# Problem Set 13 Solutions

**Problem 1.**

a) Show that the polynomial $x^4 + x + 1 \in \mathbb{Z}/2[x]$ is irreducible.

b) Give an explicit construction of a field with 16 elements.

*Proof.*

a) Let $f = x^2 + x^2 + 1 \in \mathbb{Z}/2[x]$. First, note that $f$ has no roots over $\mathbb{Z}/2$, since $f(1) = 1$ and $f(0) = 1$. If $f$ were reducible, it would then have to be a product of two degree 2 polynomials, say
$$f = (x^2 + ax + c)(x^2 + bx + d).$$
Then $cd = 1$, so $c = d = 1$, and
$$f = (x^2 + ax + 1)(x^2 + bx + 1).$$
Moreover, $a + b = 1$, so we without loss of generality we can assume $a = 1$ and $b = 0$, so
$$f = (x^2 + x + 1)(x^2 + 1).$$
But
$$f = (x^2 + x + 1)(x^2 + 1) = x^4 + x^2 + x^3 + x + x^2 + 1 = x^4 + x^3 + 1.$$
But that is not $f$, so we conclude that $f$ is in fact irreducible.

b) Let $L = \mathbb{Z}/2[x]/(x^4 + x + 1)$. By Problem Set 6, the elements $1 + (f), x + (f), x^2 + (f), x^3 + (f)$ form a basis for $L$ as a vector space over $\mathbb{Z}/(2)$. Since there are 2 elements in $\mathbb{Z}/(2)$, $L$ has a total of $2^4 = 16$ elements.

On the other hand, if $F$ is any field and $f \in F[x]$ is an irreducible polynomial, then $(f)$ is a maximal ideal in $F[x]$, and thus $F[x]/(f)$ is a field. In particular, $L$ is a field with 4 elements. □

**Problem 2.** Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ is a Galois extension of degree 4 with Galois group that is a cyclic group of order 4.

*Proof.* Let $\alpha = \sqrt{2+\sqrt{2}}$ and $L = \mathbb{Q}(\alpha)$. This element $\alpha$ is a root of $f = x^4 - 4x^2 + 2$, which is irreducible.[1] So $m_{\alpha,\mathbb{Q}} = f$ and Moreover, using the quadratic formula, the roots of this polynomial $f$ are
$$\pm\sqrt{2 \pm \sqrt{2}}.$$
Note that $\alpha^2 = 2 + \sqrt{2}$, and so $\sqrt{2} \in L$. Set $\beta = \sqrt{2-\sqrt{2}}$. Note that $\beta = \frac{\sqrt{2}}{\alpha}$, and, since $\sqrt{2} \in L$, it follows that $\beta \in L$. Thus $f$ splits into linear factors in $L$, and so the splitting field of $f$ is contained in $L$. But since the splitting field of $f$ contains the roots of $f$, and in particular $\alpha$, then $L = \mathbb{Q}(\alpha)$ is contained in the splitting field of $f$, and hence $L$ is the splitting field of $f$. Since $\mathbb{Q}$ is a perfect field, then any irreducible polynomial is separable over $\mathbb{Q}$, so $L$ is Galois over $\mathbb{Q}$.

Let $G = \operatorname{Gal}(L/\mathbb{Q})$. By definition of Galois extension, $|G| = [L : \mathbb{Q}] = 4$. Such a group $G$ is either cyclic of order 4 or isomorphic to the Klein 4-group $\mathbb{Z}/2 \times \mathbb{Z}/2$.

[1] Insert here the usual argument using Eisenstein's criterion and Gauss's lemma.

Let $\tau \in \operatorname{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ be an automorphism sending $\sqrt{2}$ to $-\sqrt{2}$, which exists since $\mathbb{Q}(\sqrt{2})$ is the splitting field of the irreducible polynomial $x^2-2$ over $\mathbb{Q}$. Since $\mathbb{Q}(\sqrt{2})$ is Galois over $\mathbb{Q}$, by the Fundamental Theorem of Galois Theory we have an isomorphism

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \operatorname{Gal}(L/\mathbb{Q})/\operatorname{Gal}(L/\mathbb{Q}(\sqrt{2}))$$

with the isomorphism induced by $\sigma \mapsto \sigma|_{\mathbb{Q}(\sqrt{2})}$. In particular, there exists a $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$ such that $\sigma|_{\mathbb{Q}(\sqrt{2})} = \tau$, or, in other words, $\sigma(\sqrt{2}) = -\sqrt{2}$. We claim $\sigma$ must have order 4.

