Abstract Algebra Homework 9

Michael Nelson

Problem 1

Let $f(X) = X^5 - 3$ and let $g(X) = X^4 + X^3 + X^2 + X + 1$. Also let α be a complex root of f and let β be a complex root of g. Observe that f is irreducible over $\mathbb{Q}$ since it is Eisenstein at 3 and g is irreducible over $\mathbb{Q}$ since

$$\begin{aligned} g(X+5) &= (X+1)^4 + (X+1)^3 + (X+1)^2 + (X+1) + 1 \\ &= X^4 + 5X^3 + 10X^2 + 10X + 5 \end{aligned}$$

is Eisenstein at 5 (also g is the 5th cyclotomic polynomial).

Let $\zeta_5 = e^{2\pi i/5}$. We can factor f over $\mathbb{C}$ as

$$f(X) = (X - \sqrt[5]{3})(X - \zeta_5 \sqrt[5]{3})(X - \zeta_5^2 \sqrt[5]{3})(X - \zeta_5^3 \sqrt[5]{3})(X - \zeta_5^4 \sqrt[5]{3}). \tag{1}$$

Indeed, $\zeta_5^b \sqrt[5]{3}$ is a root of f for all $b \in \mathbb{Z}/5\mathbb{Z}$ (you'll see in a second why I'm writing $b \in \mathbb{Z}/5\mathbb{Z}$ and not simply just $0 \leq b \leq 4$). Since these five roots are distinct from each other and since $\deg f = 5$, they must exhaust all the roots of f. In particular, $\alpha = \zeta_5^b \sqrt[5]{3}$ for some $b \in \mathbb{Z}/5\mathbb{Z}$. Similarly, we can factor g over $\mathbb{C}$ as

$$g(X) = (X - \zeta_5)(X - \zeta_5^2)(X - \zeta_5^3)(X - \zeta_5^4). \tag{2}$$

Indeed, ζ_5^a is a root of g for all $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ (again, you'll see in a second why I'm writing $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ and not simply just $1 \leq a \leq 4$). Since these four roots are distinct from each other and since $\deg g = 4$, they must exhaust all the roots of g (alternatively, one can see this from the fact that g is the 5th cyclotomic polynomial). In particular, $\beta = \zeta_5^a$ for some $a \in (\mathbb{Z}/5\mathbb{Z})^\times$.

Problem 1.a

Exercise 1. Find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and show that this extension is not Galois.

Solution 1. As shown above, f is irreducible over $\mathbb{Q}$ with $\deg f = 5$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. To see why $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois, it suffices to show that $\mathbb{Q}(\sqrt[5]{3})/\mathbb{Q}$ is not Galois (since there is a $\mathbb{Q}$-isomorphism taking $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\sqrt[5]{3})$). A $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[5]{3})$ must send $\sqrt[5]{3}$ to $\zeta_5^b \sqrt[5]{3}$ for some $b \in \mathbb{Z}/5\mathbb{Z}$, but $\zeta_5^b \sqrt[5]{3}$ is not a real number if $b \neq 0$, so it can't belong to $\mathbb{Q}(\sqrt[5]{3})$, so the only possibility is $\sqrt[5]{3} \mapsto \sqrt[5]{3}$. Thus $\mathrm{Aut}(\mathbb{Q}(\sqrt[5]{3})/\mathbb{Q})$ is trivial. Thus $\mathbb{Q}(\sqrt[5]{3})/\mathbb{Q}$ is not Galois, which implies $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois.

Problem 1.b

Exercise 2. Show that g is irreducible over $\mathbb{Q}(\alpha)$.

Solution 2. We showed above that g is irreducible over $\mathbb{Q}$, but now we want to show it is irreducible over $\mathbb{Q}(\alpha)$. Since f and g are monic irreducible polynomials over $\mathbb{Q}$ which kill α and β respectively, we see that f is the minimal polynomial for α and g is the minimal polynomial for β. Since $\deg f = 5$ and $\deg g = 4$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Since $\gcd(4,5) = 1$, it follows that $[\mathbb{Q}(\alpha, \beta) \colon \mathbb{Q}] = 4 \cdot 5 = 20$ (by a previous HW problem). This also implies g is the minimal polynomial for β over $\mathbb{Q}(\alpha)$. Indeed, if $h(X)$ is an irreducible monic polynomial with coefficients in $\mathbb{Q}(\alpha)$ which kills β, then $20 = 4 \cdot \deg h$, which implies $\deg h = 5$, but g is also a monic polynomial with coefficients in $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ which kills β, thus $h \mid g$. Since $\deg h = \deg g$ and both g and h are monic, we must have $g = h$. Thus g is the minimal polynomial for β over $\mathbb{Q}(\alpha)$. In particular, it is irreducible over $\mathbb{Q}(\alpha)$.

