Problem Set 12 solutions

Problem 1. Prove that if F is a field, then any finite subgroup G of $(F^{\times}, \cdot)$ is cyclic.
Hint: Use the classification of Finitely Generated Modules over PIDs to find a polynomial of the form $p = x^n - 1 \in F[x]$ such that every element of G is a root for p. Compare the number of roots of p to $\deg(p)$.

Proof. By the Classification of Finitely Generated Modules over PIDs, since abelian groups are $\mathbb{Z}$-modules and $\mathbb{Z}$ is a PID, there is a group isomorphism

$$G \cong \mathbb{Z}^t \times Z/d_1 \times \cdots \times \mathbb{Z}/d_s$$

for unique $r \geqslant 0$, $1 < d_1 \mid d_2 \mid \cdots \mid d_s$. Since $\mathbb{Z}^r$ is infinite whenever $r > 0$, but G is finite, we have $r = 0$. From Problem Set 5, we also have that

$$\operatorname{ann}(G) = \operatorname{ann}(\mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_s) = (d_s).$$

This means that $d_s x = 0$ for any $x \in \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_s$, or in multiplicative notation $x^{d_s} = 1_G$ for any $x \in (G, \cdot)$. This can be written as

$$x^{d_s} - 1 = 0 \quad \text{for all } x \in G \subseteq F,$$

which means that the polynomial $x^{d_s} - 1 \in F[x]$ has $|G| = d_1 \cdots d_s$ roots in F. Since a polynomial has at most as many roots as its degree, we conclude that $d_1 \cdots d_s \leqslant d_s$, but since $d_i > 1$ for all $1 \leqslant i \leqslant s$, the previous inequality can only hold if $s = 1$. Therefore, $G \cong \mathbb{Z}/d_1$ is cyclic. □

Problem 2. Let p be a prime number and let L be the splitting field of $x^p - 2$ over $\mathbb{Q}$. In Problem Set 10, you showed that $L = \mathbb{Q}(b, \zeta)$ for $b = \sqrt[p]{2}$ and $\zeta = e^{2\pi i/p}$, and $[L : \mathbb{Q}] = p(p-1)$.

a) Determine all the elements of $\operatorname{Aut}(L/\mathbb{Q})$, assuming that $|\operatorname{Aut}(L/\mathbb{Q})| = [L : \mathbb{Q}]$.

Hint: we will prove shortly that indeed $|\operatorname{Aut}(L/\mathbb{Q})| = [L : \mathbb{Q}]$ since $\operatorname{char}(\mathbb{Q}) = 0$ and L is the splitting field of an irreducible polynomial over $\mathbb{Q}$.

Proof. We showed in problem set 10 that $[L : \mathbb{Q}(b)] = p - 1$, and ζ is a root of $x^{p-1} + \cdots + x + 1$. Therefore, the minimum polynomial of ζ over $\mathbb{Q}(b)$ must be

$$m_{\zeta, \mathbb{Q}(b)} = x^{p-1} + \cdots + x + 1.$$

Then $1, \zeta, \ldots, \zeta^{p-2}$ is a basis for L as a $\mathbb{Q}(b)$-vector space. Combining this with the basis for $\mathbb{Q}(b)/\mathbb{Q}$ above shows as in the proof of the Degree Formula that

$$B := \{b^m \zeta^j \mid 0 \leqslant m \leqslant p-1, 0 \leqslant j \leqslant p-2\}$$

is a basis for L as a vector space over $\mathbb{Q}$.

Let σ be any element of $G = \operatorname{Aut}(K/\mathbb{Q})$. Then by a theorem from class, $\sigma(b)$ must be another root of $x^p - 2$, so $\sigma(b) = b\zeta^{r_\sigma}$ for some $0 \leqslant r_\sigma \leqslant p - 1$. Likewise, σ maps the root ζ of the polynomial $\Phi_p(x) = x^{p-1} + \cdots + 1 \in \mathbb{Q}[x]$ to another root $\sigma(\zeta) = \zeta^{s_\sigma}$ of Φ_p for some $1 \leqslant s_\sigma \leqslant p - 1$. Hence for each element $b^m\zeta^j$ of the basis B above, we have

$$\sigma(b^m\zeta^j) = \sigma(b)^m \sigma(\zeta)^j = (b\zeta^{r_\sigma})^m (\zeta^{s_\sigma})^j = b^m \zeta^{mr_\sigma + js_\sigma}.$$

Since σ fixes $\mathbb{Q}$, then σ is a $\mathbb{Q}$-linear transformation, so the numbers $r_\sigma \in \{0, ..., p-1\}$ and $s_\sigma \in \{1, ..., p-1\}$ completely determine the automorphism σ of K.