We know $\sigma(\alpha)$ is one of $\alpha, -\alpha, \beta, -\beta$. If either $\sigma(\alpha) = \alpha$ or $\sigma(\alpha) = -\alpha$, then we would get $\sigma(\alpha^2) = \alpha^2$ and hence $\sigma(2+\sqrt{2}) = 2+\sqrt{2}$. This implies $\sigma(\sqrt{2}) = \sqrt{2}$, which is a contradiction. Thus $\sigma(\alpha) = \pm\beta$. If $\sigma(\alpha) = \beta$, then since $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\beta = \sqrt{2}/\alpha$, we have $\sigma(\beta) = -\alpha$. It follows that $\sigma^2 \neq \mathrm{id}$ and hence $\sigma$ has order 4. Likewise, if $\sigma(\alpha) = -\beta$, then $\sigma(-\beta) = -\alpha$ and $\sigma$ has order 4. This shows that $G \cong C_4 = \langle \sigma \rangle$. □

**Problem 3.** Let $L$ be the splitting field of $x^3-2$ over $\mathbb{Q}$.

a) Prove that there is a unique intermediate field $K$ such that $[K : \mathbb{Q}] = 2$.

b) Find, with justification, a primitive element for $K$ over $\mathbb{Q}$, that is, find an explicit $\alpha$ such that $K = \mathbb{Q}(\alpha)$.

**Solution.**

a) Let $\zeta_3 = e^{2\pi i/3}$. Note that $x^3-2$ has three distinct roots $\alpha = \sqrt[3]{2}$, $\zeta_3\alpha$, and $\zeta_3^2\alpha$. In particular, $x^3-2$ is separable. Since $L$ is the splitting field of an irreducible polynomial over $\mathbb{Q}$, then the extension $\mathbb{Q} \subseteq L$ is Galois. In particular, $|\operatorname{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$. We have shown in Problem Set 12 that $|\operatorname{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6$. On the other hand, since $f$ has 6 roots, $\operatorname{Gal}(L/\mathbb{Q})$ is a subgroup of $S_3$. Since the only subgroup of $S_3$ with 6 elements is $S_3$, we conclude that $\operatorname{Gal}(L/\mathbb{Q}) \cong S_3$.

   By the Fundamental Theorem of Galois Theory, an intermediate field $K$ with $[K : \mathbb{Q}] = 2$ corresponds to a subgroup $N = \operatorname{Gal}(L/K)$ of $G = \operatorname{Gal}(L/\mathbb{Q}) \cong S_3$ with index 2. But $S_3$ has a unique subgroup of order 2, which is $A_3$. Thus there is a unique intermediate field with $[K : \mathbb{Q}] = 2$.

b) By the Fundamental Theorem of Galois Theory, our intermediate field $K$ is the fixed field of

$$A_3 = \langle (1\ 2\ 3) \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}.$$

   Also by the Fundamental Theorem of Galois Theory,

$$K = L^{A_3}.$$

   Let $\tau_{(1\ 2\ 3)} \in \operatorname{Gal}(L/\mathbb{Q})$ be the element corresponding to $(1\ 2\ 3)$ and $\tau_{(1\ 3\ 2)} \in \operatorname{Gal}(L/\mathbb{Q})$ be the element corresponding to $(1\ 3\ 2)$. Here 1 corresponds to $\alpha$, 2 to $\zeta_3\alpha$, and 3 to $\zeta_3^2\alpha$. Then

$$\tau_{(1\ 2\ 3)}(\zeta_3) = \frac{\tau_{(1\ 2\ 3)}(\zeta_3\alpha)}{\tau_{(1\ 2\ 3)}(\alpha)} = \frac{\zeta_3^2\alpha}{\zeta_3\alpha} = \zeta_3$$

   and

$$\tau_{(1\ 3\ 2)}(\zeta_3) = \frac{\tau_{(1\ 3\ 2)}(\zeta_3\alpha)}{\tau_{(1\ 3\ 2)}(\alpha)} = \frac{\alpha}{\zeta_3^2\alpha} = \zeta_3^{-2} = \zeta_3.$$

