Solution 25

Finite fields

1. Let k be a field.

   (a) Show that k is an extension of a field k_0, called *prime field*, given by $k_0 = \mathbb{Q}$ if $\operatorname{char}(k) = 0$ $k_0 = \mathbb{F}_p$ and if $\operatorname{char}(k) = p > 0$.

   (b) Show that any field homomorphism restricts to the identity on the prime field.

   Solution:

   (a) The characteristic of the field k is precisely the non-negative generator of the kernel of the unique ring homomorphism $\varphi\colon \mathbb{Z} \to k$.

   If $\operatorname{char}(k) = 0$, then φ is an injective map. Since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, the inclusion φ extends to an inclusion of $\mathbb{Q}$ inside k.

   If $\operatorname{char}(k) > 0$, then it is a prime number p and by the first homomorphism theorem φ induces an injection $\varphi\colon \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \to k$, and k_0 coincides with the additive subgroup of k generated by 1_k.

   (b) If $\theta\colon k \to \ell$ is a field homomorphism, then the composition of ring homomorphisms $\mathbb{Z} \xrightarrow{\varphi_k} k \xrightarrow{\theta} \ell$ must coincide with the unique homomorphism $\varphi_\ell\colon \mathbb{Z} \to \ell$. Moreover θ is necessarily injective (as is every field homomorphism, because the image of $x \in k^\times = k \smallsetminus \{0\}$ has inverse $\theta(x^{-1})$, hence it cannot be zero). Thus

   $$\ker(\varphi_\ell) = \{m \in \mathbb{Z} : \varphi_k(m) \in \ker(\theta)\} = \{m \in \mathbb{Z} : \varphi_k(m) = 0\} = \ker(\varphi_k)$$

   so that k and ℓ have the same characteristic.

   If the two fields have characteristic $p > 0$, then they contain the prime field $\mathbb{F}_p$ as images of φ_k and φ_ℓ and those prime fields are mapped "identically" because $\varphi_\ell = \theta \circ \varphi_k$.

   If the two fields have characteristic 0, then θ maps each integer $m \cdot 1_k$ to $m \cdot 1_\ell$. The inclusion $\varphi_k\colon \mathbb{Z} \to k$ extends to an inclusion $\overline{\varphi_k}\colon \mathbb{Q} \to k$ by sending m/n to $\varphi_k(m)\varphi_k(n)^{-1}$ for $m, n \in \mathbb{Z}$ with $n \neq 0$. Similarly, φ_ℓ extends to $\overline{\varphi_\ell}\colon \mathbb{Q} \to \ell$. In order to conclude, it is enough to prove that $\overline{\varphi_\ell} = \theta \circ \overline{\varphi_k}$, so that θ restricts to the identity on the prime fields $\mathbb{Q}$ seen as images of $\overline{\varphi_k}$ and $\overline{\varphi_\ell}$. This is again done by using the fact that $\varphi_\ell = \theta \circ \varphi_k$: for all $m, n \in \mathbb{Z}$ with $n \neq 0$,

$$\begin{aligned}(\theta \circ \overline{\varphi_k})(m/n) &= \theta(\overline{\varphi_\ell}(m/n)) = \theta(\varphi_\ell(m)\varphi_\ell(n)^{-1}) \\ &= (\theta \circ \varphi_\ell)(m) \cdot (\theta \circ \varphi_\ell)(n)^{-1} = \varphi_\ell(m)\varphi_\ell(n)^{-1} = \overline{\varphi_\ell}(m/n).\end{aligned}$$

2. We say that a field k is *perfect* if every algebraic field extension of k is separable.

   (a) Prove that k is perfect if and only if every irreducible polynomial in $k[X]$ is *separable*, i.e. has no multiple roots.

   (b) Let $f \in k[X]$ be an irreducible polynomial. Show that f is separable if and only if its derivative is nonzero.

   (c) For f as in Part (b), show that the derivative of f is zero if and only if $\operatorname{char}(k) = p > 0$ and $f(X) = g(X^p)$ for some irreducible $g \in k[X]$.

