Problem Set 10 solutions

Problem 1. Let $F \subseteq L$ be a field extension and let $S \subseteq L$ be an arbitrarily subset of L whose elements are all algebraic over F. Show that $F \subseteq F(S)$ is algebraic.

Proof. Given $\alpha \in F(S)$, we want to show that α is algebraic over F. First, note that α can be written as a polynomial in S with coefficients in F, which means it uses only finitely many elements $\alpha_1, \ldots, \alpha_n \in S$, so $\alpha \in F(\alpha_1, \ldots, \alpha_n)$. Since $\alpha_1, \ldots, \alpha_n \in S$ are all algebraic over F, the extensions $F \subseteq F(\alpha_1)$, $F(\alpha_1) \subseteq F(\alpha_1, \alpha_2), \ldots, F(\alpha_1, \ldots, \alpha_{n-1}) \subseteq F(\alpha_1, \ldots, \alpha_n)$ are all algebraic. We showed in class that the composition of algebraic extensions is algebraic; thus the tower of algebraic extensions

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2), \ldots, F(\alpha_1, \ldots, \alpha_{n-1}) \subseteq F(\alpha_1, \ldots, \alpha_n)$$

implies that $F \subseteq F(\alpha_1, \ldots, \alpha_n)$ is algebraic. In particular, $\alpha \in F(\alpha_1, \ldots, \alpha_n)$ is algebraic over F. We conclude that $F \subseteq F(S)$ is algebraic. $\square$

Problem 2. Suppose $F \subseteq L$ and $F \subseteq L'$ be two field extensions. Let S be the set of pairs (E, i) where E is a subfield of L that contains F and $i : E \hookrightarrow L'$ is a ring map with $i|_F = \mathrm{id}_F$. Make S into a poset by declaring that $(E, i) \leq (E', i')$ if and only if $E \subseteq E'$ and $i'|_E = i$. Show that the poset $(S, \leq)$ satisfies the hypothesis of Zorn's Lemma.

Proof. First, we show that S is nonempty. Let $i : F \to L'$ be the inclusion of F in L'. Then $F \subseteq F \subseteq L$, F is a field, and $i \colon F \to L'$ is a ring homomorphism with $i|_F = \mathrm{id}_F$, so $(F, i) \in S$.

Now we need to check that given any chain $C = \{(E_j, i_j)\}_j$ of elements in S, there is an upper bound for C in S. Note that in particular the set $\{E_j\}$ is totally ordered by inclusion. In Problem Set 9, we essentially showed that $E := \bigcup E_i$ is a subfield of L containing F:

- Since $E_i \subseteq L$ for all i, $E \subseteq L$.
- $0, 1 \in E_i$ for all i, so $0, 1 \in E$. In particular, E is nonempty.
- Given $a, b \in E$, there exist j, k such that $a \in E_i$ and $b \in E_k$. Assume without loss of generality that $E_i \subseteq E_k$. Then $a, b \in E_k$, and since E_k is a field, $a \pm b, ab \in E_k \subseteq E$.
- For any nonzero $a \in E$, there exists some j such that $a \in E_j$. Since E_j is a field, $a^{-1} \in E_j \subseteq E$.

Moreover, consider the function $i \colon E \to L'$ defined as follows: for any $a \in E$, consider k such that $a \in E_k$, and define $i(a) = i_k(a)$. This is well-defined: if j is another index such that $a \in E_j$, then $E_k \subseteq E_j$ or $E_j \subseteq E_k$; if $E_k \subseteq E_j$, then $a \in E_k \subseteq E_j$, so $i_j(a) = i_j|_{E_k}(a) = i_k(a)$. Moreover, we claim that i is a ring homomorphism:

- Since $1 \in E_k$ for all k and i_k is a ring homomorphism for all k, $i(1) = i_k(1) = 1$.
- Given $a, b \in E$, there exist j, k such that $a \in E_i$ and $b \in E_k$. Assume without loss of generality that $E_i \subseteq E_k$. Then $a, b \in E_k$, and since i_k is a ring homomorphism,

  $$i(a+b) = i_k(a+b) = i_k(a) + i_k(b) = i(a) + i(b) \quad \text{and} \quad i(ab) = i_k(ab) = i_k(a)i_k(b) = i(a)i(b).$$

Finally, since $F \subseteq E_k$ for all k, $i|_F = i_k|F = \mathrm{id}_F$. We conclude that $(E, i) \in S$. Moreover, $E_k \subseteq E$ and $i|_{E_k} = i_k$ for all k by construction, so (E, i) is an upper bound for C. $\square$

Problem 3. For any prime p, the p**th cyclotomic polynomial**

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 \in \mathbb{Z}[x]$$

is irreducible in $\mathbb{Q}[x]$.

