes n}$ by permuting factors (called the **position action**), ie.

$$\sigma \cdot (x_1 \otimes \cdots \otimes x_n) = x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}.$$

Let

$$S(V) := T(V)/\sim$$

where $(x_1 \otimes \cdots \otimes x_n) \sim \sigma \cdot (x_1 \otimes \cdots \otimes x_n)$. This is called the **polynomial (symmetric) algebra** on V.

Example 4.10.1. *If $x_1, \ldots, x_m$ form a basis for V then*

$$S(V) \overset{\cong}{\longmapsto} K[x_1, \ldots, x_m]$$
$$x_{i_1} \otimes \cdots \otimes x_{i_n} \mapsto x_{i_1} \cdots x_{i_n}.$$

Likewise, the **exterior algebra** on V is

$$\Lambda(V) := T(V)/\sim$$

where

$$x_1 \otimes \cdots \otimes x_n \sim (-1)^\sigma x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}.$$

If $x_1, \ldots, x_m$ is a basis for V then S_m acts on V (on the right) by

$$x_j \cdot \sigma = x_{\sigma^{-1}(j)}.$$

$\therefore$ Get induced action of S_m on $T(V), S(V)$, and $\Lambda(V)$. This is called the **internal action**. Let

$$\Sigma(V) = \mathrm{Fix}^{S_m}(S(V)) = \{a \in S(V) \mid a = a \cdot \sigma \ \forall \sigma \in S_m\}.$$

When K is a field, the isomorphism $S(V) \cong K[x_1, \ldots, x_m]$ takes $\Sigma(V)$ to the ring of symmetric polynomials over K, as defined in Section 3.9. Recall the definition in that section of the elementary symmetric polynomials $s_1, \ldots, s_m$:

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

By identifying $S(V)$ with $K[x_1, \ldots, x_m]$, we have $s_j \in \Sigma(V)\ \forall j$.

Theorem 4.10.2. $\Sigma(V) \cong K[s_1, \ldots, s_m]$.

If rank$V = m$, write $\Sigma^K[m] = \Sigma^K(V)$.

$$\begin{aligned} K[x_1, \ldots, x_{m+1}] &\mapsto K[x_1, \ldots, x_m] \\ x_j &\mapsto x_j \quad j \le m \\ x_{m+1} &\mapsto 0 \end{aligned}$$

induces the map

$$\begin{aligned} \rho_{m+1} : \Sigma[m+1] &\mapsto \Sigma[m] \\ s_k(x_1, \ldots, x_{m+1}) &\mapsto s_k(x_1, \ldots, x_m). \end{aligned}$$

Set $\Sigma := \varprojlim_m \Sigma[m]$, the inverse limit of graded rings. That is,

$$\Sigma = \{(a_m \in \Sigma[m])_{m=1}^{\infty} \mid \rho_{m+1}(a_{m+1}) = a_m \ \forall m\}.$$

Σ is a graded ring; the elements of Σ_n are sequences $(f[m])_{m=1}^{\infty}$, where $f[m]$ is a degree n symmetric poly. in m variables, and

$$f[m](x_1, \ldots, x_m) = f[m+1](x_1, \ldots, x_m, 0).$$

$\therefore$ $f[m]$ determines $f[k]$ for all $k \le m$. However, since each $f[m]$ is of degree n, $f[n]$ determines $f[m]$ $\forall m$. ie. Given

$$f[n] = \rho\big(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)\big),$$

we then have, for any $m \ge n$,

$$f[m] = \rho\big(s_1(x_1, \ldots, x_m), \ldots, s_n(x_1, \ldots, x_m)\big).$$

Equivalently, $f[m]$ is obtained from $f[n]$ by "symmetrizing over the m variables".