   (d) Suppose that $\operatorname{char}(k) = p > 0$. Prove that k is perfect if and only if the Frobenius homomorphism $\varphi \colon k \to k$, $x \mapsto x^p$ is surjective.

   (e) Deduce that fields of characteristic zero and finite fields are perfect.

Solution:

(a) Suppose k is a perfect field and let $f \in k[X]$ be an irreducible polynomial with x a root of f in an algebraic closure $\bar{k}$ of k. Then $k(x)$ is a field extension of k and it is separable because k is perfect. Hence x is a separable element, meaning that its minimal polynomial f is separable.

Conversely, assume that every irreducible polynomial in $k[X]$ is separable and let ℓ/k be an algebraic extension. Every $\alpha \in \ell$ has a minimal polynomial over k because ℓ/k is algebraic; it is a separable polynomial by assumption, meaning that α is separable. Hence ℓ/k is a separable field extension.

(b) Let $a_1, \dots, a_r \in \bar{k}$ be the distinct roots of f with respective multiplicities $n_1, \dots, n_r \geqslant 1$. Over $\bar{k}$ we thus have the factorization

$$f = \prod_{i=1}^{r} (X - a_i)^{n_i},$$

with derivative

$$f' = \sum_{i=1}^{r} n_i (X - a_i)^{n_i - 1} \cdot \prod_{j \neq i} (X - a_j)^{n_j}.$$

From this we see that $f'(a_i) = n_i(a_i - a_i)^{n_i - 1} \cdot \prod_{j \neq i}(a_i - a_j)^{n_j}$ is nonzero if $n_i = 1$, proving "$\Rightarrow$".

Conversely, suppose f has a multiple root a in its splitting field E. Then from the above we see that a is a root of both f and f', so $X - a$ divides their gcd g (over E), i.e. g has degree at least 1. Moreover, if $f' \neq 0$, then g has degree strictly less than that of f. But the gcd over E is the same as the gcd over k (see Solution 16, Exercise 1(a)), so f is divisible by g over k and hence not irreducible – contrary to the assumption.

(c) If $\operatorname{char}(k) = p > 0$ and $f(X) = g(X^p)$, then $f'(X) = pX^{p-1} \cdot g'(X) = 0$.
For the converse, write $f = \sum_{i=0}^{n} a_i X^i \in k[X]$ with $a_n \neq 0$. Then we have $f' = \sum_{i=1}^{n} i \cdot a_i X^{i-1} = 0$ if and only if $i \cdot a_i = 0$ for all $1 \leqslant i \leqslant n$. In particular, $na_n = 0$; hence $n = 0$ in k, which implies that k has positive characteristic p. Moreover, for any index i not divisible by p, the equation $i \cdot a_i = 0$ yields $a_i = 0$. Thus, we can write $f(X) = \sum_{j=0}^{n/p} a_{jp} X^{jp} =: g(X^p) \in k[X^p]$. Note that any factorization of g yields one of f. Thus g is irreducible because f is.

(d) Suppose that k is a perfect field. We want to show that each $y \in k$ has a p-th root in k. Since k is perfect, the polynomial $f = X^p - y \in k[X]$ must be either separable, or reducible by Part (a). Let $x \in \bar{k}$ be a root of f, i.e. $x^p = y$. Since k has characteristic p, we can compute

$$(X - x)^p = X^p - x^p = X^p - y = f.$$

Hence x is the only root of f in $\bar{k}$ and so f is not separable; in fact, a factor of f in $k[X]$ has no multiple roots in $\bar{k}$ if and only if it is a linear factor. As each irreducible factor of f in $k[X]$ must separable, the only possibility is that f splits completely in $k[X]$. In particular, $x \in k$.

Conversely, suppose that the Frobenius map $\varphi \colon k \to k$ is surjective. By (a) it suffices to prove that every irreducible polynomial f in $k[X]$ is separable. Suppose $f \in k[X]$ is irreducible and has multiple roots. Then by Part (c) we have $f \in k[X^p]$. Moreover, every coefficient of f is a p-th power of an element in k, since φ is surjective by assumption. So we can write

$$f = \sum_{i=0}^{n} b_i^p X^{pi} = \left(\sum_{i=0}^{n} b_i X^i \right)^p,$$

which is a proper factorization of f in $k[X]$, contradicting the assumption that f is irreducible. Hence f has no multiple roots.

