Appendix A
Commutative Rings and Ideals

By a *ring* we will always mean a commutative ring with a multiplicative identity 1. An *ideal* in a ring R is an additive subgroup $I \subset R$ such that

$$ra \in I \quad \forall r \in R, a \in I.$$

Considering R and I as additive groups we form the factor group R/I which is actually a ring: There is an obvious way to define multiplication, and the resulting structure is a ring. (Verify this. Particularly note how the fact that I is an ideal makes the multiplication well-defined. What would go wrong if I were just an additive subgroup, not an ideal?) The elements of R/I can be regarded as equivalence classes for the congruence relation on R defined by

$$a \equiv b \pmod{I} \text{ iff } a - b \in I.$$

What are the ideals in the ring $\mathbb{Z}$? What are the factor rings?

Definition. An ideal of the form $(a) = aR = \{ar : r \in R\}$ is called a *principal ideal*. An ideal $\neq R$ which is not contained in any other ideal $\neq R$ is called a *maximal ideal*. An ideal $\neq R$ with the property

$$rs \in I \Rightarrow r \text{ or } s \in I \; \forall r, s \in R$$

is called a *prime ideal*.

What are the maximal ideals in $\mathbb{Z}$? What are the prime ideals? Find a prime ideal which is not maximal.

Define addition of ideals in the obvious way:

$$I + J = \{a + b : a \in I, b \in J\}.$$

(Show that this is an ideal.)

D. A. Marcus, *Number Fields*, Universitext,
https://doi.org/10.1007/978-3-319-90233-3

It is easy to show that every maximal ideal is a prime ideal: If $r, s \notin I$, I maximal, then the ideals $I + rR$ and $I + sR$ are both strictly larger than I, hence both must be R. In particular both contain 1. Write $1 = a + rb$ and $1 = c + sd$ with $a, c \in I$ and $b, d \in R$ and multiply the two equations together. If $rs \in I$, we obtain the contradiction $1 \in I$. (Note that for an ideal I, $I \neq R$ iff $1 \notin I$.)

Each ideal $I \neq R$ is contained in some maximal ideal. The proof requires Zorn's lemma, one version of which says that if a family of sets is closed under taking nested unions, then each member of that family is contained in some maximal member. Applying this to the family of ideals $\neq R$, we find that all we have to show is that a nested union of ideals $\neq R$ is another ideal $\neq R$. It is easy to see that it is an ideal, and it must be $\neq R$ because none of the ideals contain 1.

An ideal I is maximal iff R/I has no ideals other than the whole ring and the zero ideal. The latter condition implies that R/I is a field since each nonzero element generates a nonzero principal ideal which necessarily must be the whole ring. Since it contains 1, the element has an inverse. Conversely, if R/I is a field then it has no nontrivial ideals. Thus we have proved that I is maximal iff R/I is a field.

An *integral domain* is a ring with no zero divisors: If $rs = 0$ then r or $s = 0$. We leave it to the reader to show that I is a prime ideal iff R/I is an integral domain. (Note that this gives another way of seeing that maximal ideals are prime.)

Two ideals I and J are called *relatively prime* iff $I + J = R$. If I is relatively prime te each of $J_1, \ldots, J_n$ then I is relatively prime to the intersection J of the J_i: For each i we can write $a_i + b_i = 1$ with $a_i \in I$ and $b_i \in J_i$. Multiplying all of these equations together gives $a + (b_1 b_2 \cdots b_n) = 1$ for some $a \in I$; the result follows since the product is in J.

Note that two members of $\mathbb{Z}$ are relatively prime in the usual sense iff they generate relatively prime ideals.

Chinese Remainder Theorem. Let $I_1, \ldots, I_n$ be pairwise relatively prime ideals in a ring R. Then the obvious mapping

$$R/\bigcap_{i=1}^{n} I_i \to R/I_1 \times \cdots \times R/I_n$$

is an isomorphism.

Proof. We will prove this for the case $n = 2$. The general case will then follow by induction since I_1 is relatively prime to $I_2 \cap \cdots \cap I_n$. (Fill in the details.)

Thus assume $n = 2$. The kernel of the mapping is obviously trivial. To show that the mapping is onto, fix any r_1 and $r_2 \in R$: we must show that there exists $r \in R$ such that

$$\begin{aligned} r &\equiv r_1 \pmod{I_1} \\ r &\equiv r_2 \pmod{I_2}. \end{aligned}$$

This is easy: Write $a_1 + a_2 = 1$ with $a_1 \in I_1$ and $a_2 \in I_2$, then set $r = a_1 r_2 + a_2 r_1$. It works. □

The product of two ideals I and J consists of all finite sums of products $ab, a \in I$, $b \in J$. This is the smallest ideal containing all products ab. We leave it to the reader to prove that the product of two relatively prime ideals is just their intersection. By induction this is true for any finite number of pairwise relatively prime ideals. Thus the Chinese Remainder Theorem could have been stated with the product of the I_i rather than the intersection.

