Problem Set 11 solutions

Problem 1. Let n be a positive integer and let p be a prime integer. Let $q(x) = x^{p^n} - x \in (\mathbb{Z}/p)[x]$, and let K be the splitting field of q over $\mathbb{Z}/p$.

a) Show that the subset $E \subseteq K$ consisting of all roots of q in K is a subfield of K.

b) Show that $|E| = p^n$ and $E = K$.

c) Let L be any field with $|L| = p^n$, and let F be the prime field of L. Show that $F \cong \mathbb{Z}/p$ and that L is the splitting field of the polynomial $q_F(x) = x^{p^n} - x \in F[x]$ over F.

   Hint: Consider the multiplicative group $(L^\times, \cdot)$.

d) Show that any two fields of order p^n are isomorphic.

Proof.

a) Since $\mathbb{Z}/p[x]$ has prime characteristic p, the Frobenius map $h_n \colon K \to K$ defined by $h_n(a) := a^{p^n}$ for all $a \in K$ is a ring homomorphism.

   Note that
   $$q(0) = 0^{p_n} - 0 = 0 - 0 = 0 \text{ and } q(1) = 1^{p^n} - 1 = 1 - 1 = 0,$$
   so $0, 1 \in E$, so E is nonempty. Suppose that $e, e' \in E$. Using the fact that h_n is a homomorphism gives
   $$\begin{aligned} q(e-e') &\overset{def\ q}{=} (e-e')^{p^n} - (e-e') \overset{def\ h_n}{=} h_n(e-e') - e + e' \\ &\overset{h_n\ hom}{=} h_n(e) - h_n(e') - e + e' \overset{def\ h_n}{=} e^{p^n} - (e')^{p^n} - e + e' = q(e) - q(e') = 0 - 0 = 0; \end{aligned}$$
   hence $e - e' \in K$ is another root of q, and so $e - e' \in E$. We also have
   $$\begin{aligned} q(ee') &= (ee')^{p^n} - ee' = e^{p^n}(e')^{p^n} - ee' = e^{p^n}(e')^{p^n} - e^{p^n}e' + e^{p^n}e' - ee' \\ &= e^{p^n}q(e') + q(e)e' = e^{p^n}(0) = (0)e' = 0; \end{aligned}$$
   hence $ee' \in K$ is a root of q, and so $ee' \in E$. Since E is closed under subtraction and multiplication, E is a subring of K. Since $q(e^{-1}) = (e^{-1})^{p^n} - e^{-1} = (e^{p^n})^{-1} - e^{-1} = e^{-1} - e^{-1} = 0$ $e^{-1} \in K$ is a root of q, and so $e^{-1} \in E$. Therefore, since E is also closed under taking inverses, E is a subfield of K.

b) Since q has degree p^n and it splits into linear factors in $K[x]$, then q has p^n roots in K, counting multiplicity. Since the derivative is $q'(x) = p^n x^{p^n - 1} - 1 = -1$, q' has no roots. Since any root of q of multiplicity $\geqslant 2$ is also a root of q', we deduce that q has only roots of multiplicity 1. Thus all of the roots of q are distinct and so q has exactly p^n distinct roots. By definition, E is precisely the set of these p^n distinct roots of q, hence $|E| = p^n$.

   Since E contains all of the roots of q, then q splits completely into linear factors in $E[x]$. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$, Lagrange's Theorem gives that $|a|$ divides $|(\mathbb{Z}/p\mathbb{Z})^x| = p - 1$. Then $a^p = a \cdot a^{p-1} = a \cdot 1 = a$. Now an inductive argument shows that $a^{p^n} = a$ for all $n \geqslant 1$, since $a^{p^n} = (a^{p^{n-1}})^p$. Hence
   $$q(a) = a^{p^n} - a = a - a = 0.$$
   Hence $\mathbb{Z}/p\mathbb{Z} \subseteq E$. Then E is a subfield of the splitting field K of q over $\mathbb{Z}/p\mathbb{Z}$ that contains the base field $\mathbb{Z}/p\mathbb{Z}$, and q splits linearly over E. By the minimality condition in the definition of splitting field, it follows that E cannot be a proper subfield of K, so $E = K$.

c) Since F is a subfield of L, and L is a finite set, then L is a vector space of finite dimension m over F', for some some $m \geqslant 1$. Therefore, $p^n = |L| = |F|^m$. Hence $|F|$ is a power of p. In a previous problem set and in class, we gave a classification of prime fields that tells us that if $|F|$ is finite then $|F|$ must be a prime number; hence $|F| = p$ and therefore $F \cong \mathbb{Z}/p\mathbb{Z}$.