Moreover, if $\sigma, \tau \in \operatorname{Aut}(K/\mathbb{Q})$ satisfy $r_\sigma = r_\tau$ and $s_\sigma = s_\tau$, then σ and τ fix both $\mathbb{Q}$ and have the same action on the basis B of $K/\mathbb{Q}$, so $\sigma = \tau$. Hence, there are at most $p(p-1)$ automorphisms of K/Q, each one associated to a pair of numbers $0 \leqslant r \leqslant p-1$ and $1 \leqslant s \leqslant p-1$.

Note that $x^p - 2$ is a polynomial of degree p with p distinct roots, so it is separable. Thus K is the splitting field of a separable polynomial over $\mathbb{Q}$, and thus $\mathbb{Q} \subseteq K$ is Galois. Therefore,

$$|G| = |\operatorname{Aut}(K/\mathbb{Q})| = [K : \mathbb{Q}] = p(p-1).$$

Hence for each $0 \leqslant r \leqslant p-1$ and $1 \leqslant s \leqslant p-1$ there is an automorphism $\tau_{r,s} : K \to K$ that fixes $\mathbb{Q}$ and satisfies

$$\tau_{r,s}(b^m \zeta^j) = b^m \zeta^{mr+js} \quad \text{for all} \quad b^m \zeta^j \in B.$$

Therefore,

$$\operatorname{Aut}(K/\mathbb{Q}) = \{\tau_{r,s} \mid 0 \leqslant r \leqslant p-1, 1 \leqslant s \leqslant p-1\}. \quad \square$$

b) Decide, with justification, whether $G = \operatorname{Aut}(L/\mathbb{Q})$ is abelian.

Proof. First, we have

$$\begin{aligned} \tau_{r,s} \circ \tau_{r',s'}(b^m \zeta^j) &= \tau_{r,s}(b^m \zeta^{mr'+js'}) \\ &= b^m \zeta^{mr+(mr'+js')s} \\ &= b^m \zeta^{mr+mr's+js's} \end{aligned}$$

and thus, interchanging the roles of r, s and r', s' we have

$$\tau_{r,s} \circ \tau_{r',s'}(b^m \zeta^j) = b^m \zeta^{mr'+mrs'+js's}.$$

This shows that

$$\begin{aligned} \tau_{r,s} \circ \tau_{r',s'} = \tau_{r,'s'} \circ \tau_{r,s} &\iff mr + mr's + js's \equiv mr' + mrs' + js's \pmod{p} \text{ for all } m, j \\ &\iff m(r - r' + r's - rs') \equiv 0 \pmod{p} \text{ for all } 0 \leqslant m \leqslant p-1 \\ &\iff r - r' + r's - rs' \equiv 0 \pmod{p}. \end{aligned}$$

If $p = 2$ then $s = s' = 1$ and the above shows that G is abelian. In fact, note that when $p = 2$ then $|\operatorname{Gal}(K/\mathbb{Q})| = 2$, and since there is only one group of order 2, we conclude that $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2$ is abelian.

However, if $p > 2$, then taking for example $r = 0$, $r' = 1$, and $s = 2$ shows that that

$$\tau_{0,2} \circ \tau_{1,s'} \neq \tau_{1,s'} \circ \tau_{0,2},$$

since

$$1 \not\equiv 0 \pmod{p}.$$

Thus G is not abelian for $p > 2$. $\square$

Problem 3. Let L be the splitting field of $x^6 - 4$ over $\mathbb{Q}$. Let $\alpha = \sqrt[3]{2}$ be the unique positive real root of $x^6 - 4$, and $\zeta = e^{2\pi i/6}$. You showed in Problem Set 10 that $K = \mathbb{Q}(\alpha, \zeta)$ and $[K : \mathbb{Q}] = 6$.

a) Give, with justification, an explicit basis of K as a vector space over $\mathbb{Q}$.

Proof. From Problem Set 10, we have $K = \mathbb{Q}(\alpha, \zeta)$ and:

- $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $m_{b,\mathbb{Q}} = x^3 - 2$, thus a basis for $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space is given by $A = \{1, \alpha, \alpha^2\}$.
- $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(b)] = 2$ and $m_{\zeta,\mathbb{Q}(\alpha)} = x^2 - x + 1$, thus a basis for $\mathbb{Q}(\alpha, \zeta)$ as a $\mathbb{Q}(\alpha)$-vector space is given by $B = \{1, \zeta\}$.

