MATD01 Fields and Groups

Assignment 6

Solutions

1. We leave this to the reader.

2. (a) The order of every element of the group μ_n divides $|\mu_n| = n$. Grouping the elements of μ_n based on their orders we have

$$x^n - 1 \;=\; \prod_{\zeta\in\mu_n}(x-\zeta) \;=\; \prod_{d\Big|n}\left(\prod_{\zeta\in\mu_n,|\zeta|=d}(x-\zeta)\right) \;=\; \prod_{d|n}\phi_d(x).$$

(b) We shall need the following version of the division algorithm: if R is an integral domain, $f(x), g(x) \in R[x]$ with the leading coefficient of $g(x)$ a unit, then there exist unique $q(x), r(x) \in R[x]$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$.
We prove by induction on n that the cyclotomic polynomial $\phi_n(x)$ has integral coefficients. Indeed, the assertion certainly holds for $n = 1$ as $\phi_1(x) = x - 1$. Suppose $\phi_d(x)$ has integral coefficients for every $d < n$. Take

$$g(x) = \prod_{d|n,d\neq n}\phi_d(x).$$

Then $g(x)$ is monic and with coefficients in $\mathbb{Z}$ (as each $\phi_d(x)$ is monic and with coefficients in $\mathbb{Z}$). Applying the division algorithm in $\mathbb{Z}[x]$ there are unique $q(x), r(x) \in \mathbb{Z}[x]$ such that $x^n - 1 = q(x)g(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$. The same $q(x)$ and $r(x)$ satisfy the properties of a quotient and remainder of $x^n - 1$ in division by $g(x)$ in $\mathbb{C}[x]$. By uniqueness of quotient and remainder, they are *the* quotient and remainder of of $x^n - 1$ in division by $g(x)$ in $\mathbb{C}[x]$. But we also know that in $\mathbb{C}[x]$,

$$x^n - 1 = \phi_n(x)g(x).$$

It follows that $q(x) = \phi_n(x)$ and $r(x) = 0$. In particular, $\phi_n(x)$ is in $\mathbb{Z}[x]$.

(c) Step One: We show that given any monic $h(x) \in \mathbb{Z}[x]$ of positive degree, we have $h(x) = f(x)g(x)$ for some monic $f(x), g(x) \in \mathbb{Z}[x]$ with $f(x)$ irreducible over $\mathbb{Q}$. We do this by induction on the degree of $h(x)$. If $h(x)$ is of degree 1, take $f(x) = h(x)$ and $g(x) = 1$. Suppose the assertion holds for polynomials of degree $< m$. Consider a monic polynomial $h(x) \in \mathbb{Z}[x]$ of degree m. If $h(x)$ is irreducible over $\mathbb{Q}$, take $f(x) = h(x)$ and $g(x) = 1$. Otherwise, by Gauss lemma $h(x)$ factors as $h(x) = k(x)l(x)$ for some $k(x), l(x) \in \mathbb{Z}[x]$ of degree less than $\deg(h(x)) = m$. Since $h(x)$ is monic, (by possibly multiplying both polynomials with -1) we may assume that $k(x)$ and $l(x)$ are monic. Then by the induction hypothesis we can express $k(x) = k_1(x)k_2(x)$ for some monic $k_1(x), k_2(x) \in \mathbb{Z}[x]$ and $k_1(x)$ irreducible over $\mathbb{Q}$. Taking $f(x) = k_1(x)$ and $g(x) = k_2(x)l(x)$ we get the desired decomposition of $h(x)$.
Step Two:

(i) ζ is a root of $\phi_n(x)$, hence is a primitive n-th root of unity. Since n and p are relatively prime, ζ^p is also primitive n-th root of unity. Thus $f(\zeta^p)g(\zeta^p) = \phi_n(\zeta^p) = 0$. Since $f(\zeta^p) \neq 0$, it follows that $g(\zeta^p) = 0$. Thus ζ is a root of $g(x^p)$.
Since $f(x)$ is monic and irreducible in $\mathbb{Q}[x]$ and $f(\zeta) = 0$, it follows that $f(x)$ is the minimal polynomial of ζ over $\mathbb{Q}$. Since $g(x^p) \in \mathbb{Q}[x]$ and ζ is a root of $g(x^p)$, we have $f(x) \mid g(x^p)$ in $\mathbb{Q}[x]$. Since both $f(x)$ and $g(x^p)$ have coefficients in $\mathbb{Z}$ and $f(x)$ is monic, the uniqueness of quotient and remainder in the division algorithm implies that $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$ (similar to the argument we gave in part (b)).

