MATD01 Fields and Groups

Assignment 3

Solutions

1. By Lagrange's theorem every element $\alpha \in F^\times$ satisfies $\alpha^{q-1} = \alpha^{|F^\times|} = 1$, so that every element of $F^\times$ is a root of $x^{q-1} - 1$. Thus

$$\prod_{\alpha \in F^\times} (x - \alpha) \;\Big|\; (x^{q-1} - 1).$$

Comparing first the degrees and then the leading coefficients we get

$$\prod_{\alpha \in F^\times} (x - \alpha) \;=\; x^{q-1} - 1.$$

Now compare coefficients of x^{q-2} (resp. 1) in the two sides of the equality to get the formulas (i) and (ii). (For (ii) you should consider the case of characteristic 2 separately.)

2. (a) Suppose (r) is maximal for some nonzero r. Then by the definition of a maximal ideal, $(r) \neq R$ and hence r is not a unit. Now suppose $r = ab$ for some $a, b \in R$. We then have $(r) \subset (a)$. It follows from the maximality of (r) that either $(a) = (r)$ or $(a) = R$. In the former case, since R is an integral domain, we must have $r = au$ for some unit u (why?), and again since R is an integral domain and $a \neq 0$ (as $r \neq 0$) it follows from $ab = au$ that $b = u$; hence b is a unit. On the other hand, if $(a) = R$ then a is a unit.

Remark: We will shortly see that the hypothesis of maximality of (r) here can be weakened; it is enough to assume that the ideal (r) is prime. (We'll define prime ideals soon. Any maximal ideal is prime.)

(b) Suppose R is a PID and $r \in R$ is irreducible. Let $(r) \subset I$ for some ideal $I \subset R$. We shall argue that I is either (r) or R. Since R is a PID, $I = (a)$ for some $a \in R$. Then $(r) \subset (a)$ gives $r = ab$ for some $b \in R$. Since r is irreducible, either a or b must be a unit. In the former case $I = R$ and in the latter case $(r) = (a)$ (why?).

(c) Let F be any field. Let $f(x)$ be an irreducible element of $F[x]$. Since $F[x]$ is a PID, by Part (b) above the ideal $(f(x))$ of $F[x]$ is maximal. By Problem 3 of last assignment $F[x]/(f(x))$ is a field.

Take $F = \mathbb{F}_2$ and $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Being of degree 2, the polynomial $f(x)$ is irreducible in $\mathbb{F}_2[x]$ if and only if $f(x)$ has no root in $\mathbb{F}_2$. Checking $x = 0, 1$ we see that $x^2 + x + 1$ indeed has no root in $\mathbb{F}_2$, hence is irreducible. Thus $K = \mathbb{F}_2[x]/(x^2 + x + 1)$ is a field. By Problem 5 of last assignment K has 4 elements.

3. (a) true

(b) Let I be any proper ideal of a principal ideal domain R. Suppose I contains an irreducible element r. We claim that then $I = (r)$. Indeed, by Problem 2(b) above, the ideal (r) is maximal. Combining with $(r) \subset I$ and properness of I it follows that $(r) = I$. Applying this to $R = F[x]$ and $I = \ker(ev_\alpha)$ we get that if $f(x) \in \ker(ev_\alpha)$ is irreducible, then $\ker(ev_\alpha) = (f(x))$.

Conversely, suppose $\ker(ev_\alpha) = (f(x))$. Since $\ker(ev_\alpha)$ is a proper ideal (of $F[x]$), $f(x)$ is not a unit. Suppose $f(x) = g(x)h(x)$. Then $0 = f(\alpha) = g(\alpha)h(\alpha)$, so that $g(\alpha)$ or $h(\alpha)$ must be zero. Suppose $g(\alpha) = 0$. Then $g(x) \in \ker(ev_\alpha)$, so that $f(x) \mid g(x)$ (why?).

Combining with $f(x) = g(x)h(x)$, in view of $f(x) \neq 0$ (which holds because α is algebraic) and the fact that $F[x]$ is a domain, it follows that $h(x)$ must be a unit (why?). (Alternative argument using results from Chapter 7: By the first isomorphism theorem $F[x]/\ker(ev_\alpha)$ is isomorphic to a subring of K, hence is an integral domain (why?). Thus $\ker(ev_\alpha)$ is a prime ideal. Since α is algebraic, $\ker(ev_\alpha)$ is nonzero. Thus any generator of $\ker(ev_\alpha)$ is irreducible.)