In particular, $\zeta_3 \in L^{A_3} = K$. On the other hand, $\zeta_3$ satisfies the polynomial $x^3 - 1 = (x-1)(x^2+x+1)$, and since $\zeta_3 \neq 1$, then $\zeta_3$ must satisfy the polynomial $x^2+x+1$. By Problem Set 10 Problem 3, $x^2+x+1$ is irreducible, since $2 = 3-1$ and 3 is prime. Therefore, $x^2+x+1$ is the minimal polynomial of $\zeta_3$. In particular, $[\mathbb{Q}(\zeta_3):\mathbb{Q}] = 2$.

But now we have $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3) \subseteq K$ and

$$[\mathbb{Q}(\zeta_3):\mathbb{Q}] = 2 = [K:\mathbb{Q}].$$

By the Degree Formula, we conclude that $[K:\mathbb{Q}(\zeta_3)] = 1$, and thus $K = \mathbb{Q}(\zeta_3)$.

**Problem 4.** Let $L$ be the splitting field of $x^4 - 2022$ over $\mathbb{Q}$. Prove that there exists a unique intermediate field $\mathbb{Q} \subseteq K \subseteq L$ such that $[K:\mathbb{Q}] = 4$ and $\mathbb{Q} \subseteq K$ is Galois.

*Proof.* First, note that 2022 is even but not divisible by $2^2 = 4$, so $f = x^4 - 2022$ is irreducible over $\mathbb{Z}$ by Eisenstein's Criterion, and thus irreducible over $\mathbb{Q}$ by Gauss' Lemma. Consider the four distinct roots

$$\alpha = \alpha_1 = \sqrt[4]{2022}, \quad \alpha_2 = i\sqrt[4]{2022}, \quad \alpha_3 = -\alpha_1, \quad \alpha_4 = -i\sqrt[4]{2022} = -\alpha_2$$

of $f$. In particular, $f$ is separable, and thus $\mathbb{Q} \subseteq L$ is Galois. Moreover, $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \subseteq \mathbb{Q}(\alpha, i)$, while

$$\zeta = \frac{\alpha_2}{\alpha_1} \in L.$$

Thus $L = \mathbb{Q}(\alpha, i)$. Since $f$ is irreducible and monic, it must be the minimal polynomial of $\alpha$, $\alpha_2$, $\alpha_3$, and $\alpha_4$. In particular, $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$. On the other hand, $\alpha \in \mathbb{R}$ and $\zeta \notin \mathbb{R}$, so $\mathbb{Q}(\alpha) \subsetneq L$ and $[L:\mathbb{Q}(\alpha)] \geqslant 2$. On the other hand, $i$ satisfies the polynomial $x^2+1$. In particular, this shows that

$$[L:\mathbb{Q}(\alpha)] \leqslant 2 \quad \text{and thus} \quad [L:\mathbb{Q}(\alpha)] = 2.$$

By the Degree Formula,

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 2 \cdot 4 = 8.$$

Since $\mathbb{Q} \subseteq L$ is Galois, we now know that $|\operatorname{Gal}(L/\mathbb{Q})| = 8$.

Our polynomial $f$ has 4 distinct roots, so $\operatorname{Gal}(L/\mathbb{Q})$ is a subgroup of $S_4$, and we know it must have order 8. We identify $\alpha_i$ with $i$, so that an element of $S_4$ that sends $i$ to $j$ corresponds to an automorphism sending $\alpha_i$ to $\alpha_j$.

Complex conjugation induces a bijection $L \to L$, so it gives an element $s \in \operatorname{Gal}(L/\mathbb{Q})$ corresponding to the permutation $(2\ 4)$, since $s(\alpha_2) = \alpha_4$ and $s$ fixes $\alpha_1$ and $\alpha_3$.