So, we may identify the sequence $(f[m])$ with the single element $f[n]$. ie. Σ_n has a basis consisting of the symmetric polynomials of degree n in n variables. (Alternatively, Σ_n has a basis consisting of the symmetric polynomials of degree n in m variables, for any $m \ge n$.) So

$$\Sigma \cong K[s_1, s_2, \ldots, s_k, \ldots].$$

Definition 4.10.3. *A* ***partition*** *of n is a sequence $\lambda = (\lambda_1, \ldots, \lambda_r)$ of non-negative integers s.t.*

$$n = \lambda_1 + \cdots + \lambda_r.$$

$\lambda \vdash n$ means that λ is a partition of n.

Pick $n \geq 0$, let K be a field and let V be the free module with basis $x_1, \ldots, x_r$. For an unordered partition $\lambda = (\lambda_1, \ldots, \lambda_r)$ of n, set V^λ to be the $K[S_n]$-submodule of $V^{\otimes n}$ (position action) generated by

$$x_1^{\otimes \lambda_1} \otimes \cdots \otimes x_r^{\otimes \lambda_r}.$$

That is, V^λ is the subspace of $V^{\otimes n}$ with basis

$$\{x_{i_1} \otimes \cdots \otimes x_{i_n} \mid \{i_1, \ldots, i_n\} \text{ contains } \lambda_j \text{ copies of } j\}.$$

Given $A \subset V^{\otimes n}$ a subspace, the **characteristic polynomial** of A is

$$\mathrm{Ch}(A) := \sum_{\lambda \vdash n} d_\lambda x^\lambda$$

where $d_\lambda = \dim(A \cap V^\lambda)$ and $x^\lambda = x_1^{\lambda_1} \ldots x_r^{\lambda_r}$.

It is clear from the definition that

$$\mathrm{Ch}(A \oplus B) = \mathrm{Ch}(A) + \mathrm{Ch}(B)$$
$$\mathrm{Ch}(A \otimes B) = \mathrm{Ch}(A)\mathrm{Ch}(B).$$

If A is closed under the internal action of S_r on V then $\mathrm{Ch}(A)$ is symmetric.

Let P be a projective $K[S_n]$-module, so that $P = K[S_n]e$ for some idempotent $e \in K[S_n]$. For any right $K[S_n]$-module N,

$$N \cong Ne \oplus N(1-e)$$

as vector spaces. Applying this in particular to $V^{\otimes n}$ with the position action,

$$V^{\otimes n} = V^{\otimes n}e \oplus V^{\otimes n}(1-e).$$

Set $P(V) := V^{\otimes n}e$. Then

$$K\text{-vector spaces} \mapsto K\text{-vector spaces}$$
$$V \mapsto P(V)$$

is a functor.

Example 4.10.4. *Suppose $p \nmid n!$. Then letting P be the trivial 1-dimensional rep. of S_n, P is an indecomposable proj. module with idempotent*

$$e = \frac{1}{n!} \sum_{\sigma \in S_n} \sigma.$$

We have:

$$\begin{aligned} P(V) &= \operatorname{span}\left\{\frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(n)} \mid v_1,\dots,v_n\in V\right\}\subset V^{\otimes n}\\ &\cong S(V). \end{aligned}$$

Let $V = \langle x_1,\dots,x_m\rangle$, ie. V is the vector space with basis $x_1,\dots,x_m$. Then $\mathrm{Ch}(P(V))$ is a symmetric polynomial in $x_1,\dots,x_m$ of degree n. In fact, if we let

$$P[m] = \mathrm{Ch}(P(\langle x_1,\dots,x_m\rangle))$$

then

$$\begin{aligned} \langle x_1,\dots,x_{m+1}\rangle &\mapsto \langle x_1,\dots,x_m\rangle\\ x_j &\mapsto x_j \quad j\le m\\ x_{m+1} &\mapsto 0 \end{aligned}$$

induces by functoriality a map

$$P(\langle x_1,\dots,x_{m+1}\rangle)) \mapsto P(\langle x_1,\dots,x_m\rangle))$$

so by applying $\mathrm{Ch}(\cdot)$, we get

$$\begin{aligned} P[m+1] &\mapsto P[m]\\ x_j &\mapsto x_j \quad j\le m\\ x_{m+1} &\mapsto 0. \end{aligned}$$