Problem 1.c

Exercise 3. Let $\overline{F}$ be the field obtained by adjoining all of the roots of f to $\mathbb{Q}$. Find the Galois group $\mathrm{Gal}(\overline{F}/\mathbb{Q})$.

Solution 3. From the polynomial factorization (1), we see that $\overline{F} = \mathbb{Q}(\zeta_5, \sqrt[5]{3})$. Indeed, since $\zeta_5 = \zeta_5\sqrt[5]{3}/\sqrt[5]{3}$, we have $\zeta_5 \in \overline{F}$, and hence $\mathbb{Q}(\zeta_5, \sqrt[5]{3}) \subseteq \overline{F}$. Conversely, $\zeta_5^b\sqrt[5]{3}$ is clearly in $\mathbb{Q}(\zeta_5, \sqrt[5]{3})$ for all $b \in \mathbb{Z}/5\mathbb{Z}$. Thus $\mathbb{Q}(\zeta_5, \sqrt[5]{3}) \supseteq \overline{F}$.

Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_5, \sqrt[5]{3})$ is completely determined by where it sends ζ_5 and where it sends $\sqrt[5]{3}$. There are 4 places to send ζ_5, namely ζ_5, ζ_5^2, ζ_5^3, and ζ_5^4. Similarly, there are 5 places to send $\sqrt[5]{3}$, namely $\sqrt[5]{3}$, $\zeta_5\sqrt[5]{3}$, $\zeta_5^2\sqrt[5]{3}$, $\zeta_5^3\sqrt[5]{3}$, and $\zeta_5^4\sqrt[5]{3}$. In total, there are $4 \cdot 5 = 20$ possible automorphisms. In fact all such possibilities are realized since $[\mathbb{Q}(\zeta_5, \alpha) : \mathbb{Q}] = 20$. Let us describe them now:

For $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ and $b \in \mathbb{Z}/5\mathbb{Z}$, let $\sigma_{a,b}\colon \mathbb{Q}(\zeta_5, \sqrt[5]{3}) \to \mathbb{Q}(\zeta_5, \sqrt[5]{3})$ be the $\mathbb{Q}$-automorphism which sends ζ_5 to ζ_5^a and $\sqrt[5]{3}$ to $\zeta_5^b\sqrt[5]{3}$ (any $\mathbb{Q}$-automorphism has a unique expression of this form). By a direct calculation, we have

$$\sigma_{a,b}\sigma_{a',b'} = \sigma_{aa',ab'+b} \tag{3}$$

for all $a, a' \in (\mathbb{Z}/5\mathbb{Z})^\times$ and $b, b' \in \mathbb{Z}/5\mathbb{Z}$, where multiplication and addition in the subscripts are taken modulo 5. The multiplcation rule (3) behaves just like matrix multiplication:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix}.$$

So we have an isomorphism from

$$\mathrm{Aff}(\mathbb{Z}/5\mathbb{Z}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/5\mathbb{Z})^\times,\ b \in \mathbb{Z}/5\mathbb{Z} \right\}$$

to $\mathrm{Gal}(\mathbb{Q}(\zeta_5, \sqrt[5]{3})/\mathbb{Q})$ given by $\sigma_{a,b} \mapsto \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$.

Problem 1.d

Exercise 4. Find an explicit formula for the roots of $f(X)$.

Solution 4. This was done above.

Problem 2

Let F be the field obtained by adjoining all roots of the polynomial $f(X) = X^6 - 3X^3 + 1$. From the quadratic formula, we can factor f as

$$f(X) = \left(X^3 - \left(\frac{3-\sqrt{5}}{2}\right)\right)\left(X^3 - \left(\frac{3+\sqrt{5}}{2}\right)\right). \tag{4}$$

Let $\zeta_3 = e^{2\pi i/3}$, $\alpha = \sqrt[3]{\frac{3-\sqrt{5}}{2}}$, and $\beta = \sqrt[3]{\frac{3+\sqrt{5}}{2}}$ (by cubed root here we mean the real cube root). Then we can factor (4) even further as

$$f(X) = (X-\alpha)(X-\zeta_3\alpha)(X-\zeta_3^2\alpha)(X-\beta)(X-\zeta_3\beta)(X-\zeta_3^2\beta). \tag{5}$$