By the proof of the degree formula, a basis for K as a $\mathbb{Q}$-vector space is

$$AB = \{1, \alpha, \alpha^2, \zeta, \alpha\zeta, \alpha^2\zeta\}. \quad \square$$

Alternative proof. Alternatively, we can first show that $K = \mathbb{Q}(\alpha, \zeta_3)$, where $\zeta_3 = e^{2\pi i/3}$, and following the same argument as above we can then prove that

$$\{1, \alpha, \alpha^2, \zeta_3, \alpha\zeta_3, \alpha^2\zeta_3\}$$

is a basis for K over $\mathbb{Q}$. $\square$

b) Let $g \in \operatorname{Aut}(K/\mathbb{Q})$ be an automorphism that maps $g(\alpha) = \alpha\zeta^2$ and $g(\alpha\zeta^2) = \alpha$. Determine all the possibilities for g by describing where g maps each element of your basis for K and checking that the resulting $\mathbb{Q}$-linear transformation g is also a field automorphism.

Proof. First, note that $\zeta^3 = -1$, which will we use a few times below. Moreover, we showed in Problem Set 10 that ζ satisfies $x^2 - x + 1$, so

$$\zeta^2 = \zeta - 1 \iff \zeta = \zeta^2 + 1.$$

Using the multiplicative property of g, we have

$$g(\zeta^2) = \frac{g(\alpha\zeta^2)}{g(\alpha)} = \frac{\alpha}{\alpha\zeta^2} = \zeta^{-2} = \zeta^4 = -\zeta.$$

Thus

$$g(\zeta) = g(\zeta^2 + 1) = 1 + g(\zeta^2) = 1 - \zeta.$$

Moreover,

$$g(\alpha^2) = g(\alpha)^2 = (\alpha\zeta^2)^2 = \alpha^2\zeta^4 = -\alpha^2\zeta.$$

It will be convenient to rewrite all the images in terms of our chosen basis; note that

$$g(\alpha) = \alpha\zeta^2 = \alpha(\zeta - 1) = \alpha\zeta - \alpha.$$

Finally,

$$g(\alpha\zeta) = g(\alpha)g(\zeta) = (\alpha\zeta^2)(1 - \zeta) = \alpha\zeta^2 - \alpha\zeta^3 = \alpha(\zeta - 1) + \alpha = \alpha\zeta$$

and

$$g(\alpha^2\zeta) = (-\alpha^2\zeta)(1 - \zeta) = \alpha^2\zeta^2 - \alpha^2\zeta = \alpha^2(\zeta - 1) - \alpha^2\zeta = -\alpha^2.$$

Summarizing, on the basis AB for K given above, g acts as follows:

x	1	α	α^2	ζ	$\alpha\zeta$	$\alpha^2\zeta$
$g(x)$	1	$\alpha\zeta-\alpha$	$-\alpha^2\zeta$	$1-\zeta$	$\alpha\zeta$	$-\alpha^2$

By the UMP of the $\mathbb{Q}$-vector space K, there is a unique linear transformation of K that acts on the basis AB as shown above. To check that this unique g is also multiplicative, hence an automorphism, it is sufficient check that g is multiplicative when restricted to just the basis elements in AB, since g is defined on a general element by extending it linearly from the basis elements. I will skip that check here, but this would be sufficient to show that the $\mathbb{Q}$-linear map g we described in the map above is a ring homomorphism $K \to K$.

Finally, we have to show that g is an isomorphism, and for that it is sufficient to show that its image has dimension 6 as a $\mathbb{Q}$-vector space. And indeed,

$$\operatorname{span}\{\alpha\zeta-\alpha,\alpha\zeta\}=\operatorname{span}\{\alpha\zeta,\alpha\} \quad \text{and} \quad \operatorname{span}\{1,1-\zeta\}=\operatorname{span}\{1,\zeta\},$$

so

$$\operatorname{im} g=\operatorname{span}\{1,\alpha\zeta-\alpha,-\alpha^2\zeta,1-\zeta,\alpha\zeta,-\alpha^2\} \ =\operatorname{span}\{1,\alpha,\alpha\zeta,\alpha^2\zeta,\zeta,\alpha\zeta,\alpha^2\}=K. \qquad \square$$

Alternative Proof. Alternatively, one can show that $K=\mathbb{Q}(\alpha,\zeta_3)$, where $\zeta_3=e^{\frac{2\pi i}{3}}$, and use this to give the following alternative basis for K over $\mathbb{Q}$:

$$\{1,\alpha,\alpha^2,\zeta_3,\alpha\zeta_3,\alpha^2\zeta_3\}.$$

Under this basis, similar calculations as the ones above give us the following:

x	1	α	α^2	ζ_3	$\alpha\zeta_3$	$\alpha^2\zeta_3$
$g(x)$	1	$\alpha\zeta_3$	$\alpha^2\zeta_3^2$	ζ_3^2	α	$\alpha^2\zeta_3$