Proof. We cannot apply Eisenstein directly, but we can apply it after a linear change of variables. Consider the ring homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{Q}[y]$ given by $\phi(h(x)) = h(y+1)$. We claim that

$$\phi(f) = y^{p-1} + py^{p-2} + \binom{p}{2} y^{p-3} + \binom{p}{3} y^{p-4} + \cdots + \binom{p}{p-1} y + p.$$

To see this, we note that $f(x)(x-1) = x^p - 1$ and by the binomial theorem we have

$$\phi(x^p - 1) = (y+1)^p - 1 = y^p + py^{p-1} + \binom{p}{2} y^{p-2} + \cdots + py.$$

Since $\phi(x^p - 1) = \phi(f)\phi(x-1) = \phi(f)y$, the claim follows.

By Eisenstein's Criterion, $\phi(f)$ is irreducible in $\mathbb{Z}[y]$: p divides all coefficients of $\phi(f)$ except for the coefficeint of highest degree, and p^2 does not divide the coefficient of $\phi(f)$ of degree 0. By Gauss' Lemma, $\phi(f)$ is irreducible over $\mathbb{Q}$. Finally, we claim that this implies that f is irreducible in $\mathbb{Q}[x]$. Indeed, if f was reducible, then we would be able to write $f = gh$ for some nonconstant polynomials g, h, and thus $\phi(f) = \phi(g)\phi(h)$ would factor. By construction, $\phi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, and if q is a polynomial of degree n, then $\phi(q)$ also has degree n. In particular, $\phi(g)$ and $\phi(h)$ are nonconstant polynomials, and thus $\phi(f)$ would also be reducible. □

Problem 4. Let q be a quadratic polynomial with coefficients in $\mathbb{R}$. Show that the splitting field of q is either $\mathbb{R}$ or $\mathbb{C}$.

Proof. If q is reducible, then it must factor as a product of two linear factors, and thus all of its roots are in $\mathbb{R}$. In that case, the splitting field of q must be $\mathbb{R}$.

Now suppose that q is irreducible. Since $\mathbb{C}$ is algebraically closed, we know that q completely splits as a product of linear factors over $\mathbb{C}$, and thus the splitting field of q is contained in $\mathbb{C}$. Let $a + bi$ be one of the complex roots of q.[1] Since q is irreducible over $\mathbb{R}$, then we must have $b \neq 0$. Now consider $F = \mathbb{R}(a + bi)$. Since $a, b \in \mathbb{R}$, then $a + bi \in \mathbb{R}(i) = \mathbb{C}$. On the other hand,

$$i = b^{-1}(a + bi) - b^{-1}a \in \mathbb{R}(a + bi).$$

We conclude that $\mathbb{R}(a + bi) = \mathbb{C}$. Thus adjoining any complex number to $\mathbb{C}$ gives us $\mathbb{C}$. We showed in class that the splitting field of q is obtained by adjoining the two complex roots of q to $\mathbb{R}$. Therefore, the splitting field of q is $\mathbb{C}$. □

Problem 5. Determine, with justification, the splitting field K of the polynomial $x^6 - 4$ over $\mathbb{Q}$ and the degree $[K : \mathbb{Q}]$.

Proof. Let $b := \sqrt[6]{4}$ be the unique positive real root of $x^6 - 4$, and let $\zeta := e^{2\pi i/6}$, a primitive 6th root of 1. Then the roots of $x^6 - 4$ in $\mathbb{C}$ are $b\zeta^j$ for $j \in \{0, 1, 2, 3, 4, 5\}$, and the splitting field K of $x^6 - 4$ over $\mathbb{Q}$ is $K = \mathbb{Q}(b, b\zeta, ..., b\zeta^5)$.

Since $\zeta = (b)^{-1}(b\zeta) \in K$, then $\mathbb{Q}(b, \zeta) \subseteq K$. Since $b\zeta^j \in \mathbb{Q}(b, \zeta)$ for all j, the reverse containment also holds. Therefore $K = \mathbb{Q}(b, \zeta)$.

[1] In fact, the two roots of q must be of the form $a \pm bi$, but we won't need that fact here.