An integral domain in which every ideal is principal is called a *principal ideal domain* (PID). Thus $\mathbb{Z}$ is a PID. So is the polynomial ring $F[x]$ over any field F. (Prove this by considering a polynomial of minimal degree in a given ideal.)

In a PID, every nonzero prime ideal is maximal. Let $I \subset J \subset R$, I prime, and write $I = (a)$, $J = (b)$. Then $a = bc$ for some $c \in R$, and hence by primeness I must contain either b or c. If $b \in I$ then $J = I$. If $c \in I$ then $c = ad$ for some $d \in R$ and then by cancellation (valid in any integral domain) $bd = 1$. Then b is a unit and $J = R$. This shows that I is maximal.

If α is algebraic (a root of some nonzero polynomial) over F, then the polynomials over F having α as a root form a nonzero ideal I in $F[x]$. It is easy to see that I is a prime ideal, hence I is in fact maximal (because $F[x]$ is a PID). Also, I is principal; a generator f is a polynomial of smallest degree having α as a root. Necessarily f is an irreducible polynomial.

Now map

$$F[x] \to F[\alpha]$$

in the obvious way, where $F[\alpha]$ is the ring consisting of all polynomial expressions in α. The mapping sends a polynomial to its value at α. The kernel of this mapping is the ideal I discussed above, hence $F[\alpha]$ is isomorphic to the factor ring $F[x]/I$. Since I is maximal we conclude that $F[\alpha]$ is a field whenever α is algebraic over F. Thus we employ the notation $F[\alpha]$ for the field generated by an algebraic element α over F, rather than the more common $F(\alpha)$. Note that $F[\alpha]$ consists of all linear combinations of the powers

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

with coefficients in F, where n is the degree of f. These powers are linearly independent over F (why?), hence $F[\alpha]$ is a vector space of dimension n over F.

A *unique factorization domain* (UFD) is an integral domain in which each nonzero element factors into a product of irreducible elements (which we define to be those elements p such that if $p = ab$ then either a or b is a unit) and the factorization is unique up to unit multiples and the order of the factors.

It can be shown that if R is a UFD then so is the polynomial ring $R[x]$. Then by induction so is the polynomial ring in any finite number of commuting variables. We will not need this result.

We claim that every PID is a UFD. To show that each nonzero element can be factored into irreducible elements it is sufficient to show that there cannot be an infinite sequence

$$a_1, a_2, a_3, \ldots$$

such that each a_i is divisible by a_{i+1} but does not differ from it by a unit factor. (Keep factoring a given element until all factors are irreducible; if this does not happen after finitely many steps then such a sequence would result.) Thus assume such a sequence exists. Then the a_i generate infinitely many distinct principal ideals (a_i), which are nested upward:

$$(a_1) \subset (a_2) \subset \ldots.$$

The union of these ideals is again a principal ideal, say (a). But the element a must be in some (a_n), implying that in fact all $(a_i) = (a_n)$ for $i \geq n$. This is a contradiction.

It remains for us to prove uniqueness. Each irreducible element p generates a maximal ideal (p): If $(p) \subset (a) \subset R$ then $p = ab$ for some $b \in R$, hence either a or b is a unit, hence either $(a) = (p)$ or $(a) = R$. Thus $R/(p)$ is a field.

Now suppose a member of R has two factorizations into irreducible elements

$$p_1 \cdots p_r = q_1 \cdots q_s.$$

Considering the principal ideals (p_i) and (q_i), select one which is minimal (does not properly contain any other). This is clearly possible since we are considering only finitely many ideals. Without loss of generality, assume (p_1) is minimal among the (p_i) and (q_i).

We claim that (p_1) must be equal to some (q_i): If not, then (p_1) would not contain any q_i, hence all q_i would be in nonzero congruence classes mod (p_i). But then reducing mod (p_i) would yield a contradiction.

Thus without loss of generality we can assume $(p_1) = (q_1)$. Then $p_1 = uq_1$ for some unit u. Cancelling q_1, we get

$$up_2 \cdots p_r = q_2 \cdots q_s.$$

Notice that up_2 is irreducible. Continuing in this way (or by just applying induction) we conclude that the two factorizations are essentially the same. □

Thus in particular if F is a field then $F[x]$ is a UFD since it is a PID. This result has the following important application.

Eisenstein's Criterion. Let M be a maximal ideal in a ring R and let

$$f(x) = a_n x^n + \cdots + a_0 \quad (n \geq 1)$$

be a polynomial over R such that $a_n \notin M$, $a_i \in M$ for all $i < n$, and $a_0 \notin M^2$. Then f is irreducible over R.