We now know that the following two conditions are equivalent for any element $f(x) \in \ker(ev_\alpha)$:

(i) $f(x)$ is monic and generates $\ker(ev_\alpha)$.
(ii) $f(x)$ is monic and irreducible.

Being a nonzero ideal of $F[x]$, the ideal $\ker(ev_\alpha)$ has a unique element $f(x)$ satisfying (i). The same element is the unique element satisfying (ii).

(c) The minimal polynomial of i over $\mathbb{Q}$ is $f(x) = x^2 + 1$ ($f(x)$ is irreducible, monic and satisfies $f(i) = 0$). The minimal polynomial of $\sqrt{2} + 1$ over $\mathbb{Q}$ is $g(x) = x^2 - 2x - 1$ (why?).

(d) Let n be the dimension of K as a vector space over F. Given $\alpha \in K$, consider the elements α^j ($0 \leq j \leq n$). Since K is n-dimensional over F, any $n + 1$ elements of K are F-linearly dependent. In particular, there are $c_j \in F$ ($0 \leq j \leq n$), not all zero, such that $\sum_{j=0}^{n} c_j\alpha^j = 0$. Then α is a root of the nonzero polynomial $\sum_{j=0}^{n} c_j x^j \in F[x]$.

4. For each $\alpha \in \mathbb{C}$, let $ev_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ be the map defined by $ev_\alpha(f(x)) = f(\alpha)$ (evaluation at α). We claim that

$$\mathrm{Hom}(\mathbb{Q}[x], \mathbb{C}) = \{ev_\alpha : \alpha \in \mathbb{C}\}.$$

We leave it to the reader to check that the maps ev_α are indeed ring homomorphisms. Given arbitrary $\phi \in \mathrm{Hom}(\mathbb{Q}[x], \mathbb{C})$, set $\alpha = \phi(x)$. Then for any $f(x) = \sum_i c_i x^i \in \mathbb{Q}[x]$,

$$\phi(f(x)) \overset{\text{why?}}{=} \sum_i \phi(c_i)\phi(x)^i \overset{(*)}{=} \sum_i c_i\alpha^i = ev_\alpha(f(x)),$$

so that $\phi = ev_\alpha$. (Note that in $(*)$ we used the following fact, which we leave it to the reader to check: if $\phi : \mathbb{Q} \to \mathbb{C}$ is a ring homomorphism, then $\phi(c) = c$ for every $c \in \mathbb{Q}$.)

(b) Throughout the solution, given any $r \in R$ we write $\bar{r}$ for the element $r + I$ of R/I.

First we show the "if" statement. Suppose there is a ring homomorphism $\overline{\phi} : R/I \to S$ such that $\phi = \overline{\phi} \circ \pi$. Then

$$I = \ker(\pi) \overset{\text{why?}}{\subset} \ker(\phi).$$

To prove the "only if" statement, let us assume for the moment that a map $\overline{\phi} : R/I \to S$ satisfying $\phi = \overline{\phi} \circ \pi$ exists. Given any $T \in R/I$, we have $T = \bar{r}$ for some $r \in R$, and from $\phi = \overline{\phi} \circ \pi$ we have

$$\overline{\phi}(T) = \overline{\phi}(\bar{r}) = \overline{\phi}(\pi(r)) = \phi(r).$$

Back to the proof of the "only if" statement, suppose $I \subset \ker(\phi)$. *Define* $\overline{\phi} : R/I \to S$ by the formula suggested above, that is, given $T \in R/I$ with $T = \bar{r}$, set $\overline{\phi}(T) = \phi(r)$ (as observed above, if the map $\overline{\phi}$ exists, it has to be given by this formula). The assumption $I \subset \ker(\phi)$ guarantees that $\overline{\phi}$ is well-defined. Indeed, if $\bar{r} = \overline{r'}$ for some $r, r' \in R$, then $r - r' \in I$. Thanks to $I \subset \ker(\phi)$ we thus have $\phi(r) = \phi(r')$. We leave it to the reader to check that $\overline{\phi}$

(which at the moment, is a function $R/I \to S$) is a ring homomorphism. That $\phi = \overline{\phi} \circ \pi$ holds is by construction of $\overline{\phi}$:

$$\overline{\phi} \circ \pi(r) = \overline{\phi}(\overline{r}) = \phi(r).$$

Now the "moreover" statement: this follows from the following general fact about functions: if $f : X \to Y$ and $g_1, g_2 : Y \to Z$ are functions, f is surjective, and $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$. We leave checking this to the reader. Applying it to our situation, $\overline{\phi} \circ \pi = \overline{\phi}' \circ \pi$ implies $\overline{\phi} = \overline{\phi}'$.