Now consider the field extension $\mathbb{Q}(i) \subseteq L$. Since $[L:\mathbb{Q}] = 8$ and $[\mathbb{Q}(i):\mathbb{Q}] = 2$, by the Degree Formula we must have $[L:\mathbb{Q}(i)] = 4$. Since $L = \mathbb{Q}(i)(\alpha_1)$, the degree of $m_{\alpha_1,\mathbb{Q}(i)}$ must be 4. In particular, this shows that $x^4 - 2$ remains irreducible as a polynomial in $\mathbb{Q}(i)[x]$. So $L$ is the splitting field of the irreducible polynomial $x^4 - 2$ over $\mathbb{Q}(i)$, and $\operatorname{Aut}(L/\mathbb{Q}(i))$ acts transitively on the roots of $f$. In particular, there is an element $\tau \in \operatorname{Aut}(L/\mathbb{Q}(i))$ such that $\tau(\alpha_1) = \alpha_2$. We may regard $\tau$ as an element of $\operatorname{Aut}(L/\mathbb{Q})$ too. Such a $\tau$ satisfies $\tau(i) = i$, so

$$\tau(\alpha_2) = \tau(i\alpha_1) = i\tau(\alpha_1) = i\alpha_2 = \alpha_3.$$

We also get $\tau(\alpha_3) = \alpha_4$ and $\tau(\alpha_4) = \alpha_1$, so $\tau$ corresponds to the permutation $(1\,2\,3\,4)$.

The proves that $G$ is isomorphic to a subgroup of $S_4$ of order 8 that contains $(2\,4)$ and $(1\,2\,3\,4)$. We proved in class that the only such subgroup is $\rangle(2\ 4), (1\ 2\ 3\ 4)\langle$, and that it is isomorphic to the group $D_8$ of permutations of the square.

Now since the extension $\mathbb{Q} \subseteq L$ is Galois, by the Fundamental Theorem of Galois Theory we know that any intermediate field $K$ such that $[K : \mathbb{Q}] = 4$ corresponds to a subgroup $H$ of $\operatorname{Gal}(L/\mathbb{Q}) \cong D_8$ of index 4. In particular, note that

$$|H| = \frac{|\operatorname{Gal}(L/\mathbb{Q})|}{[\operatorname{Gal}(L/\mathbb{Q}) : H]} = \frac{8}{4} = 2.$$

On the other hand, the Fundamental Theorem of Galois Theory says that such an intermediate field $K$ is Galois over $\mathbb{Q}$ if and only if $H$ is a normal subgroup of $\operatorname{Gal}(L/\mathbb{Q}) \cong D_8$. Thus to show that there exists a unique such $K$, it suffices to show that $D_8$ has a unique normal subgroup of order 2. $\square$

**Problem 5.** Let $F \subseteq L$ be Galois field extension of degree 45. Prove there exists a unique intermediate field $E$ such that $[E : F] = 5$.

**Solution.** Since $F \subseteq L$ is Galois, then $G := \operatorname{Gal}(L/F) = \operatorname{Aut}(L/F)$ is a group of order $[L : F] = 45$. By the Fundamental Theorem of Galois Theory, an intermediate field $E$ with $[E : F] = 5$ would correspond to a subgroup $H$ of $G$ of index 5. Thus

$$|H| = \frac{|G|}{[G : H]} = \frac{45}{5} = 9.$$

Since $9 = 3^2$, 3 is prime, $\gcd(5, 9) = 1$, and $|G| = 5 \cdot 3^2$, by the Main Theorem of Sylow Theory we know there exists a Sylow 3-subgroup of $G$. By definition, such a subgroup has order 9. Then indeed, there does exist a subgroup of $G$ of order 9. Moreover, the Main Theorem of Sylow Theory also says that the number $n$ of Sylow 3-subgroups of $G$ must satisfy the following properties:

- $n \equiv 1 \pmod 3$, and
- $n | 5$.

Since $n|5$, we must have $n = 1$ or $n = 5$. On the other hand, $5 \not\equiv 1 \pmod 3$, so we must have $n = 1$. Therefore, there exists a unique subgroup of $G$ of order 9. By the Fundamental Theorem of Galois Theory, there exist a unique intermediate field $E$ with $[E : F] = 5$.