Proof. Suppose $f = gh$ where g and h are non-constant polynomials over R. Reducing all coefficients mod M and denoting the corresponding polynomials over R/M by $\overline{f}$, $\overline{g}$ and $\overline{h}$, we have $\overline{f} = \overline{g}\overline{h}$. R/M is a field, so $(R/M)[x]$ is a UFD. $\overline{f}$ is just

ax^n where a is a nonzero member of R/M, so by unique factorization in $(R/M)[x]$ we conclude that $\overline{g}$ and $\overline{h}$ are also monomials:

$$\overline{g} = bx^m, \quad \overline{h} = cx^{n-m}$$

where b and c are nonzero members of R/M and $1 \leq m < n$. (Note that nonzero members of R/M are units in the UFD $(R/M)[x]$, while x is an irreducible element.) This implies that g and h both have constant terms in M. But that is a contradiction since $a_0 \notin M^2$. □

In particular we can apply this result with $R = \mathbb{Z}$ and $M = (p)$, p a prime in $\mathbb{Z}$, to prove that certain polynomials are irreducible over $\mathbb{Z}$. Together with exercise 8(c), chapter 3, this provides a sufficient condition for irreducibility over $\mathbb{Q}$.

Appendix B
Galois Theory for Subfields of $\mathbb{C}$

Throughout this section K and L are assumed to be subfields of $\mathbb{C}$ with $K \subset L$. Moreover we assume that the degree $[L : K]$ of L over K is finite. (This is the dimension of L as vector space over K.) All results can be generalized to arbitrary finite separable field extensions; the interested reader is invited to do this.

A polynomial f over K is called *irreducible* (over K) iff whenever $f = gh$ for some $g, h \in K[x]$, either g or h is constant. Every $\alpha \in L$ is a root of some irreducible polynomial f over K; moreover f can be taken to be monic (leading coefficient $= 1$). Then f is uniquely determined. The ring $K[\alpha]$ consisting of all polynomial expressions in α over K is a field and its degree over K is equal to the degree of f. (See Appendix A.) The roots of f are called the *conjugates* of α over K. The number of these roots is the same as the degree of f, as we show below.

A monic irreducible polynomial f of degree n over K splits into n monic linear factors over $\mathbb{C}$. We claim that these factors are distinct: Any repeated factor would also be a factor of the derivative f' (prove this). But this is impossible because f and f' generate all of $K[x]$ as an ideal (why? See Appendix A) hence 1 is a linear combination of f and f' with coefficients in $K[x]$. (Why is that a contradiction?) It follows from this that f has n distinct roots in $\mathbb{C}$.

We are interested in embeddings of L in $\mathbb{C}$ which fix K pointwise. Clearly such an embedding sends each $\alpha \in L$ to one of its conjugates over K.

Theorem 50. *Every embedding of K in $\mathbb{C}$ extends to exactly $[L : K]$ embeddings of L in $\mathbb{C}$.*

Proof. (*Induction on* $[L : K]$) This is trivial if $L = K$, so assume otherwise. Let σ be an embedding of K in $\mathbb{C}$. Take any $\alpha \in L - K$ and let f be the monic irreducible polynomial for α over K. Let g be the polynomial obtained fom f by applying σ to all coefficients. Then g is irreducible over the field σK. For every root β of g, there is an isomorphism

$$K[\alpha] \to \sigma K[\beta]$$

which restricts to σ on K and which sends α to β. (Supply the details. Note that $K[\alpha]$ is isomorphic to the factor ring $K[x]/(f)$.) Hence σ can be extended to an

D. A. Marcus, *Number Fields*, Universitext,
https://doi.org/10.1007/978-3-319-90233-3

embedding of $K[\alpha]$ in $\mathbb{C}$ sending α to β. There are n choices for β, where n is the degree of f; so σ has n extensions to $K[\alpha]$. (Clearly there are no more than this since an embedding of $K[\alpha]$ is completely determined by its values on K and at α.) By inductive hypothesis each of these n embeddings of $K[\alpha]$ extends to $[L : K[\alpha]]$ embeddings of L in $\mathbb{C}$. This gives

$$[L : K[\alpha]]n = [L : K[\alpha]][K[\alpha] : K] = [L : K]$$

distinct embeddings of L in $\mathbb{C}$ extending σ. Moreover every extension of σ to L must be one of these. (Why?) □

Corollary. *There are exactly* $[L : K]$ *embeddings of* L *in* $\mathbb{C}$ *which fix* K *pointwise.* □

Theorem 51. $L = K[\alpha]$ *for some* α.

Proof. (*Induction on* $[L : K]$) This is trivial if $L = K$ so assume otherwise. Fix any $\alpha \in L - K$. Then by inductive hypothesis $L = K[\alpha, \beta]$ for some β. We will show that in fact $L = K[\alpha + a\beta]$ for all but finitely many elements $a \in K$.