(ii) Since $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$ and π^* is a ring map, we have $\pi^*(f(x)) \mid \pi^*(g(x^p))$ in $\mathbb{F}_p[x]$. The equality $\pi^*(g(x^p)) = (\pi^*(g(x)))^p$ is because Fröbenius $\mathbb{F}_p[x] \to \mathbb{F}_p[x]$ is a ring map and $\alpha^p = \alpha$ for every $\alpha \in \mathbb{F}_p$: if $g(x) = \sum a_i x^i$ then

$$\pi^*(g(x^p)) = \pi^*(\sum a_i x^{pi}) = \sum \pi(a_i)x^{pi} \overset{(*)}{=} (\sum \pi(a_i)x^i)^p = (\pi^*(g(x)))^p.$$

(Note that in $(*)$ not only we used the fact that $Fr : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$ defined by $h(x) \mapsto h(x)^p$ is a ring map, we also used the fact that $\alpha^p = \alpha$ for every $\alpha \in \mathbb{F}_p$.)

(iii) From (ii) we know that $\pi^*(f(x)) \mid (\pi^*(g(x)))^p$ (in $\mathbb{F}_p[x]$). Since $f(x)$ is monic and with positive degree, so is $\pi^*(f(x))$. Since $\mathbb{F}_p[x]$ is a PID, the polynomial $\pi^*(f(x)) \in \mathbb{F}_p[x]$ is a product of irreducible polynomials. Any of these irreducible factors of $\pi^*(f(x))$ also divides $(\pi^*(g(x)))^p$, and hence (by Euclid's lemma for a PID) divides $\pi^*(g(x))$ as well. (Remember that in a PID, if an irreducible element r divides ab, then r divides a or b.)
Take a common irreducible factor $h(x)$ of $\pi^*(f(x))$ and $\pi^*(g(x))$. Then $h(x)^2 \mid \pi^*(f(x))\pi^*(g(x)) = \pi^*(\phi_n(x))$. Since $\phi_n(x) \mid x^n - 1$ in $\mathbb{Z}[x]$ and π^* is a ring map, we have $\pi^*(\phi_n(x)) \mid x^n - 1$. It follows that $h(x)^2 \mid x^n - 1$. Any root of $h(x)$ (in any field extension of $\mathbb{F}_p$) is then a repeated root of $x^n - 1$.

(iv) Up to this point, assuming that $f(\zeta^p) \neq 0$ we have shown that $x^n - 1 \in \mathbb{F}_p[x]$ has repeated roots. Now we use the criterion for having repeated roots in terms of the derivative to show that actually $x^n - 1 \in \mathbb{F}_p[x]$ has no repeated roots (and the contradiction would prove that $f(\zeta^p) = 0$, as desired). The derivative of $x^n - 1 \in \mathbb{F}_p[x]$ is nx^{n-1}. Note that $n \neq 0$ as $p \nmid n$. The only root of nx^{n-1} (in any extension of $\mathbb{F}_p$) is zero, and zero is not a root of $x^n - 1$. Thus indeed $x^n - 1 \in \mathbb{F}_p[x]$ has no repeated roots.