Finally, for the last assertion, consider

$$\Gamma : \{\phi \in \mathrm{Hom}(R, S) : I \subset \ker(\phi)\} \;\to\; \mathrm{Hom}(R/I, S)$$

given by

$$\phi \;\mapsto\; \overline{\phi}$$

(with notation as above). This makes sense by the "only if" part of the statement we proved earlier(and its proof, where we said what $\overline{\phi}$ is). We claim that Γ is a bijection. Indeed, we shall construct the inverse to Γ: given any $\psi \in \mathrm{Hom}(R/I, S)$, the composition $\psi \circ \pi$ is a ring homomorphism $R \to S$ and satisfies $I = \ker(\pi) \subset \ker(\psi \circ \pi)$. Define

$$\Lambda : \mathrm{Hom}(R/I, S) \to \{\phi \in \mathrm{Hom}(R, S) : I \subset \ker(\phi)\}$$

by

$$\psi \mapsto \pi \circ \psi.$$

We now check that $\Lambda = \Gamma^{-1}$: for any $\phi \in \mathrm{Hom}(R, S)$ satisfying $I \subset \ker(\phi)$, we have

$$\Lambda \circ \Gamma(\phi) = \Lambda(\overline{\phi}) = \pi \circ \overline{\phi} = \phi.$$

(so the composition $\Lambda \circ \Gamma$ is identity). On the other hand, given any $\psi \in \mathrm{Hom}(R/I, S)$,

$$\Gamma \circ \Lambda(\psi) = \Gamma(\psi \circ \pi) = \overline{\psi \circ \pi} = \psi.$$

(For the last equality, we have used $\overline{\psi \circ \pi} \circ \pi = \psi \circ \pi$ (which holds by definition of $\overline{\psi \circ \pi}$) and surjectivity of π - see the remark we made in the proof of the "moreover" statement.)

(c) Let us focus on homomorphisms $\mathbb{Q}[x]/(x^3 - 2) \to \mathbb{C}$ first. By Part (b), we need to find homomorphisms $\mathbb{Q}[x] \to \mathbb{C}$ which map $I = (x^3 - 2)$ to zero. Part (a) describes all homomorphisms $\mathbb{Q}[x] \to \mathbb{C}$: each is of the form $ev_\alpha : f(x) \mapsto f(\alpha)$ for some $\alpha \in \mathbb{C}$. For ev_α to send $x^3 - 2$ to zero, α has to be a root of $x^3 - 2$. Thus there are three homomorphisms $\mathbb{Q}[x] \to \mathbb{C}$ that vanish on I, namely $ev_{\sqrt[3]{2}} : f(x) \mapsto f(\sqrt[3]{2})$, $ev_{\sqrt[3]{2}\omega} : f(x) \mapsto f(\sqrt[3]{2}\omega)$, and $ev_{\sqrt[3]{2}\omega^2} : f(x) \mapsto f(\sqrt[3]{2}\omega^2)$, where $\sqrt[3]{2}$ is the positive third root of 2 and $\omega = e^{2\pi i/3}$. Each induces a map $\mathbb{Q}[x]/(x^3-2) \to \mathbb{C}$ (and these are the only homomorphisms $\mathbb{Q}[x]/(x^3-2) \to \mathbb{C}$); they are the maps

$$\overline{ev_{\sqrt[3]{2}}} : \overline{f(x)} \mapsto f(\sqrt[3]{2}), \quad \overline{ev_{\sqrt[3]{2}\omega}} : \overline{f(x)} \mapsto f(\sqrt[3]{2}\omega), \quad \overline{ev_{\sqrt[3]{2}\omega^2}} : \overline{f(x)} \mapsto f(\sqrt[3]{2}\omega^2).$$

Out of these only the first one gives a map into $\mathbb{R}$.