Suppose $a \in K$, $K[\alpha + a\beta] \neq L$. Then $\alpha + a\beta$ has fewer than $n = [L : K]$ conjugates over K. We know that L has n embeddings in $\mathbb{C}$ fixing K pointwise, so two of these must send $\alpha + a\beta$ to the same conjugate. Call them σ and τ; then

$$a = \frac{\sigma(\alpha) - \tau(\alpha)}{\tau(\beta) - \sigma(\beta)}.$$

(Verify this. Show that the denominator is nonzero.) Finally, this restricts a to a finite set because there are only finitely many possibilities for $\sigma(\alpha)$, $\tau(\alpha)$, $\sigma(\beta)$ and $\tau(\beta)$. □

Definition. L is *normal over* K iff L is closed under taking conjugates over K.

Theorem 52. L *is normal over* K *iff every embedding of* L *in* $\mathbb{C}$ *fixing* K *pointwise is actually an automorphism; equivalently,* L *has exactly* $[L : K]$ *automorphisms fixing* K *pointwise.*

Proof. If L is normal over K then every such embedding sends L into itself since it sends each element to one of its conjugates. L must in fact be mapped *onto* itself because the image has the same degree over K. (Convince yourself.) So every such embedding is an automorphism.

Conversely, if every such embedding is an automorphism, fix $\alpha \in L$ and let β be a conjugate of α over K. As in the proof of Theorem 50 there is an embedding σ of L in $\mathbb{C}$ fixing K pointwise and sending α to β; then $\beta \in L$ since σ is an automorphism. Thus L is normal over K.

The equivalence of the condition on the number of automorphisms follows immediately from the corollary to Theorem 50. □

Theorem 53. *If $L = K[\alpha_1, \ldots, \alpha_n]$ and L contains the conjugates of all of the α_i, then L is normal over K.*

Proof. Let σ be an embedding of L in $\mathbb{C}$ fixing K pointwise. L consists of all polynomial expressions

$$\alpha = f(\alpha_1, \ldots, \alpha_n)$$

in the α_i with coefficients in K, and it is clear that σ sends α to

$$f(\sigma\alpha_1, \ldots, \sigma\alpha_n).$$

The $\sigma\alpha_i$ are conjugates of the α_i, so $\sigma\alpha \in L$. This shows that σ sends L into itself, hence onto itself as in the proof of Theorem 52. Thus σ is an automorphism of L and we are finished. □

Corollary. *If L is any finite extension of K (finite degree over K) then there is a finite extension M of L which is normal over K. Any such M is also normal over L.*

Proof. By Theorem 51, $L = K[\alpha]$; let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α and set

$$M = K[\alpha_1, \ldots, \alpha_n].$$

Then M is normal over K by Theorem 53.

The second part is trivial since every embedding of M in $\mathbb{C}$ fixing L pointwise also fixes K pointwise and hence is an automorphism of M. □

Galois Groups and Fixed Fields

We define the *Galois group* $\mathrm{Gal}(L/K)$ of L over K to be the group of automorphisms of L which fix K pointwise. The group operation is composition. Thus L is normal over K iff $\mathrm{Gal}(L/K)$ has order $[L : K]$. If H is any subgroup of $\mathrm{Gal}(L/K)$, define the *fixed field* of H to be

$$\{\alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in H\}.$$

(Verify that this is actually a field.)

Theorem 54. *Suppose L is normal over K and let $G = \mathrm{Gal}(L/K)$. Then K is the fixed field of G, and K is not the fixed field of any proper subgroup of G.*

Proof. Set $n = [L : K] = |G|$. Let F be the fixed field of G. If $K \neq F$ then L has too many automorphisms fixing F pointwise.

Now let H be any subgroup of G and suppose that K is the fixed field of H. Let $\alpha \in L$ be such that $L = K[\alpha]$ and consider the polynomial

$$f(x) = \prod_{\sigma \in H} (x - \sigma\alpha).$$

It is easy to see that the coefficients of f are fixed by H, hence f has coefficients in K. Moreover α is a root of f. If $H \neq G$ then the degree of f is too small. □

The Galois Correspondence

Let L be normal over K and set $G = \text{Gal}(L/K)$. Define mappings

$$\left\{ \begin{matrix} \text{fields } F, \\ K \subset F \subset L \end{matrix} \right\} \Leftrightarrow \left\{ \begin{matrix} \text{groups } H, \\ H \subset G \end{matrix} \right\}$$

by sending each field F to $\text{Gal}(L/F)$ and each group H to its fixed field.

Theorem 55. *(*Fundamental Theorem of Galois Theory*) The mappings above are inverses of each other; thus they provide a one-to-one correspondence between the two sets. Moreover if $F \leftrightarrow H$ under this correspondence then F is normal over K iff H is a normal subgroup of G. In this case there is an isomorphism*

$$G/H \to \text{Gal}(F/K)$$

obtained by restricting automorphisms to F.