Step Three: In the previous step we showed that for any root ζ of $f(x)$ and any prime number $p \nmid n$, the number ζ^p is also a root of $f(x)$. Let m be a positive integer with $gcd(m, n) = 1$. We want to show that if ζ is a root of $f(x)$, then so is ζ^m. This is trivial for $m = 1$. If $m > 1$, we can express m as $m = p_1 \cdots p_k$ for some (non necessarily distinct) primes $p_1, ..., p_k \nmid n$. Then by the result of Step Two, ζ^{p_1} is a root of $f(x)$. Next, by the same result, $\zeta^{p_1 p_2} = (\zeta^{p_1})^{p_2}$ is a root of $f(x)$. Applying the same result again we see $\zeta^{p_1 p_2 p_3} = (\zeta^{p_1 p_2})^{p_3}$ is a root of $f(x)$, and so on.

Showing $f(x) = \phi_n(x)$: Since $f(x)$ is irreducible, it has positive degree. Let ζ_0 be a root of $f(x)$. By $f(x) \mid \phi_n(x)$ we know that ζ_0 is a primitive n-th root of unity. Now every primitive n-th root of unity is of the form ζ_0^m for some positive integer coprime to n. It follows that every primitive n-th root of unity is a root of $f(x)$. Thus $\phi_n(x) \mid f(x)$ (why?). Since $f(x)$ and $\phi_n(x)$ are both monic we get $\phi_n(x) = f(x)$ (note that we already knew that $f(x) \mid \phi_n(x)$).

(d) Because we wanted to pass on to $\mathbb{F}_p[x]$ and for that we needed to know that the coefficients of the polynomials in the picture are integers.

3. (a) Let F be the set of elements of K which are fixed by Fröbenius (that is, the set of $\alpha \in K$ such that $\alpha^p = \alpha$). Then $\mathbb{F}_p$ is certainly contained in F (by Fermat's little theorem). To see that $F = \mathbb{F}_p$, now note that F is the set of all roots of $x^p - p$ in K. Being of degree p, the polynomial $x^p - p$ can have at most p roots in K. We know every element of $\mathbb{F}_p$ is a root; that is already p roots and thus there are no more roots.

(b) Since K has characteristic p, the map $Fr : K \to K$ is a ring map. Since K is a field, Fr is injective. Finally, since K is finite, any injective function $K \to K$ is also surjective.

4. (a) $(a, b) \sim (a, b)$ means $ab = ba$.
$(a, b) \sim (c, d)$ and $(c, d) \sim (a, b)$ both amount to $ad = bc$.
Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. Multiplying the two we get $af(cd) = be(cd)$. Since c and d are nonzero and R is an integral domain, this implies that $af = be$, i.e. $(a, b) \sim (e, f)$.

(b) Since R is a domain, $bd \neq 0$ if b and d are nonzero, so the expressions $\frac{ad+bc}{bd}$ and $\frac{ac}{bd}$ make sense. To check that the operations are well-defined, we need to check that if $a/b = a'/b'$ and $c/d = c'/d'$, then

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} \tag{1}$$

and

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}. \tag{2}$$

Eq. (1) amounts to

$$(ad + bc)b'd' = (a'd' + b'c')bd,$$

which can be rewritten as

$$dd'(ab' - a'b) + bb'(cd' - c'd) = 0,$$

which in turn is clear because $ab' = a'b$ and $cd' = c'd$. As for Eq. (2), it can be rewritten as

$$acb'd' = a'c'bd,$$

which follows right away from $ab' = a'b$ and $cd' = c'd$ (just multiply them).

(c) We leave the verification of the various axioms to the reader. The zero element is $0/1$ ($= 0/a$ for any nonzero a) and the multiplicative identity is $1/1$ ($= a/a$ for any nonzero a), the additive inverse of a/b is $(-a)/b$, and the multiplicative inverse of a/b with both a and b nonzero is b/a.

Define $\iota : R \to Frac(R)$ defined by $\iota(a) = \frac{a}{1}$. Then ι is a ring map, because $\iota(1) = 1/1 = 1_{Frac(R)}$,

$$\iota(a+b) = (a+b)/1 = a/1 \ + \ b/1 = \iota(a) + \iota(b)$$

and

$$\iota(ab) = (ab)/1 = (a/1) \cdot (b/1) = \iota(a)\iota(b).$$

(Note that the middle equalities in both equations can be seen from the definition of addition and multiplication in $Frac(R)$.)
Finally, to see that ι is injective, let $a \in \ker(\iota)$. Then $a/1 = 0_{Frac(R)} = 0/1$, so that $a \cdot 1 = 1 \cdot 0$. It follows that $a = 0$.