Now on to the kernels and images. The kernels are all zero, as irreducibility of $x^3 - 2$ over $\mathbb{Q}$ implies that $\mathbb{Q}[x]/(x^3-2)$ is a field. The image of $\overline{ev_\alpha}$ (for $\alpha = \sqrt[3]{2}$, $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$) is by definition $\{f(\alpha) : f[x] \in \mathbb{Q}[x]\}$. By Question 1 on Assignment 1, this can be expressed more simply as

$$\mathrm{Im}(\overline{ev_\alpha}) = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$$

(make sure you agree). Each of the images is a 3-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \alpha, \alpha^2\}$. (The dimension is 3 and not less since otherwise α would be a root of a polynomial of degree < 3 with coefficients in $\mathbb{Q}$, which is absurd: being irreducible, $x^3 - 2$ is the minimal polynomial of α over $\mathbb{Q}$.)

Note that $\mathrm{Im}(\overline{ev_{\sqrt[3]{2}}})$ is real, and hence is different from $\mathrm{Im}(\overline{ev_{\sqrt[3]{2}\omega}})$ and $\mathrm{Im}(\overline{ev_{\sqrt[3]{2}\omega^2}})$. We claim that the latter two images are also different. Indeed, if

$$\mathrm{Im}(\overline{ev_{\sqrt[3]{2}\omega}}) = \mathrm{Im}(\overline{ev_{\sqrt[3]{2}\omega^2}}) =: K,$$

then K contains both $\sqrt[3]{2}^2\omega^2$ and $\sqrt[3]{2}\omega^2$, and hence contains $\sqrt[3]{2}$ (why? do we know that K is a field?). It follows that K contains $\mathrm{Im}(\overline{ev_{\sqrt[3]{2}}})$, and then comparing dimensions (as vector spaces over $\mathbb{Q}$) we get $K = \mathrm{Im}(\overline{ev_{\sqrt[3]{2}}})$, which is absurd.

(d) Similar to the previous part, there are three maps $\mathbb{Q}[x]/(x^3 - 8) \to \mathbb{C}$ and they are induced by evaluation maps at the roots of $x^3 - 8$:

$$\overline{ev_2} : \overline{f(x)} \mapsto f(2), \quad \overline{ev_{2\omega}} : \overline{f(x)} \mapsto f(2\omega), \quad \overline{ev_{2\omega^2}} : \overline{f(x)} \mapsto f(2\omega^2)$$

(where $\omega = e^{2\pi i/3}$ again).

The situation for images and kernels is different from the previous part, as $x^3 - 8$ is not irreducible over $\mathbb{Q}$. Its factorization as a product of irreducible elements is $(x-2)(x^2 + 2x + 4)$. Here 2ω and $2\omega^2$ are roots of $x^2 + 2x + 4$. The image of $\overline{ev_\alpha}$ (which by definition is $\{f(\alpha) : f[x] \in \mathbb{Q}[x]\}$) is simply $\mathbb{Q}$ if $\alpha = 2$. On the other hand, for $\alpha = 2\omega, 2\omega^2$ the image $\mathrm{Im}(ev_\alpha)$ is a 2-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \alpha\}$ (why?). We leave it to the reader to check that

$$\mathrm{Im}(ev_{2\omega}) = \mathrm{Im}(ev_{2\omega^2}).$$

(Use $\omega^2 = -\omega - 1$.)

Finally, here are the kernels:

$$\ker(\overline{ev_2}) = (\overline{x-2}), \qquad \ker(\overline{ev_{2\omega}}) = \ker(\overline{ev_{2\omega^2}}) = (\overline{x^2 + 2x + 4}).$$

5. (a) $x^2 - 1$. We leave the calculations to the reader. (See the last few practice questions on Assignment 5 for a general result regarding the gcd of $x^m - 1$ and $x^n - 1$.)

(b) The gcd does not change if we enlarge the field, as the calculations in Euclid's algorithm will stay exactly the same.

(c) in $\mathbb{Q}[x]$: $x^6 - 1 = (x-1)(x+1)(x^2 + x + 1)(x^2 - x + 1)$. The last two factors are irreducible over $\mathbb{Q}$ because they don't have any rational roots.

in $\mathbb{C}[x]$: $x^6 - 1 = \prod_{i=0}^{5}(x - \zeta^i)$, $\zeta = e^{2\pi i/6}$.