To rewrite this in our chosen basis, it helps to note that ζ_3 is a root of $x^3-1=(x-1)(x^2+x+1)$, and thus of x^2+x+1, so

$$\zeta_3^2=-\zeta_3-1.$$

Thus

x	1	α	α^2	ζ_3	$\alpha\zeta_3$	$\alpha^2\zeta_3$
$g(x)$	1	$\alpha\zeta_3$	$-\alpha^2\zeta_3-\alpha^2$	$-\zeta_3-1$	α	$\alpha^2\zeta_3$

The remaining details are similar to what we described in the other situation. $\square$

c) Let $h \in \operatorname{Aut}(K/\mathbb{Q})$ be the restriction of the complex conjugation map to K. Determine the subfield $K^{\langle h\rangle} := \{k \in K \mid h(k)=k\}$ explicitly.

Proof. We will use without proof that h is indeed an element of $\operatorname{Aut}(K/\mathbb{Q})$.

Notice that the complex numbers fixed by conjugation are precisely the reals, therefore $K^{\langle h\rangle}=K\cap\mathbb{R}$. Since $\alpha\in\mathbb{R}$, we have $\alpha\in K^{\langle h\rangle}$ and in fact $\mathbb{Q}(\alpha)\subseteq K^{\langle h\rangle}$ by minimality of the field generated by α. Notice that $\zeta\notin\mathbb{R}$ so $K\neq K^{\langle h\rangle}$ and thus $[K:K^{\langle h\rangle}]\geqslant 2$. By the degree formula we have

$$2=[K:\mathbb{Q}(\alpha)]=[K:K^{\langle h\rangle}][K^{\langle h\rangle}:\mathbb{Q}(\alpha)]\geqslant 2[K^{\langle h\rangle}:\mathbb{Q}(\alpha)].$$

This is only possible if $[K^{\langle h\rangle}:\mathbb{Q}(\alpha)]=1$ and so we conclude that $K^{\langle h\rangle}=\mathbb{Q}(\alpha)$.

Alternatively, we can show that $K^{\langle h\rangle} = \mathbb{Q}(\alpha)$ using the Fundamental Theorem of Galois Theory. First, we note that $\mathbb{Q} \subseteq K$ is Galois since K is the splitting field of the separable polynomial $x^6 - 4$. Moreover, $h^2 = 2$, $|\langle h\rangle| = 2$, so

$$[\mathrm{Gal}(K/\mathbb{Q}) : \langle h\rangle] = \frac{|\mathrm{Gal}(K/\mathbb{Q})|}{|\langle h\rangle|} = \frac{6}{2} = 3.$$

By the Fundamental Theorem of Galois Theory, the fixed field $L^{\langle h\rangle|}$ has degree 3 over $\mathbb{Q}$. Since $\mathbb{Q}(\alpha) \subseteq L^{\langle h\rangle|}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, we conclude that $L^{\langle h\rangle|} = \mathbb{Q}(\alpha)$. □

Problem 4. Let F be a perfect field. Prove that if L is the splitting field over F of a (not necessarily separable) polynomial in $f \in F[x]$, then $F \subseteq L$ is a Galois extension.

Proof. Let L be the splitting field over F of a polynomial $q \in F[x]$. Since $F[x]$ is a UFD, we can write

$$q = cp_1 \cdots p_m$$

such that each $p_i \in F[x]$ is irreducible and monic and $c \in F$.

Let b be any root of q. Then there exists an index i such that b is a root of p_i. Since $p_i \in F[x]$ is a monic irreducible polynomial with root b, then $p_i = m_{b,F}$. Conversely for any p_i there is a root b of q (in fact any root of p_i will do) such that $p_i = m_{b,F}$. If $p_i \neq p_j$ then p_i and p_j have no common roots, since the existence of a common root b would imply $p_i = m_{b,F} = p_j$.

Let $t_1, \ldots, t_r$ be the *distinct* monic irreducible factors of q. The p_i are all separable, since they are irreducible over F and F is perfect. Then $f = \prod_{i=1}^r t_i$ is also a separable polynomial, since the roots of distinct p_i are also all distinct. Furthermore, f has the same roots as q, say $b_1, \ldots, b_n$, so the splitting fields of f and q are both $F(b_1, \ldots, b_n)$. Therefore, L is the splitting field of the separable polynomial f over F.