ie. $(P[m])$ forms an elt. of $\Sigma^{\mathbb{Z}}$ (symmetric polys. with coeffs. in $\mathbb{Z}$). We write $\mathrm{Ch}(P)$ for this elt. of $\Sigma^{\mathbb{Z}}$. It is determined by the degree n symmetric polynomial $\mathrm{Ch}(P(V))$ in n vars. obtained from

$$V = \langle x_1,\dots,x_n\rangle.$$

For an arbitrary $K[S_n]$-module P, we can write

$$P = \sum n_j P_j$$

where each P_j is an indecomposable proj. module and $n_j\ge 0$. Set $\mathrm{Ch}(P) := \sum n_j \mathrm{Ch}(P_j)$.

More generally, elements of $K_0(K[S_n])$ are sums

$$\sum n_j P_j$$

with $n_j \in \mathbb{Z}$. So by extending the definition to this case via

$$\mathrm{Ch}(\sum n_j P_j) = \sum n_j \mathrm{Ch}(P_j)$$

yields a homomorphism

$$\mathrm{Ch} : K_0(K[S_n]) \mapsto \Sigma^{\mathbb{Z}}[n].$$

We shall show, for char $K = 0$, that $\mathrm{Ch}(P)$ determines P.

For $n \geq 0$, set

$$\begin{aligned} R_n &:= \text{Underlying group of the representation ring } R(S_n) \\ &= K_0(K[S_n]) \\ &= \mathrm{span}_{\mathbb{Z}}\{\text{simple } K[S_n]\text{-modules}\} \\ &\cong \mathrm{span}_{\mathbb{Z}}\{\text{simple characters of } S_n\} \end{aligned}$$

and set $R = \bigoplus_n R_n$. The map $\mathrm{Ch} : R_n \mapsto \Sigma_n^{\mathbb{Z}}$ for each n yields $\mathrm{Ch} : R_n \mapsto \Sigma^{\mathbb{Z}}$.

Define a ring structure on R as follows: Let M be a $K[S_m]$-module, in R_m, and N a $K[S_n]$-module, in R_n. Set

$$M \cdot N = (M \otimes N)^{S_{m+n}} \in R_{m+n}.$$

ie. $M \otimes N$ is a $(S_m \times S_n)$-module in an obvious way, and $S_m \times S_n \subset S_{m+n}$; $M \cdot N$ is the induced S_{m+n}-module.

Theorem 4.10.5. $\mathrm{Ch} : R \mapsto \Sigma$ *is a ring isomorphism.*

Proof. We know that $\mathrm{Ch}(M \oplus n) = \mathrm{Ch}(M) + \mathrm{Ch}(N)$. We must show that $\mathrm{Ch}(M \cdot N) = \mathrm{Ch}(M)\mathrm{Ch}(N)$. It suffices to consider the case where M is a simple $K[S_m]$-module and N is a simple $K[S_n]$-module. Write $M = K[S_m] \cdot e$, $N = K[S_n] \cdot f$. Then $e \otimes f \in K[S_m] \otimes K[S_n] = K[S_m \times S_n]$, and

$$M \otimes N = K[S_m \times S_n] \cdot (e \otimes f).$$

Now $K[S_m \times S_n] \subset K[S_{m+n}]$ and so

$$M \cdot N = K[S_{m+n}] \cdot (e \otimes f).$$

For any V,

$$\begin{aligned} \mathrm{Ch}(M \cdot N(V)) &= \mathrm{Ch}(V^{\otimes(m+n)} \cdot (e \otimes f)) \\ &= \mathrm{Ch}(V^{\otimes m} \cdot e \otimes V^{\otimes n} \cdot f) \\ &= \mathrm{Ch}(V^{\otimes m} \cdot e)\mathrm{Ch}(V^{\otimes n} \cdot f) \\ &= \mathrm{Ch}(M(V))\mathrm{Ch}(N(V)) \end{aligned}$$

$\therefore$ Ch(MN) = Ch(M)Ch(N). Thus, Ch is a ring homomorphism.