Proof. For each F, let F' be the fixed field of $\text{Gal}(L/F)$. Applying Theorem 54 in the right way, we obtain $F' = F$. (How do we know that L is normal over F?)

Now let H be a subgroup of G and let F be the fixed field of H.

Setting $H' = \text{Gal}(L/F)$, we claim that $H = H'$: Clearly $H \subset H'$, and by Theorem 54, F is not the fixed field of a proper subgroup of H'.

This shows that the two mappings are inverses of each other, establishing a one-to-one correspondence between fields F and groups H.

To prove the normality assertion, let F correspond to H and notice that for each $\sigma \in G$ the field σF corresponds to the group $\sigma H \sigma^{-1}$. F is normal over K iff $\sigma F = F$ for each embedding of F in $\mathbb{C}$ fixing K pointwise, and since each such embedding extends to an embedding of L which is necessarily a member of G, the condition for normality is equivalent to

$$\sigma F = F \; \forall \sigma \in G.$$

Since σF corresponds to $\sigma H \sigma^{-1}$, this condition is equivalent to

$$\sigma H \sigma^{-1} = H \; \forall \sigma \in G;$$

in other words, H is a normal subgroup of G.

Finally, assuming the normal case, we have a homomorphism

$$G \to \mathrm{Gal}(F/K)$$

whose kernel is H. This gives an embedding

$$G/H \to \mathrm{Gal}(F/K)$$

which must be onto since both groups have the same order. (Fill in the details.) □

Theorem 56. *Let L be normal over K and let E be any extension of K in $\mathbb{C}$. Then the composite field EL is normal over E and* $\mathrm{Gal}(EL/E)$ *is embedded in* $\mathrm{Gal}(L/K)$ *by restricting automorphisms to L. Moreover the embedding is an isomorphism iff $E \cap L = K$.*

Proof. Let $L = K[\alpha]$. Then

$$EL = E[\alpha]$$

which is normal over E because the conjugates of α over E are among the conjugates of α over K (why?), all of which are in L.

There is a homomorphism

$$\mathrm{Gal}(EL/E) \to \mathrm{Gal}(L/K)$$

obtained by restricting automorphisms to L, and the kernel is easily seen to be trivial. (If σ fixes both E and L pointwise then it fixes EL pointwise.) Finally consider the image H of $\mathrm{Gal}(EL/E)$ in $\mathrm{Gal}(L/K)$: Its fixed field is $E \cap L$ (because the fixed field of $\mathrm{Gal}(EL/E)$ is E), so by the Galois correspondence H must be $\mathrm{Gal}(L/E \cap L)$). Thus $H = \mathrm{Gal}(L/K)$ iff $E \cap L = K$. □

Appendix C
Finite Fields and Rings

Let F be a finite field. The additive subgroup generated by the multiplicative identity 1 is in fact a subring isomorphic to $\mathbb{Z}_m$, the ring of integers mod m, for some m. Moreover m must be a prime because F contains no zero divisors. Thus F contains $\mathbb{Z}_p$ for some prime p. Then F contains p^n elements, where $n = [F : \mathbb{Z}_p]$.

The multiplicative group $F^* = F - \{0\}$ must be cyclic because if we represent it as a direct product of cyclic groups

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$$

with $d_1 \mid d_2 \mid \cdots \mid d_r$ (every finite abelian group can be represented this way), then each member of F^* satisfies $x^d = 1$ where $d = d_r$. Then the polynomial $x^d - 1$ has $p^n - 1$ roots in F, implying $d \geq p^n - 1 = |F^*|$. This shows that F^* is just $\mathbb{Z}_d$.

F has an automorphism σ which sends each member of F to its p^{th} power. (Verify that this is really an automorphism. Use the binomial theorem to show that it is an additive homomorphism. Show that it is onto by first showing that it is one-to-one.) From the fact that F^* is cyclic of order $p^n - 1$ we find that σ^n is the identity mapping but no lower power of σ is; in other words σ generates a cyclic group of order n.

Taking α to be a generator of F^* we can write $F = \mathbb{Z}_p[\alpha]$. This shows that α is a root of an n^{th} degree irreducible polynomial over $\mathbb{Z}_p$. Moreover an automorphism of F is completely determined by its value at α, which is necessarily a conjugate of α over $\mathbb{Z}_p$. This shows that there are at most n such automorphisms, hence the group generated by σ is the full Galois group of F over $\mathbb{Z}_p$. All results from Appendix B are still true in this situation; in particular subgroups of the Galois group correspond to intermediate fields. Thus there is a unique intermediate field of degree d over $\mathbb{Z}_p$ for each divisor d of n.