We showed in class that if L is the splitting field of a separable polynomial, then $F \subseteq L$ is Galois. Therefore, $F \subseteq L$ is Galois. □

Problem 5. Assume $F \subseteq L$ is a finite extension of fields and that the characteristic of F is p, where p is a prime. Suppose there exists an element $a \in L$ such that $a \notin F$ but $a^p \in F$.

a) Prove $\sigma(a) = a$ for all $\sigma \in \mathrm{Aut}(L/F)$.

Proof. Let $a^p = b \in F$. Since a is a root of the polynomial $x^p - b$, all of whose coefficients are in F, we know $\sigma(a)$ must also be root of this polynomial. But, by the Freshman's Dream, $x^p - b$ factors as $(x-a)^b$ in $\overline{F}[x]$, and so this polynomial has just one root, which is a. So $\sigma(a) = a$. □

b) Prove that $F \subseteq L$ is not Galois.

Proof. By part (a), every element of $\mathrm{Aut}(L/F)$ fixes a and thus also fixes $F(a)$. That is, $\mathrm{Aut}(L/F) = \mathrm{Aut}(L/F(a))$. Since $F \neq F(a)$, $[L : F(a)] < [L : F]$. Then

$$|\mathrm{Aut}(L/F)| = |\mathrm{Aut}(L/F(a))| \leqslant [L : F(a)] < [L : F].$$

In particular, $|\mathrm{Aut}(L/F)| < [L : F]$, so the extension is not Galois. □

Problem 6. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic (degree 3) polynomial having exactly one real root. Let L be the splitting field of f over $\mathbb{Q}$. Show that $\mathrm{Aut}(L/\mathbb{Q}) \cong S_3$.

We give two alternative proofs.

Proof 1. Let a be the real root of f, and let b, c be the other two roots. Note that b and c are complex conjugates. In particular, a, b, and c are all distinct. Thus f is separable, and thus $\mathbb{Q} \subseteq L$ is Galois, so $|\operatorname{Aut}(L/\mathbb{Q})| = [L : \mathbb{Q}]$.

Since f has three distinct roots, $\operatorname{Gal}(L/\mathbb{Q})$ is a subgroup of S_3, and thus $|\operatorname{Gal}(L/\mathbb{Q})| \leqslant |S_3| = 6$. Since f is irreducible, it is the minimal polynomial of a, b, and c. In particular, $[L : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] = 3$. Applying the Degree Formula to $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq L$, we conclude that $3|[L : \mathbb{Q}]$. Moreover, $b, c \notin \mathbb{R}$, so $b, c \notin \mathbb{Q}(a)$. In particular, $[L : \mathbb{Q}(a)] \geqslant 2$. Thus by the Degree Formula we have $[L : \mathbb{Q}] \geqslant 2 \cdot 3 = 6$, and we conclude that $[L : \mathbb{Q}] = 6$. The only subgroup of S_3 of order 6 is S_3, so $\operatorname{Aut}(L/\mathbb{Q}) \cong S_3$. $\square$

Proof 2. Let a be the real root of f, and let b, c be the other two roots. Note that b and c are complex conjugates. Since f has three distinct roots, $\operatorname{Gal}(L/\mathbb{Q})$ is a subgroup of S_3. The complex conjugation map σ satisfies $\sigma|_{\mathbb{Q}} = \mathrm{id}_Q$, $\sigma(a) = a$, $\sigma(b) = c$, and $\sigma(c) = b$, so $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$. Identifying a with 1, b with 2, and c with 3, σ corresponds to $(2\,3) \in \S_3$.

Since L is the splitting field of the irreducible polynomial f, we know that $\operatorname{Gal}(L/\mathbb{Q})$ acts transitively on the roots of f. In particular, there exists an element $\tau \in \operatorname{Gal}(L/\mathbb{Q})$ such that $\tau(a) = b$. Such τ must send roots of f to roots of f, so we must have $\tau(b) = c$ or $\tau(b) = a$. If $\tau(b) = c$, then $\tau(c) = a$, and τ would correspond to $(1\,2\,3) \in S_3$. If $\tau(b) = a$, then $\tau(c) = c$, and τ would correspond to $(1\,2) \in S_3$. Since

$$\langle (2\,3), (1\,2\,3) \rangle = S_3 \quad \text{and} \quad \langle (2\,3), (1\,2) \rangle = S_3,$$

in either case we have $\operatorname{Gal}(L/\mathbb{Q}) \cong S_3$. $\square$