In particular, $F = \mathbb{Q}(\zeta_3, \alpha)$. To see this, note that $\zeta_3 \in F$ since $\zeta_3 = \zeta_3\alpha/\alpha$, so $F \supseteq \mathbb{Q}(\zeta_3, \alpha)$. Conversely, observe that

$$\begin{aligned}(\alpha\beta)^3 &= \left(\frac{3-\sqrt{5}}{2}\right)\left(\frac{3+\sqrt{5}}{2}\right) \\ &= \frac{9-5}{4} \\ &= 1\end{aligned}$$

implies $(\alpha\beta)^3 = 1$. Since both α and β are *real* numbers, we must have $\alpha\beta = 1$. Thus $\beta = \alpha^{-1}$, which implies $\beta \in \mathbb{Q}(\zeta_3, \alpha)$. Clearly now, all the other roots of f are in $\mathbb{Q}(\zeta_3, \alpha)$ as well. Thus we may rewrite (5) as

$$f(X) = (X-\alpha)(X-\zeta_3\alpha)(X-\zeta_3^2\alpha)(X-\alpha^{-1})(X-\zeta_3\alpha^{-1})(X-\zeta_3^2\alpha^{-1}). \tag{6}$$

Problem 2.a

Exercise 5. Show that complex conjugation is a nontrivial automorphism of F.

Solution 5. Note that complex conjugation is an automorphism of F which fixes $\mathbb{Q}$ since it is an automorphism of $\mathbb{C}$ which fixes $\mathbb{Q}$ and $F/\mathbb{Q}$ is Galois. That complex conjugation is nontrivial follows from the fact that F contains a nonreal complex number, namely ζ_3. So complex conjugation will send ζ_3 to $\overline{\zeta_3}$, and $\zeta_3 \neq \overline{\zeta_3}$.

Problem 2.b

Exercise 6. If γ is a real root of this polynomial, show that the map induced by $\gamma \mapsto \gamma^{-1}$ gives rise to an automorphism of $\mathbb{Q}(\gamma)$.

Solution 6. From the polynomial factorization (6), we see that the real roots of f are given by α and α^{-1}. Without loss of generality, assume $\gamma = \alpha$. Then $\alpha \mapsto \alpha^{-1}$ induces the automorphism $\varphi\colon \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha^{-1}] = \mathbb{Q}[\alpha]$ given by

$$\varphi(\pi(\alpha)) = \pi(\alpha^{-1})$$

for all $\pi(\alpha) \in \mathbb{Q}[\alpha]$.

Problem 2.c

Exercise 7. Show that $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] = 12$.

Solution 7. Since $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$, we know from a previous HW that $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] \leq 12$. Therefore

$$\begin{aligned} 12 &\geq [\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] \\ &= [\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \\ &= [\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)] \cdot 6 \\ &\geq 12, \end{aligned}$$

where the last inequality follows from the fact that ζ_3 is a nonreal complex number and $\mathbb{Q}(\alpha)$ consists of real numbers (so $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)] \geq 2$). It follows that $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] = 12$.

Problem 2.d

Exercise 8. Find $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \alpha)/\mathbb{Q})$.

Solution 8. Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_3, \alpha)$ is completely determined by where it sends ζ_3 and where it sends α. There are 2 places to send ζ_3, namely ζ_3 and ζ_3^2. Similarly, there are 6 places to send α, namely α, $\zeta_3\alpha$, $\zeta_3^2\alpha$, α^{-1}, $\zeta_3\alpha^{-1}$ and $\zeta_3^2\alpha^{-1}$. In total, there are $2 \cdot 6 = 12$ possible automorphisms. In fact all such possibilities are realized since $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] = 12$. Let us describe them now:

For $a \in (\mathbb{Z}/3\mathbb{Z})^\times$ and $b \in \mathbb{Z}/3\mathbb{Z}$, let $\sigma_{a,b}^{\pm}\colon \mathbb{Q}(\zeta_3, \alpha) \to \mathbb{Q}(\zeta_3, \alpha)$ be the $\mathbb{Q}$-automorphism which sends ζ_3 to ζ_3^a and α to $\zeta_3^b\alpha^{\pm}$ (any such $\mathbb{Q}$-automorphism has a unique expression of this form). By a direct calculation, we have

$$\begin{aligned} \sigma_{a,b}^{+}\sigma_{a',b'}^{+} &= \sigma_{aa',b+ab'}^{+} \\ \sigma_{a,b}^{-}\sigma_{a',b'}^{+} &= \sigma_{aa',b+ab'}^{-} \\ \sigma_{a,b}^{+}\sigma_{a',b'}^{-} &= \sigma_{aa',b+ab'}^{-} \\ \sigma_{a,b}^{-}\sigma_{a',b'}^{-} &= \sigma_{aa',b+ab'}^{+} \end{aligned}$$