Every member of F is a root of the polynomial $x^{p^n} - x$. This shows that $x^{p^n} - x$ splits into linear factors over F. Then so does each of its irreducible factors over $\mathbb{Z}_p$. The degree of such a factor must be a divisor of n because if one of its roots α is adjoined to $\mathbb{Z}_p$ then the resulting field $\mathbb{Z}_p[\alpha]$ is a subfield of F. Conversely, if f is an irreducible polynomial over $\mathbb{Z}_p$ of degree d dividing n, then f divides $x^{p^n} - x$. To see this, consider the field $\mathbb{Z}_p[x]/(f)$. This has degree d over $\mathbb{Z}_p$ and contains a root

D. A. Marcus, *Number Fields*, Universitext,
https://doi.org/10.1007/978-3-319-90233-3

α of f. By the previous argument every member of this field is a root of $x^{p^d} - x$, so f divides $x^{p^d} - x$. Finally, $x^{p^d} - x$ divides $x^{p^n} - x$.

The above shows that $x^{p^n} - x$ is the product of all monic irreducible polynomials over $\mathbb{Z}_p$ having degree dividing n.

This result can be used to prove the irreducibility of certain polynomials. For example to prove that $x^5 + x^2 + 1$ is irreducible over $\mathbb{Z}_2$ it is enough to show that it has no irreducible factors of degree 1 or 2; such a factor would also be a divisor of $x^4 - x$, so it is enough to show that $x^5 + x^2 + 1$ and $x^4 - x$ are relatively prime. Reducing mod $x^4 - x$ we have $x^4 \equiv x$, hence $x^5 \equiv x^2$, hence $x^5 + x^2 + 1 \equiv 1$. That proves it.

As another example we prove that $x^5 - x - 1$ is irreducible over $\mathbb{Z}_3$. It is enough to show that it is relatively prime to $x^9 - x$. Reducing mod $x^5 - x - 1$ we have $x^5 \equiv x + 1$, hence $x^9 \equiv x^5 + x^4 \equiv x^4 + x + 1$, hence $x^9 - x \equiv x^4 + 1$. The greatest common divisor of $x^9 - x$ and $x^5 - x - 1$ is the same as that of $x^4 + 1$ and $x^5 - x - 1$. Reducing mod $x^4 + 1$ we have $x^4 \equiv -1$, hence $x^5 \equiv -x$, hence $x^5 - x - 1 \equiv x - 1$. Finally it is obvious that $x - 1$ is relatively prime to $x^4 + 1$ because 1 is not a root of $x^4 + 1$.

The Ring $\mathbb{Z}_m$

Consider the ring $\mathbb{Z}_m$ of integers mod m for $m \geq 2$. The Chinese Remainder Theorem shows that $\mathbb{Z}_m$ is isomorphic to the direct product of the rings $\mathbb{Z}_{p^r}$ for all prime powers p^r exactly dividing m (which means that $p^{r+1} \nmid m$). Thus it is enough to examine the structure of the $\mathbb{Z}_{p^r}$. In particular we are interested in the multiplicative group $\mathbb{Z}_{p^r}^*$.

We will show that $\mathbb{Z}_{p^r}^*$ is cyclic if p is odd (we already knew this for $r = 1$) and that $\mathbb{Z}_{2^r}^*$ is almost cyclic when $r \geq 3$, in the sense that it has a cyclic subgroup of index 2.

More specifically, $\mathbb{Z}_{2^r}^*$ is the direct product

$$\{\pm 1\} \times \{1, 5, 9, \ldots, 2^r - 3\}.$$

We claim that the group on the right is cyclic, generated by 5. Since this group has order 2^{r-2}, it is enough to show that 5 has the same order.

Lemma. *For each $d \geq 0$, $5^{2^d} - 1$ is exactly divisible by 2^{d+2}.*

Proof. This is obvious for $d = 0$. For $d > 0$, write

$$5^{2^d} - 1 = (5^{2^{d-1}} - 1)(5^{2^{d-1}} + 1)$$

and apply the inductive hypothesis. Note that the second factor is $\equiv 2 \pmod 4$. □

Apply the lemma with 2^d equal to the order of 5. (It is clear that this order is a power of 2 since the order of the group is a power of 2.) We have $5^{2^d} \equiv 1 \pmod{2^r}$, so the lemma shows that $r \leq d + 2$. Equivalently, the order of 5 is at least 2^{r-2}. That completes the proof. □

Now let p be an odd prime and $r \geq 1$. We claim first that if $g \in \mathbb{Z}$ is any generator for $\mathbb{Z}_p^*$ then either g or $g + p$ is a generator for $\mathbb{Z}_{p^2}^*$. To see why this is true, note that $\mathbb{Z}_{p^2}^*$ has order $(p-1)p$ and both g and $g + p$ have orders divisible by $p - 1$ in $\mathbb{Z}_{p^2}^*$. (This is because both have order $p - 1$ in $\mathbb{Z}_p^*$.) Thus, to show that at least one of g and $g + p$ is a generator for $\mathbb{Z}_{p^2}^*$, it is sufficient to show that g^{p-1} and $(g + p)^{p-1}$ are not both congruent to 1 (mod p^2). We do this by showing that they are not congruent to each other. From the binomial theorem we get

$$(g + p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2},$$

which proves what we want. □

Finally we claim that any $g \in \mathbb{Z}$ which generates $\mathbb{Z}_{p^2}^*$ also generates $\mathbb{Z}_{p^r}^*$ for all $r \geq 1$.