Since $\Sigma = \mathbb{Z}[s_1, s_2, \ldots]$, to show Ch is onto, is suffices to show that $s_n \in \mathrm{Im(Ch)}\ \forall n$. Let P be the one-dimensional sign rep. of S_n. ie. $P = \langle w \rangle$ with $\sigma \cdot w = (-1)^{\mathrm{sgn}\sigma} w$. Then $P = K[S_n] \cdot e$ with

$$e = \frac{1}{n!} \sum_{\sigma \in S_n} (-1)^{\mathrm{sgn}\sigma} \sigma,$$

an idempotent. For any vector space V,

$$P(V) = (V^{\otimes n}) \cdot e = \Lambda(V).$$

$\therefore$ Ch$(P(V))$ = Ch$(\Lambda(V)) = s_n$. Thus, Ch is onto.

Claim. For each n, R_n and Σ_n are free abelian groups whose rank equals the number of partitions of n (into positive integers).

Proof of claim. The rank of R_n is equal to the number of non-isomorphic simple $K[S_n]$-reps, which is equal to the number of conjugacy classes in S_n. Each conjugacy class is determined by its cycle type, which is a partition of n (by Corollary 1.6.3). Moreover, it is obvious that every partition of n is the cycle type of some element in S_n. Thus, the rank of R_n is equal to the number of partitions of n.

For Σ_n, this follows from the fact that $\Sigma = \mathbb{Z}[s_1, s_2, \ldots]$ and the degree of s_k is k. ie. A basis for Σ_n consists of monomials in $\{s_k\}$ of total degree n, and since $\deg s_k = k$, each such monomial corresponds to a partition of n via

$$(\lambda_1, \ldots, \lambda_r) \leftrightarrow s_{\lambda_1} \ldots s_{\lambda_r}.$$

□

Since Ch is one-to-one, this claim shows that Ch is also onto, whence an isomorphism. □

4.10.1 Other Bases for Σ_n

There are 6 bases for $\Sigma_n^{\mathbb{Q}}$ in "common" use, of which 5 form bases in $\Sigma_n^{\mathbb{Z}}$. All bases are indexed by partitions λ of n.

1. Elementary Symmetric Functions

$$s_\lambda = s_{\lambda_1} s_{\lambda_2} \cdots s_{\lambda_r}.$$

eg.

$$s_{(2)} = x_1 x_2, \qquad s_{(1,2)} = (x_1 + x_2)^2.$$

2. Monomial Basis

$$m_\lambda = \text{symmetrization of } x_1^{\lambda_1} x_2^{\lambda_2} \dots x_r^{\lambda_r}.$$

eg.

$$m_{(2)} = x_1^2 + x_2^2, \qquad m_{(1,1)} = x_1 x_2.$$

3. Homogeneous Functions
Let

$$h_k = \sum_k \text{monomials of degree } k.$$

Then

$$h_\lambda = h_{\lambda_1} h_{\lambda_2} \cdots h_{\lambda_r}.$$

eg.

$$h_{(2)} = x_1^2 + x_1 x_2 + x_2^2, \qquad h_{(1,1)} = (x_1 + x_2)^2.$$

4. Power Functions
Let

$$\psi_k = x_1^k + x_2^k + \cdots + x_n^k.$$

Then

$$\psi_\lambda = \psi_{\lambda_1} \psi_{\lambda_2} \cdots \psi_{\lambda_r}.$$

eg.

$$\psi_{(2)} = x_1^2 + x_2^2 \qquad \psi_{(1,1)} = (x_1 + x_2)^2.$$

5. Schur Functions
For $\mu = (\mu_1, \dots, \mu_n)$, with $\mu_j \geq 0 \ \forall j$, let

$$\begin{aligned} V_\mu &:= \sum_{\sigma \in S_n} (-1)^{\mathrm{sgn}\sigma} x_{\sigma(1)}^{\mu_1} \cdots x_{\sigma(n)}^{\mu_n} \\ &= \det \begin{pmatrix} x_1^{\mu_1} & x_1^{\mu_2} & \cdots & x_1^{\mu_n} \\ x_2^{\mu_1} & x_2^{\mu_2} & \cdots & x_2^{\mu_n} \\ \vdots & \vdots & & \vdots \\ x_n^{\mu_1} & x_n^{\mu_2} & \dots & x_n^{\mu_n} \end{pmatrix}. \end{aligned}$$