The multiplcation rules above behaves just like matrix multiplication (with a sign involved):

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \\ -\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} &= -\begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\left(-\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}\right) &= -\begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \\ \left(-\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\right)\left(-\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}\right) &= \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \end{aligned}$$

So we have an isomorphism from

$$\mathbb{Z}_2 \times \mathrm{Aff}(\mathbb{Z}_3) \cong \left\{ \pm \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/3\mathbb{Z})^\times,\ b \in \mathbb{Z}/3\mathbb{Z} \right\}$$

to $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \alpha)/\mathbb{Q})$ given by $\sigma_{a,b}^{\pm} \mapsto \pm \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$.

Problem 2.e

Exercise 9. Find an explicit formula for the roots of $f(X)$.

Solution 9. This was done above.

Problem 3

Let $f(X) = X^6 - X^3 + 1$ and let F be the splitting field of F over $\mathbb{Q}$. Observe that $f(-X) = X^6 + X^3 + 1$. This is just the 9th cyclotomic polynomial. Thus if we let $\zeta_9 = e^{2\pi i/9}$, then we have

$$\begin{aligned} f(-X) &= X^6 + X^3 + 1 \\ &= (X - \zeta_9)(X - \zeta_9^2)(X - \zeta_9^4)(X - \zeta_9^5)(X - \zeta_9^7)(X - \zeta_9^8). \end{aligned}$$

In other words,

$$\begin{aligned} f(X) &= (-X - \zeta_9)(X - \zeta_9^2)(-X - \zeta_9^4)(-X - \zeta_9^5)(-X - \zeta_9^7)(-X - \zeta_9^8) \\ &= (X + \zeta_9)(X + \zeta_9^2)(X + \zeta_9^4)(X + \zeta_9^5)(X + \zeta_9^7)(X + \zeta_9^8) \end{aligned}$$

In particular, $F = \mathbb{Q}(\zeta_9)$.

Problem 3.a

Exercise 10. Show that there is an intermediate field E such that $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\zeta_9)$ with $[E : \mathbb{Q}] = 2$.

Solution 10. Observe that $\zeta_3 \in \mathbb{Q}(\zeta_9)$ since $\zeta_9^2 = \zeta_3$. Thus $\mathbb{Q}(\zeta_9)$ contains $\mathbb{Q}(\zeta_3)$, which is a degree 2 extension over $\mathbb{Q}$.

Problem 3.b

Exercise 11. Find the Galois group of $(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ and list all of the intermediate fields.

Solution 11. Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_9)$ is completely determined by where it sends ζ_9. There are are 6 places to send ζ_9 (namely ζ_9^a where $a \in (\mathbb{Z}/9\mathbb{Z})^\times$). So in total, there are 6 possible automorphisms. In fact all such possibilities are realized since $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$. Let us describe them now:

For $a \in (\mathbb{Z}/9\mathbb{Z})^\times$, let $\sigma_a \colon \mathbb{Q}(\zeta_9) \to \mathbb{Q}(\zeta_9)$ be the $\mathbb{Q}$-automorphism which sends ζ_9 to ζ_9^a. By a direct calculation, we have

$$\sigma_a \sigma_{a'} = \sigma_{aa}$$

for all $a, a' \in (\mathbb{Z}/9\mathbb{Z})^\times$, where the multiplication in the subscript is taken modulo 9. Thus we have an isomorphism from $(\mathbb{Z}/9\mathbb{Z})^\times$ to $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ given by $\sigma_a \mapsto a$. Below is the lattice of subgroups of $(\mathbb{Z}/9\mathbb{Z})^\times$

$$\begin{tikzcd}
 & \{1\} \arrow[dl, dash] \arrow[dr, dash] & \\
\{1,4,7\} \arrow[dr, dash] & & \{1,8\} \arrow[dl, dash] \\
 & \{1,2,4,5,7,8\} &
\end{tikzcd}$$

These correspond to the squares in $(\mathbb{Z}/9\mathbb{Z})^\times$ and the cubes in $(\mathbb{Z}/9\mathbb{Z})^\times$ respectively. The corresponding lattice of fields is given by

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_9) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, no head] & & \mathbb{Q}(\zeta_9^{-1} + \zeta_9) \arrow[dl, no head] \\
& \mathbb{Q} &
\end{tikzcd}$$

Problem 3.c

Exercise 12. Find an explicit formula for the roots of $f(X)$.

Solution 12. This was done above.