Note that $q_F(0) = 0^{p^n} - 0 = 0$, and so the element 0 of L is a root of q_F. Since $L^\times$ is a group of order $p^n - 1$, then Lagrange's Theorem again shows that for any $a \in L^\times$ we have $a^{p^n-1} = 1$. Therefore,

$$q_F(a) = a^{p^n} - a = aa^{p^n-1} - a = a - a = 0.$$

Thus the p^n elements of L are p^n distinct roots of q_F, and so all of the roots of q_F lie in L. Hence L is a field containing F such that q_F splits completely into linear factors in $L[x]$. Moreover, any subfield $K \subsetneq L$ of L is necessarily missing at least one of the p^n distinct roots of q. By definition of splitting field, we conclude that L is a splitting field for q_F over F.

d) Suppose that L and L' are fields of order p^n, and let F and F' be their respective prime fields. By part (c), we must have

$$F' \cong \mathbb{Z}/p\mathbb{Z} \cong F,$$

Also by c), L is the splitting field of the polynomial $q_F(x) = x^{p^n} - x \in F[x]$ over F and L' is the splitting field of the polynomial $q_{F'}(x) = x^{p^n} - x \in F'[x]$ over F'. Let $j : F \to F'$ be an isomorphism and let $\hat{j} \colon F[x] \to F'[x]$ be the induced isomorphism of polynomial rings.

Notice that there is an inclusion of F' into L given by composing j with the inclusion of F' into L', as follows:

$$F \xrightarrow{j} F' \subseteq L'.$$

Therefore, L' is an extension of F. We claim that L' is a splitting field of q_F over F. Indeed, the image of q_F in $L'[x]$ is $\hat{j}(q_F) = q_{F'}$, which splits into linear factors over L', but not in any proper subfield of L.

Now the uniqueness of the splitting field gives that $L \cong L'$ since they are both splitting fields for $q_{F'}$. Therefore, any two fields of order p^n are isomorphic. $\square$

Problem 2. Show that every algebraic field extension of a finite field is separable.

Proof. Let F be a finite field. Then its prime subfield is also finite and hence isomorphic to $\mathbb{Z}/p$ for some prime integer p, thus $\mathrm{ch}(F) = p$. By a result from class, we just need to prove that the Frobenius endomorphism $\phi : F \to F$ defined by $\phi(c) = c^p$ is surjective. But by the Freshman's Dream, ϕ is a ring homomorphism and, since F is a field, and $\phi \neq 0$, it is injective. Since $|F| < \infty$, ϕ must be a bijection by the Pigeonhole Principle. $\square$

Problem 3. Assume F is field and let $f \in F[x]$.

a) Assume $\mathrm{char}(F) = 0$. Prove that f is not separable if and only if the prime factorization of f in $F[x]$ admits a repeated factor.

b) Give a counterexample to the previous part when the assumption $\mathrm{char}(F) = 0$ is omitted.

Proof.

a) Suppose f is not separable; say $\alpha \in \overline{F}$ is a repeated root of f. Then $m_{\alpha,F}$ is irreducible and $m_{\alpha,F} \mid f$, so that $f = gh$ for some $h \in F[x]$. Moreover, since $\mathrm{char}(F) = 0$ and $m_{\alpha,F}$ is irreducible, we know that $m_{\alpha,F}$ is separable and hence α is not a repeated root of $m_{\alpha,F}$. That is, in $\overline{F}[x]$

we have $g = (x-\alpha)l$ with $l(\alpha) \neq 0$. Since $f = (x-\alpha)^2 j$, we must have that $x - \alpha$ divides h in $\overline{F}[x]$. That is, we must have $h(\alpha) = 0$. But then g divides h too and so $f = g^2 q$ for some q. So g is a repeated prime (irreducible) factor of f.