Now $\mathbb{Q} \subseteq \mathbb{Q}(b) \subseteq \mathbb{Q}(b,\zeta) = K$ and $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(b,\zeta) = K$, and so the Degree Formula says that

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(b)][\mathbb{Q}(b) : \mathbb{Q}] \quad (*)$$

and

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] \quad (**).$$

Since $b = 4^{1/6} = (2^2)^{1/6} = 2^{1/3} = \sqrt[3]{2}$, then b is a root of the polynomial $x^3 - 2$ over $\mathbb{Q}$. Since $x^3 - 2$ is a monic polynomial in $\mathbb{Z}[x]$ satisfying that all nonleading coefficients are divisible by the prime number 2 and the constant term is not divisible by 2^2, then Eisenstein's Criterion says that $x^3 - 2$ is irreducible in $\mathbb{Z}[x]$. Then Gauss' Lemma says that $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. Therefore, $x^3 - 2 = m_{b,\mathbb{Q}}$ by definition of minimal polynomial. Now a theorem from class says that

$$[\mathbb{Q}(b) : \mathbb{Q}] = \deg(m_{b,\mathbb{Q}}) = \deg(x^3 - 2) = 3.$$

Hence Equation (*) says that $3 \mid [K : \mathbb{Q}]$.

Since $\zeta^3 = e^{3(2\pi i/6)} = e^{\pi i} = -1$, then ζ is a root of x^3+1 over $\mathbb{Q}$. Since $x^3+1 = (x+1)(x^2-x+1)$ and $\zeta \neq -1$, then ζ is a root of $x^2 - x + 1$ over $\mathbb{Q}$. Then $\deg(m_{\zeta,\mathbb{Q}}) \leqslant 2$, and so again by the same theorem from class we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leqslant 2$. Now $\zeta \notin \mathbb{R}$, and hence $\zeta \notin \mathbb{Q}$ and $[Q(\zeta) : \mathbb{Q}] \neq 1$. Therefore $[Q(\zeta) : \mathbb{Q}] = 2$. Hence Equation (**) says that $2 \mid [K : \mathbb{Q}]$. Combining this with the result of the previous paragraph, since 2 and 3 are relatively prime, then $6 \mid [K : \mathbb{Q}]$.

Equation (*) also says that

$$[K : \mathbb{Q}] = [(\mathbb{Q}(b))(\zeta) : \mathbb{Q}(b)] \cdot 3.$$

Since ζ is also a root of the polynomial $x^2 - x + 1$ in $\mathbb{Q}(b)$, then the minimum polynomial of ζ over $\mathbb{Q}(b)$ has degree at most 2, and so

$$[(\mathbb{Q}(b))(\zeta) : \mathbb{Q}(b)] \leqslant 2.$$

Hence $[K : \mathbb{Q}] \leqslant 2 \cdot 3 = 6$. Combining this with the result of the previous paragraph shows that $[K : \mathbb{Q}] = 6$. □

Problem 6. Let L be the splitting field of $x^p - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$ where p is an odd prime integer. Find $[L : \mathbb{Q}]$.
Hint: Consider both chains $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{2}) \subseteq L$ and $\mathbb{Q} \subseteq \mathbb{Q}(e^{2\pi i/p}) \subseteq L$.

Proof. We have $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p$ since $x^p - 2$ is irreducible (over $\mathbb{Z}$ by Eisenstein's Criterion applied to the prime p, over $\mathbb{Q}$ by Gauss' Lemma; complete the details as we have done in many similar problems). By the degree formula, it follows that p divides $[L : \mathbb{Q}]$. We have

$$[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p - 1$$

since $x^{p-1} + x^{p-2} + \cdots + x + 1$ has $e^{2\pi i/p}$ as a root and is irreducible over $\mathbb{Q}$ by Problem 3, so it must be the minimal polynomial of $e^{2\pi i/p}$. By the degree formula, it follows that $p - 1$ divides $[L : \mathbb{Q}]$. Since p and $p - 1$ are relatively prime, we conclude that $p(p - 1)$ divides $[L : \mathbb{Q}]$. On the other hand, we have

$$L = \mathbb{Q}(\sqrt[p]{2}, e^{2\pi i/p}) \quad \text{and} \quad [L : \mathbb{Q}(e^{2\pi ip})] \leqslant p - 1,$$

since $\sqrt[p]{2}$ is a root of $x^{p-1} + x^{p-2} + \cdots + x + 1$. By the Degree Formula, we conclude that

$$[L : \mathbb{Q}] \leqslant (p - 1)p.$$

Thus

$$[L : \mathbb{Q}] = p(p - 1).$$

□