Lemma. *Let p be an odd prime and suppose that $a - 1$ is exactly divisible by p. Then for each $d \geq 0$, $a^{p^d} - 1$ is exactly divisible by p^{d+1}.*

Proof. This holds by assumption for $d = 0$. For $d = 1$ write

$$\begin{aligned} a^p - 1 &= (a-1)(1 + a + a^2 + \cdots + a^{p-1}) \\ &= (a-1)(p + (a-1) + (a^2 - 1) + \cdots + (a^{p-1} - 1)) \\ &= (a-1)(p + (a-1)s) \end{aligned}$$

where s is the sum

$$1 + (a + 1) + (a^2 + a + 1) + \cdots + (a^{p-2} + \cdots + 1).$$

Since $a \equiv 1 \pmod{p}$ we have $s \equiv p(p-1)/2 \equiv 0 \pmod{p}$. From this we obtain the fact that $a^p - 1$ is exactly divisible by p^2.

Now let $d \geq 2$ and assume that $a^{p^{d-1}} - 1$ is exactly divisible by p^d. Writing

$$a^{p^d} - 1 = (a^{p^{d-1}} - 1)(1 + a^{p^{d-1}} + (a^{p^{d-1}})^2 + \cdots + (a^{p^{d-1}})^{p-1})$$

we find that it is enough to show that the factor on the right is exactly divisible by p. But this is obvious: $a^{p^{d-1}} \equiv 1 \pmod{p^d}$, hence the factor on the right is $\equiv p \pmod{p^d}$. Since $d \geq 2$, we are finished. □

Now assume $g \in \mathbb{Z}$ generates $\mathbb{Z}_{p^2}^*$ and let $r \geq 2$. The order of g in $\mathbb{Z}_{p^r}^*$ is divisible by $p(p-1)$ (because g has order $p(p-1)$ in $\mathbb{Z}_{p^2}^*$) and is a divisor of $p^{r-1}(p-1)$, which is the order of $\mathbb{Z}_{p^r}^*$. Thus the order of g has the form $p^d(p-1)$ for some $d \geq 1$.

Set $a = g^{p-1}$ and note that $a - 1$ is exactly divisible by p (why?). Moreover $a^{p^d} \equiv 1 \pmod{p^r}$. Applying the lemma, we obtain $r \leq d + 1$; equivalently, the order of g in $\mathbb{Z}_{p^r}^*$ is at least $p^{r-1}(p-1)$, which is the order of the whole group. That completes the proof. □

Appendix D
Two Pages of Primes

2	127	283	467	661	877	1087	1297	1523
3	131	293	479	673	881	1091	1301	1531
5	137	307	487	677	883	1093	1303	1543
7	139	311	491	683	887	1097	1307	1549
11	149	313	499	691	907	1103	1319	1553
13	151	317	503	701	911	1109	1321	1559
17	157	331	509	709	919	1117	1327	1567
19	163	337	521	719	929	1123	1361	1571
23	167	347	523	727	937	1129	1367	1579
29	173	349	541	733	941	1151	1373	1583
31	179	353	547	739	947	1153	1381	1597
37	181	359	557	743	953	1163	1399	1601
41	191	367	563	751	967	1171	1409	1607
43	193	373	569	757	971	1181	1423	1609
47	197	379	571	761	977	1187	1427	1613
53	199	383	577	769	983	1193	1429	1619
59	211	389	587	773	991	1201	1433	1621
61	223	397	593	787	997	1213	1439	1627
67	227	401	599	797	1009	1217	1447	1637
71	229	409	601	809	1013	1223	1451	1657
73	233	419	607	811	1019	1229	1453	1663
79	239	421	613	821	1021	1231	1459	1667
83	241	431	617	823	1031	1237	1471	1669
89	251	433	619	827	1033	1249	1481	1693
97	257	439	631	829	1039	1259	1483	1697
101	263	443	641	839	1049	1277	1487	1699
103	269	449	643	853	1051	1279	1489	1709
107	271	457	647	857	1061	1283	1493	1721
109	277	461	653	859	1063	1289	1499	1723
113	281	463	659	863	1069	1291	1511	1733
1741	2089	2437	2791	3187	3541	3911	4271	4663
1747	2099	2441	2797	3191	3547	3917	4273	4673
1753	2111	2447	2801	3203	3557	3919	4283	4679
1759	2113	2459	2803	3209	3559	3923	4289	4691
1777	2129	2467	2819	3217	3571	3929	4297	4703
1783	2131	2473	2833	3221	3581	3931	4327	4721