Assume now that $f = g^2 m$ for some prime (irreducible) g. Then for any root α of g in $\overline{F}$, we have that $f = (x-\alpha)^2 l$ in $\overline{F}[x]$ and hence f is not separable.

b) Let $F = (\mathbb{Z}/p)(y)$, the field of fractions of the polynomial ring $(\mathbb{Z}/p)[y]$, and let $f(x) = x^p - y$. Since $(\mathbb{Z}/p)[y]$ is a PID and y is a prime element, then f is irreducible by Eisenstein's Criterion. If α is any root of f in $\overline{F}$, then $f(x) = (x-\alpha)^p$ by the Freshman's Dream. Since $p \geqslant 2$, f is not separable. But since f is irreducible over F, it doesn't have a repeated factor in its prime factorization over F. □

Problem 4. Let L be the splitting field of $f = x^5 - 11 \in \mathbb{Q}[x]$.

a) Find the degree of $[L : \mathbb{Q}]$.

b) Let $F = \mathbb{Q}(\xi)$, where $\xi = e^{\frac{2\pi i}{5}}$ is a primitive 5th root of unity. Show that f is irreducible over F.

Proof.

a) First, we claim that $L = \mathbb{Q}(\xi, \sqrt[5]{11})$. On the one hand, the roots of f are $\sqrt[5]{11}\xi^i$ for $i = 0, 1, 2, 3, 4$, so $L = \mathbb{Q}(\sqrt[5]{11}\xi^i \mid 0 \leqslant i \leqslant 4) \subseteq \mathbb{Q}(\xi, \sqrt[5]{11})$. On the other hand,

$$\xi = \frac{\sqrt[5]{11}\xi}{\sqrt[5]{11}} \in L,$$

so $L = \mathbb{Q}(\xi, \sqrt[5]{11})$.

We claim that f is irreducible over $\mathbb{Q}$: indeed, 11 divides all the coefficients of f of nonmaximal degree but the coefficient of maximal degree, 11^2 does not divide the degree 0 coefficient of f, and 11 is prime, so Eisenstein's Criterion says that f is irreducible over $\mathbb{Z}$. By Gauss' Lemma, f is irreducible over $\mathbb{Q}$. Since $\sqrt[5]{11}$ is a root of the monic irreducible polynomial f, we conclude that f is the minimal polynomial of $\sqrt[5]{11}$ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\sqrt[5]{11}) : \mathbb{Q}] = 5$.

By Problem Set 10, $g = x^4 + x^3 + x^2 + x + 1$ is irreducible, since 5 is prime. Note that ξ is a root of $(x-1)g = x^5 - 1$ but not a root of $x - 1$, so $g(\xi) = 0$. Since g is irreducible, we conclude that g is the minimal polynomial of ξ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$.

By the Degree Formula,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}] = 4[L : \mathbb{Q}(\xi)]$$

and

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[5]{11})][\mathbb{Q}(\sqrt[5]{11}) : \mathbb{Q}] = 5[L : \mathbb{Q}(\sqrt[5]{11})].$$

Thus $4 | [L : \mathbb{Q}]$ and $5 | [L : \mathbb{Q}]$. Since $\gcd(4, 5) = 1$, we conclude that $20 | [L : \mathbb{Q}]$.

Now ξ still satisfies g over $F = \mathbb{Q}(\sqrt[5]{11})$, so $m_{\xi,F} | g$. Thus the degree of $m_{\xi,F}$ is at most 4, and $[L : \mathbb{Q}(\sqrt[5]{11})] \leqslant 4$. Therefore,

$$[L : \mathbb{Q}] = 5[L : \mathbb{Q}(\sqrt[5]{11})] \leqslant 20.$$

But $20 | [L : \mathbb{Q}]$, so $[L : \mathbb{Q}] = 20$.

b) In the proof of part a) we showed that $[\mathbb{Q}(\sqrt[5]{11}) : \mathbb{Q}] = 5$, $[F : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}] = 4$, and $[L : \mathbb{Q}] = 20$. Moreover, $L = F(\sqrt[5]{2}$. By the Degree Formula,

$$[F(\sqrt[5]{2} : F][F : \mathbb{Q}] = [L : \mathbb{Q}] = 20.$$

Thus $[F(\sqrt[5]{2} : F] = 4$, so $m_{\sqrt[5]{2},F}$ has degree 5. Since $f(\sqrt[5]{2}) = 0$ and $f \in F[x]$ is monic, we conclude that f is the minimal polynomial of $\sqrt[5]{2}$ over F. In particular, f must be irreducible over F. $\square$

Problem 5. Let F be a field, let $a_1, \ldots, a_n$ be elements of an extension of F, and $L = F(a_1, \ldots, a_n)$.

a) Show that

$$F(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in F[x_1, \ldots, x_n], g \neq 0 \right\}.$$

Proof. We will use induction on n.