(e) If k is a field of characteristic zero, then by Part (c), the derivative of any irreducible polynomial over k is nonzero. By Part (b), this implies that every such polynomial is separable, which by Part (a) is equivalent to k being perfect.

Let k be a finite field of characteristic p. The Frobenius homomorphism φ from Part (d) is a generator of $\operatorname{Gal}(k/\mathbb{F}_p)$ (see Assignment 17, Exercise 3). In particular, it is an automorphism, hence surjective. By Part (d) k is thus perfect.

3. Let k be a finite field and consider a finite field extension $k(\alpha, \beta)/k$ such that $k(\alpha) \cap k(\beta) = k$ (inside an algebraic closure of k). Prove that $k(\alpha, \beta) = k(\alpha + \beta)$.

   Hint. Study the cardinality of the involved fields.

   Solution: Clearly, $k(\alpha + \beta) \subset k(\alpha, \beta)$ since $\alpha + \beta \in k(\alpha, \beta)$.

   For the reverse inclusion, let $q = |k|$ be a power of a prime p. We write $k = \mathbb{F}_q$ and we know that $\mathrm{char}\,(k) = p$. Fix an algebraic closure $\bar{k}$. Then, as seen in Algebra I, for each power q^t of q there exists a unique subfield of $\bar{k}$ containing q^t elements: it consists of those elements $\alpha \in \bar{k}$ such that $\alpha^{q^t} = \alpha$. The proof of Assignment 13, Exercise 1(b) generalizes to q and tells us that $\mathbb{F}_{q^s} \subset \mathbb{F}_{q^t}$ if and only if s divides t.

   Let $n, m \in \mathbb{N}$ be such that $k(\alpha) = \mathbb{F}_{q^n}$ and $k(\beta) = \mathbb{F}_{q^m}$. Here n is the minimal positive integer h such that $\alpha^{q^h} = \alpha$, because otherwise $k(\alpha)$ would be contained in a strictly smaller subfield of $\mathbb{F}_{q^n}$. Since $k = k(\alpha) \cap k(\beta)$ is the largest subfield of $\bar{k}$ contained in both $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^m}$, we deduce that $\gcd(m, n) = 1$. In particular, p is not a common divisor of m and n. Without loss of generality, assume that p does not divide n. Also, note that $k(\alpha, \beta)$ is the smallest subfield of $\bar{k}$ containing both $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^m}$, so $k(\alpha, \beta) = \mathbb{F}_{q^{mn}}$.

   We write $k(\alpha + \beta) = \mathbb{F}_{q^t}$. This means that

   $$\alpha^{q^t} + \beta^{q^t} = (\alpha + \beta)^{q^t} = \alpha + \beta,$$

   implying that

   $$\alpha^{q^t} - \alpha = -(\beta^{q^t} - \beta) \in k(\alpha) \cap k(\beta) = k.$$

   Write $\alpha^{q^t} = \alpha + \lambda$ for $\lambda \in \mathbb{F}_q$. Repeatedly raising to the q^t-th power, we deduce inductively that

   $$\alpha^{q^{tp}} = \alpha + p\lambda = \alpha.$$

   This means that $n \mid tp$ and since $p \nmid n$ we obtain $n \mid t$. Thus, by uniqueness of subfields mentioned above, $k(\alpha + \beta) = \mathbb{F}_{q^t}$ contains $k(\alpha)$ and, in particular, $\alpha \in k(\alpha + \beta)$. This implies that $\beta = (\alpha + \beta) - \alpha \in k(\alpha + \beta)$, as well. Hence $k(\alpha, \beta) \subset k(\alpha + \beta)$ and we conclude that $k(\alpha, \beta) = k(\alpha + \beta)$.

4. Give a detailed proof of Wedderburn's theorem: *Every finite skew-field is a field.*

   Solution: See N. Jacobson, *Basic Algebra I, 2nd Edition*, Section 7.7 **or**
   R. Lidl, H. Niederreiter, *Finite Fields*, Ch. 2, Section 6, Theorem 2.55, first proof.