In particular,

$$V_{(n-1,n-2,\dots,1,0)} = \prod_{i<j} (x_i - x_j),$$

called the Vandermonde determinant. For the partition $\lambda = (\lambda_1, \ldots, \lambda_n)$ of n (with $\lambda_j = 0$ allowed),

$$F_\lambda := \frac{V_{\lambda+(n-1,\ldots,1,0)}}{V_{(n-1,\ldots,1,0)}}.$$

eg.

$$\begin{aligned} F_{(2)} = F_{(2,0)} &= \frac{\begin{vmatrix} x_1^3 & 1 \\ x_2^3 & 1 \end{vmatrix}}{\begin{vmatrix} x_1 & 1 \\ x_2 & 1 \end{vmatrix}} \\ &= \frac{x_1^3 - x_2^3}{x_1 - x_2} \\ &= x_1^2 + x_1 x_2 + x_2^2, \\ F_{(1,1)} &= \frac{\begin{vmatrix} x_1^2 & x_1 \\ x_2^2 & x_2 \end{vmatrix}}{\begin{vmatrix} x_1 & 1 \\ x_2 & 1 \end{vmatrix}} \\ &= \frac{x_1^2 x_2 - x_1 x_2^2}{x_1 - x_2} \\ &= x_1 x_2. \end{aligned}$$

Note:

(a) $x_i = x_j \Rightarrow V_\mu = 0$. Thus, $V_{\lambda+(n-1,\ldots,1,0)}$ is divisible by $V_{(n-1,\ldots,1,0)}$, and so F_λ is a polynomial.

(b) Interchanging x_i, x_j multiplies both numerator and denominator by -1, so F_λ is symmetric.

6. Forgotten Basis
Let $m_\lambda = p(s_1, \ldots, s_k)$ be the expansion for m_λ in the elem. symmetric polys. Then

$$f_\lambda = p(h_1, \ldots, h_k).$$

eg. For $\lambda = (2)$,

$$\begin{aligned} m_(2) &= x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = s_1^2 - 2s_2, \\ \therefore\ f_{(2)} &= h_1^2 - 2h_2 = (x_1 + x_2)^2 - 2(x_1^2 + x_1x_2 + x_2^2) = -x_1^2 - x_2^2. \end{aligned}$$

For $\lambda = (1, 1)$,

$$m_{(1,1)} = x_1x_2 = s_2$$
$$\therefore\ f_{(1,1)} = h_2 = x_1^2 + x_1x_2 + x_2^2.$$

We know that 1 forms a basis for $\Sigma_n^{\mathbb{Q}}$ and it is trivial to see that 2 does. We have to prove that the others do.
Note: $\{\psi_\lambda\}$ does not form a basis for $\Sigma_n^{\mathbb{Z}}$. eg. $s_2 = \frac{1}{2}(\psi_{(1,1)} - \psi_{(2)})$ in $\sigma_n^{\mathbb{Q}}$, so

$$s_2 \notin \mathbb{Z}[\psi_1, \psi_2, \psi_3, \dots].$$

Generating Functions for s_n, h_n, ψ_n

The first three of our bases are defined as monomials in some other symmetric functions. Set

$$S(t) := \sum_{n=0}^{\infty} s_n t^n$$
$$H(t) := \sum_{n=0}^{\infty} h_n t^n$$
$$\Psi(t) := \sum_{n=0}^{\infty} \psi_n t^n.$$