Base case: $n = 1$ was shown in Problem Set 7, Problem 5.

Induction Step: Let $n \geqslant 2$, and assume that

$$F(a_1, \ldots, a_{n-1}) = \left\{ \frac{f(a_1, \ldots, a_{n-1})}{g(a_1, \ldots, a_{n-1})} \mid f, g \in F[x_1, \ldots, x_{n-1}], g \neq 0 \right\}.$$

We showed in Problem Set 9 Problem 2 that

$$F(a_1, \ldots, a_n) = F(a_1, \ldots, a_{n-1})(a_n).$$

Combining these statements gives

$$\begin{aligned} F(a_1, \ldots, a_n) &= F(a_1, \ldots, a_{n-1})(a_n) \\ &= \left\{ \frac{u(a_n)}{v(a_n)} \mid u, v \in F(a_1, \ldots, a_{n-1})[x] \right\} \\ &= \left\{ \frac{s(a_n)}{t(a_n)} \mid x, t \in F[a_1, \ldots, a_{n-1}][x] \right\} \end{aligned}$$

where the last equality follows by clearing the denominators of the coefficients of u, v. The last set is the same as

$$\left\{ \frac{f(a_1, \ldots, a_{n-1})}{g(a_1, \ldots, a_{n-1})} \mid f, g \in F[x_1, \ldots, x_{n-1}], g \neq 0 \right\}. \quad \square$$

b) Let

$$F[a_1, \ldots, a_n] := \{ f(a_1, \ldots, a_n) \mid f \in F[x_1, \ldots, x_n] \}.$$

Prove that if $a_1, \ldots, a_n$ are algebraic over F, then $L = F[a_1, \ldots, a_n]$.

Proof. By induction on n.

Base case: the case $n = 1$ was proven in class.

Induction Step: Assume $F(a_1, \ldots, a_{n-1}) = F[a_1, \ldots, a_{n-1}]$. We showed in Problem Set 9 Problem 2 that

$$F(a_1, \ldots, a_n) = F(a_1, \ldots, a_{n-1})(a_n).$$

Combining this with the inductive hypothesis and the base case gives

$$F(a_1, \dots, a_n) = F(a_1, \dots, a_{n-1})(a_n) = F[a_1, \dots, a_{n-1}][a_n] = F[a_1, \dots, a_n].$$

□

c) Prove that if $\sigma \in \mathrm{Aut}(L/F)$ and $f \in L[x_1, \dots, x_n]$, then

$$\sigma(f(a_1, \dots, a_n)) = f^\sigma(\sigma(a_1), \dots, \sigma(a_n)),$$

where f^σ denotes the polynomial obtained from f by applying σ to its coefficients and leaving the variables unchanged.

Proof. This follows since σ preserves sums and products:

$$\sigma\left(\sum c_{i_1,\dots,i_n} a_1^{i_1} \cdots a_n^{i_n}\right) = \sum \sigma(c_{i_1,\dots,i_n}) \sigma(a_1)^{i_1} \cdots \sigma(a_n)^{i_n}. \quad \square$$

d) Prove that if $\sigma \in \mathrm{Aut}(L/F)$, then σ is uniquely determined by $\sigma(a_1), \dots, \sigma(a_n)$.

Proof. By part (a), a typical element of L is $\ell = \frac{f(a_1,\dots,a_n)}{g(a_1,\dots,a_n)}$ for $f, g \in F[x_1, \dots, x_n]$. By part (c),

$$\sigma(\ell) = \frac{f^\sigma(\sigma(a_1), \dots, \sigma(a_n))}{g^\sigma(\sigma(a_1), \dots, \sigma(a_n))} = \frac{f(\sigma(a_1), \dots, \sigma(a_n))}{g(\sigma(a_1), \dots, \sigma(a_n))},$$

where the last inequality takes into account that the coefficients of f and g are in L, so they are fixed by σ. Now

$$\frac{f(\sigma(a_1), \dots, \sigma(a_n))}{g(\sigma(a_1), \dots, \sigma(a_n))}$$

above only depends on $\sigma(a_1), \dots, \sigma(a_n)$ so we get the desired conclusion. □