(d) The only assertion here is transcendence of $F(x)$ over F (as $F(x)$ is a field and contains F via the identifications $F \subset F[x] \subset F(x)$). For this it is enough to find one element of $F(x)$ which is transcendental (i.e. not algebraic) over F. We claim that x is such an element. Indeed, $F(x)$ is the subfield of $F(x)$ obtained by adjoining x to F; note that this is not by definition (and nor is just playing with words): here we defined $F(x)$ as $Frac(F[x])$, and we are claiming is that the smallest subfield of $F(x)$ which contains F and x is $F(x)$ itself. Indeed, if any subfield of $F(x)$ contains F and x, then it contains all polynomials $f(x) \in F[x]$, and hence (being closed under taking reciprocals) contains all the elements $1/f(x)$ with $f(x) \in F[x]$ nonzero, and hence all the elements of $F(x)$. Thus $F(x)$ is the subfield of $F(x)$ obtained by adjoining x to F. Now if x is algebraic over F, the extension $F(x)/F$ is finite. Since $F[x] \subset F(x)$, this implies that $F[x]$ is a finite-dimensional vector space over F, which is absurd: the elements x^n ($n \geq 0$) of $F[x]$ are F-linearly independent.

(e) Before we start the proof, let us make an observation. Let α be any element of K, algebraic or transcendental over F. The subfield $F(\alpha)$ of K is exactly the set

$$\{a(\alpha)/b(\alpha) : a(x), b(x) \in F[x],\ b(\alpha) \neq 0\}. \tag{3}$$

Indeed, being a subfield of K that contains F and α, the field $F(\alpha)$ must contains the set Eq. (3). On the other hand, one can directly check that the set Eq. (3) is indeed a field itself; moreover it clearly contains F and α. It follows that it contains $F(\alpha)$.
Now we go back to the question at hand. Suppose α is transcendental over F. Then (by definition), for every nonzero $b(x) \in F[x]$ we have $b(\alpha) \neq 0$. Now given any $f(x) = \frac{a(x)}{b(x)} \in F(x)$ with $a(x)$ and $b(x) \in F[x]$, set $f(\alpha) = a(\alpha)/b(\alpha)$. This is well-defined, as if $f = a'(x)/b'(x)$, then $a(x)b'(x) = a'(x)b(x)$ in $F[x]$, hence $a(\alpha)b'(\alpha) = a'(\alpha)b(\alpha)$ and $a'(\alpha)/b'(\alpha) = a'(\alpha)/b'(\alpha)$. Now let $\tilde{ev}_\alpha : F(x) \to K$ be the map given by $\tilde{ev}_\alpha(f(x)) = f(\alpha)$ (where $f(x) \in F(x)$). We leave it to the reader to check that $\tilde{ev}_\alpha$ is a ring map. It is injective since $F(\alpha)$ is a field. Moreover, by our observation at the start, its image is the subfield $F(\alpha)$ of K. Thus it gives an isomorphism $F(x) \to F(\alpha)$.

REMARK. (1) The fact that α is transcendental is crucial in the construction above: if α is algebraic over F with $b(x) \in F[x]$ a nonzero polynomial such that $b(\alpha) = 0$, then our $\tilde{ev}_\alpha$ does not make sense at $1/b(x)$.

(2) The evaluation map above extends the usual evaluation map $ev_\alpha : F[x] \to K$ (meaning that $\tilde{ev}_\alpha = ev_\alpha$ on $F[x] \subset F(x)$). You can prove (with a construction similar to how $\tilde{ev}_\alpha$ was defined above from ev_α) that in general, given any domain R, the fraction field $Frac(R)$ has the following property: given any *field* L and *injective* ring map $\phi : R \to L$, the map ϕ extends uniquely to a ring map $\tilde{\phi} : Frac(R) \to L$.