By expanding and examining the coefficient of t^n, we see that

$$
\begin{aligned}
S(t) &= \prod_{j=1}^{\infty}(1 + x_j t), \\
H(t) &= \prod_{j=1}^{\infty}(1 + x_j t + x_j^2 t^2 + x_j^3 t^3 + \cdots) = \prod_{j=1}^{\infty} \frac{1}{1 - x_j t}, \\
\Psi(t) &= \sum_{n=1}^{\infty} \sum_{j=1}^{\infty} x_j^n t^{n-1} \\
&= \sum_{j=1}^{\infty} \sum_{n=1}^{\infty} x_j^n t^{n-1} \\
&= \sum_{j=1}^{\infty} \frac{x_j}{1 - x_j t} \\
&= \sum_{j=1}^{\infty} -\frac{d}{dt} \log(1 - x_j t) \\
&= \frac{d}{dt} \log\left(\prod_{j=1}^{\infty} \frac{1}{1 - x_j t}\right) \\
&= \frac{d}{dt} \log(H(t)) \\
&= \frac{H'(t)}{H(t)}.
\end{aligned}
$$

Thus,

$$S(t)H(-t) = 1 \tag{1}$$

$$\Psi(t) = \frac{H'(t)}{H(t)} \tag{2}$$

$$\Psi(-t) = \frac{H'(-t)}{H(-t)} = \frac{S'(t)}{S(t)} \tag{3}$$

(1) implies that

$$s_0 h_0 = 1$$

$$\sum_{j=0}^{n} (-1)^j s_j h_{n-j} = 0 \quad n > 0 \tag{1'}$$

Define $\omega : \Lambda^{\mathbb{Z}} = \mathbb{Z}[s_1, s_2, \dots] \mapsto \Lambda^{\mathbb{Z}}$ by $\omega(s_j) = h_j$. Since (1') is symmetrical in h, s, we get that ω is an isomorphism. In particular, $\Lambda = \mathbb{Z}[h_1, h_2, \dots]$, and so the homogeneous functions form a basis.

Applying ω to (1') gives

$$\begin{aligned} 0 &= \sum_{j=0}^{n} (-1)^j h_j \omega(h_{n-j}) \\ &= \sum_{j=0}^{n} (-1)^{n-j} h_{n-j} \omega(h_j) \\ &= (-1)^n \sum_{j=0}^{n} (-1)^j \omega(h_j) h_{n-j} \quad \forall n > 0. \end{aligned}$$

Comparing with (1'), we see that $\omega(h_n) = s_n$, ie. $\omega^2 = 1$ (ω is an involution).

By (2),

$$\sum_{n=1}^{\infty} n h_n t^{n-1} = \sum_{n=1}^{\infty} \sum_{j=1}^{\infty} \psi_j h_{n-j} t^{n-1}$$

$$\sum_{j=1}^{n} \psi_j h_{n-j} = n h_n \quad \forall n. \tag{2'}$$

Similarly,

$$\sum_{j=1}^{n} (-1)^{j-1} \psi_j s_{n-j} = n s_j \quad \forall n. \tag{3'}$$

Using (3'), each s_n can inductively be written as a polynomial in $\mathbb{Q}[\psi_1, \dots, \psi_n]$, so the power functions form a basis for $\Lambda^{\mathbb{Q}}$.

Since ω interchanges h, s, comparing (2') and (3') gives

$$\omega(\psi_n) = (-1)^{n-1} \psi_n.$$

To see that the Schur Functions form a basis for $\Lambda_n^{\mathbb{Z}}$, set $V_n := V_{(n-1,\dots,0)}$. Let A_k be the set of skew symmetric polynomials of degree k in n variables. Then we have an isomorphism

$$\begin{aligned} \Lambda_n &\mapsto A_{n+\binom{n}{2}} \\ f &\mapsto f V_n \end{aligned}$$

Since $\{F_\lambda V_n\}$ is the "monomial" basis for $A_{n+\binom{2}{2}}$ (ie. the basis obtained by skew symmetrizing each monomial), $\{F_\lambda\}$ forms a basis for Λ_n.