D. A. Marcus, *Number Fields*, Universitext,
https://doi.org/10.1007/978-3-319-90233-3

1787	2137	2477	2837	3229	3583	3943	4337	4723
1789	2141	2503	2843	3251	3593	3947	4339	4729
1801	2143	2521	2851	3253	3607	3967	4349	4733
1811	2153	2531	2857	3257	3613	3989	4357	4751
1823	2161	2539	2861	3259	3617	4001	4363	4759
1831	2179	2543	2879	3271	3623	4003	4373	4783
1847	2203	2549	2887	3299	3631	4007	4391	4787
1861	2207	2551	2897	3301	3637	4013	4397	4789
1867	2213	2557	2903	3307	3643	4019	4409	4793
1871	2221	2579	2909	3313	3659	4021	4421	4799
1873	2237	2591	2917	3319	3671	4027	4423	4801
1877	2239	2593	2927	3323	3673	4049	4441	4813
1879	2243	2609	2939	3329	3677	4051	4447	4817
1889	2251	2617	2953	3331	3691	4057	4451	4831
1901	2267	2621	2957	3343	3697	4073	4457	4861
1907	2269	2633	2963	3347	3701	4079	4463	4871
1913	2273	2647	2969	3359	3709	4091	4481	4877
1931	2281	2657	2971	3361	3719	4093	4483	4889
1933	2287	2659	2999	3371	3727	4099	4493	4903
1949	2293	2663	3001	3373	3733	4111	4507	4909
1951	2297	2671	3011	3389	3739	4127	4513	4919
1973	2309	2677	3019	3391	3761	4129	4517	4931
1979	2311	2683	3023	3407	3767	4133	4519	4933
1987	2333	2687	3037	3413	3769	4139	4523	4937
1993	2339	2689	3041	3433	3779	4153	4547	4943
1997	2341	2693	3049	3449	3793	4157	4549	4951
1999	2347	2699	3061	3457	3797	4159	4561	4957
2003	2351	2707	3067	3461	3803	4177	4567	4967
2011	2357	2711	3079	3463	3821	4201	4583	4969
2017	2371	2713	3083	3467	3823	4211	4591	4973
2027	2377	2719	3089	3469	3833	4217	4597	4987
2029	2381	2729	3109	3491	3847	4219	4603	4993
2039	2383	2731	3119	3499	3851	4229	4621	4999
2053	2389	2741	3121	3511	3853	4231	4637	5003
2063	2393	2749	3137	3517	3863	4241	4639	5009
2069	2399	2753	3163	3527	3877	4243	4643	5011
2081	2411	2767	3167	3529	3881	4253	4649	5021
2083	2417	2777	3169	3533	3889	4259	4651	5023
2087	2423	2789	3181	3539	3907	4261	4657	5039
5051	5179	5309	5437	5531	5659	5791	5879	6043
5059	5189	5323	5441	5557	5669	5801	5881	6047
5077	5197	5333	5443	5563	5683	5807	5897	6053
5081	5209	5347	5449	5569	5689	5813	5903	6067
5087	5227	5351	5471	5573	5693	5821	5923	6073
5099	5231	5381	5477	5581	5701	5827	5927	6079
5101	5233	5387	5479	5591	5711	5839	5939	6089
5107	5237	5393	5483	5623	5717	5843	5953	6091
5113	5261	5399	5501	5639	5737	5849	5981	6101
5119	5273	5407	5503	5641	5741	5851	5987	6113
5147	5279	5413	5507	5647	5743	5857	6007	
5153	5281	5417	5519	5651	5749	5861	6011	
5167	5297	5419	5521	5653	5779	5867	6029	
5171	5303	5431	5527	5657	5783	5869	6037	

Further Reading

Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag, New York, 1993.

H. Cohn, *A Classical Introduction to Algebraic Number Theory and Class Field Theory*, Springer-Verlag, New York, 1978.

H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, GTM 50, Springer-Verlag, New York, 1977.

K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second edition, GTM 84, Springer-Verlag, New York, 1982.

S. Lang, *Algebraic Number Theory*, second edition, GTM 110, Springer-Verlag, New York, 1994.

J. Neukirch, *Class Field Theory*, Springer-Verlag, New York, 1986.

M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge, 1989.

P. Samuel, *Algebraic Theory oJ Numbers*, Houghton-Mifflin, Boston, 1970.

L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

D. A. Marcus, *Number Fields*, Universitext,
https://doi.org/10.1007/978-3-319-90233-3

Index of Theorems

D. A. Marcus, *Number Fields*, Universitext,
https://doi.org/10.1007/978-3-319-90233-3

Index

D. A. Marcus, *Number Fields*, Universitext,
https://doi.org/10.1007/978-3-319-90233-3

T

U

V