5. (a) This is because $\sqrt{2} = \sqrt[10]{2}^5 \in \mathbb{Q}(\sqrt[10]{2})$. (Note: If the notation $\sqrt[10]{2}$ means any 10th root of 2 (and not necessarily the positive real one), then $\sqrt{2} = \pm \sqrt[10]{2}^5$ and still is in $\mathbb{Q}(\sqrt[10]{2})$.)

(b) We have a diagram of fields

$$\begin{array}{c} \mathbb{Q}(\sqrt[10]{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

The number $\sqrt[10]{2}$ (resp. $\sqrt{2}$) is root of $x^{10}-2$ (resp. x^2-2), which is irreducible over $\mathbb{Q}$ by Eisenstein criterion. Thus $[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}] = 10$ (which is the degree of $x^{10}-2$) and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. By the degree formula,

$$[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})] = \frac{[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]} = 5.$$

(c) Since $[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})] = 5$, the minimal polynomial of $\sqrt[10]{2}$ over $\mathbb{Q}(\sqrt{2})$ has degree 5. Now we observe that $\sqrt[10]{2}$ is a root of $x^5 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$. It follows that $x^5 - \sqrt{2}$ is the minimal polynomial of $\sqrt[10]{2}$ over $\mathbb{Q}(\sqrt{2})$ (as this minimal polynomial divides $x^5-\sqrt{2}$ and has the same degree as $x^5-\sqrt{2}$). Thus $x^5-\sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$.

6. (a) Let $\alpha = \sqrt{5+2\sqrt{2}}$. Then $\alpha^2 = 5+2\sqrt{2}$, so that $\sqrt{2} \in \mathbb{Q}(\alpha)$. We have a diagram of fields

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

Since α is a root of $x^2 - (5+2\sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$, the degree of $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})]$ is 1 or 2 (why?). This degree is 1 if and only if $\alpha \in \mathbb{Q}(\sqrt{2})$ (why?). Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, the set $\{1, \sqrt{2}\}$ forms a basis for $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$. Suppose $\alpha \in \mathbb{Q}(\sqrt{2})$. Then there are unique $a, b \in \mathbb{Q}$ such that $\alpha = a+b\sqrt{2}$.

Then
$$\alpha^2 = a^2 + 2b^2 + 2ab\sqrt{2}.$$
On the other hand, $\alpha^2 = 5 + 2\sqrt{2}$. It follows that
$$a^2 + 2b^2 = 5$$
and
$$2ab = 2$$
(why?). From the latter equation, $b = 1/a$. Substituting in the former, we get
$$a^4 - 5a^2 + 2 = 0.$$
Thus
$$a^2 = \frac{10 \pm \sqrt{17}}{2}.$$
But this is absurd, as a^2 is rational whereas the right hand side is not (because $\sqrt{17}$ is not rational). This shows that $\alpha \notin \mathbb{Q}(\sqrt{2})$, hence $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = 2$. Combining with $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ the degree formula gives $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

REMARK. Here are some ways to see that $\sqrt{17}$ is not rational:
(1) by Eisenstein critertion, the polynomial $x^2 - 17$ is irreducible over $\mathbb{Q}$. Hence it has no roots in $\mathbb{Q}$.
(2) $x^2 - 17$ is monic with coefficients in $\mathbb{Z}$. By Exercise 63, every rational root of it is an integer. On the other hand $x^2 - 17$ clearly has no roots in $\mathbb{Z}$. (By the same result, for any integer N, if $\sqrt{N}$ is rational, then it is in fact an integer.)

(b) Note that
$$(1 + \sqrt{2})^2 = 3 + 2\sqrt{2},$$
thus $\sqrt{3 + 2\sqrt{2}} = \pm(1 + \sqrt{2}) \in \mathbb{Q}(\sqrt{2})$ and
$$[\mathbb{Q}(\sqrt{3 + 2\sqrt{2}}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$