Solution 17

Extensions of Finite Fields, Splitting Fields

1. Let L_1/K_1 and L_2/K_2 be two field extensions and $\varphi : L_1 \longrightarrow L_2$ an isomorphism of fields such that $\varphi(K_1) = K_2$. Prove that $[L_1 : K_1] = [L_2 : K_2]$.

   Solution: Let $(\alpha_1, \ldots, \alpha_n)$ be a K_1-basis of L_1, so that $n = [L_1 : K_1]$. Since φ is injective, $(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$ consists of n different elements of L_2. We want to prove that $(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$ is a K_2-basis of L_2, so that $[L_2 : K_2] = n = [L_1 : K_1]$.

   For every $\beta \in L_2$, there exists a unique $\alpha \in L_1$ such that $\varphi(\alpha) = \beta$. Writing $\alpha = \sum_{i=1}^n \lambda_i \alpha_i$ for $\lambda_i \in K_1$ and using the fact that φ is a group homomorphism, we obtain

   $$\beta = \varphi(\alpha) = \varphi\left(\sum_{i=1}^n \lambda_i \alpha_i\right) = \sum_{i=1}^n \varphi(\lambda_i)\varphi(\alpha_i)$$

   and since $\varphi(\lambda_i) \in K_2$ by assumption and β is arbitrary, we have proven that $(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$ is a generating set.

   Now let $\mu_1, \ldots, \mu_n \in K_2$ and assume that $\sum_{i=1}^n \mu_i \varphi(\alpha_i) = 0$. Since $K_2 = \varphi(K_1)$, there exist $\lambda_1, \ldots, \lambda_n \in K_1$ such that $\varphi(\lambda_i) = \mu_i$ for all i. Hence, using the fact that φ is a field homomorphism, we obtain that

   $$0 = \sum_{i=1}^n \mu_i \varphi(\alpha_i) = \sum_{i=1}^n \varphi(\lambda_i)\varphi(\alpha_i) = \varphi\left(\sum_{i=1}^n \lambda_i \alpha_i\right),$$

   which by injectivity of φ implies that $\sum_{i=1}^n \lambda_i \alpha_i = 0$. As $\alpha_1, \ldots, \alpha_n$ are linear independent, we obtain that $\lambda_i = 0$ for each i, so that $\mu_i = \varphi(\lambda_i) = 0$ for each i. By arbitrarity of $\mu_1, \ldots, \mu_n$, we can conclude that the elements $\varphi(\alpha_1), \ldots, \varphi(\alpha_n) \in L_2$ are K_2-linear independent.

2. Let p be a prime number. By factoring $X^{p-1} - 1$ over $\mathbb{F}_p$, show that

   $$(p-1)! + 1 \equiv 0 \pmod{p}.$$

   Solution: For $p = 2$, the above equality is immediately checked. Therefore, we assume from now on that p is an odd prime number.

By Fermat's little theorem, each $x \in \mathbb{F}_p^\times$ satisfies $x^{p-1} = 1$, that is, x is a root of $X^{p-1} - 1 \in \mathbb{F}_p[X]$, so that $X - x | X^{p-1} - 1$. Since $\mathrm{card}(\mathbb{F}_p^\times) = p - 1 = \deg(X^{p-1} - 1)$ and $\mathbb{F}_p[X]$ is a UFD, we conclude that

$$X^{p-1} - 1 = \prod_{x \in \mathbb{F}_p^\times} (X - x).$$

Evaluating at $0 \in \mathbb{F}_p$, we obtain that $0 = 1 + (-1)^{p-1} \prod_{x \in \mathbb{F}_p^\times} x = 1 + \prod_{x \in \mathbb{F}_p^\times} x$. Since the representatives of the $x \in \mathbb{F}_p^\times$ can be taken to be $1, 2, \ldots, p-1$, we obtain the desired equality.

3. Let $f = X^3 - X + 1 \in \mathbb{F}_3[X]$.

   (a) Show that f is irreducible in $\mathbb{F}_3[X]$.

   (b) Show that if E is a splitting field and $\rho \in E$ is a root, then so are $\rho + 1$ and $\rho - 1$.

   (c) Construct a splitting field of f and write out its multiplication table.

   (d) Write down explicitly the action of $\mathrm{Gal}(E/\mathbb{F}_3)$ on the elements of E.

   Solution:

   (a) Since f has degree 3, it is reducible if and only if it has a linear factor in $\mathbb{F}_3[X]$, which is equivalent to having a root in $\mathbb{F}_3$. But $f(0) = f(1) = f(-1) = 1$ so that f has no root in $\mathbb{F}_3$. Hence f is irreducible in $\mathbb{F}_3[X]$.

   (b) Recall that $x \mapsto x^3$ is a field automorphism of K whenever K has characteristic 3, which is the identity on $\mathbb{F}_3$. In particular, it respects the sum. Then for $\varepsilon \in \mathbb{F}_3$ we compute

   $$f(\rho + \varepsilon) = (\rho + \varepsilon)^3 - (\rho + \varepsilon) + 1 = \rho^3 + \varepsilon^3 - \rho - \varepsilon + 1 = f(\rho) + \varepsilon - \varepsilon = 0.$$

   This implies that $\rho + 1$ and $\rho - 1$ are roots of f as well.

   (c) By b), any field extension E containing a root ρ of f contains three distinct roots of f, hence it contains all roots of f and it is the splitting field of f. Such an extension can be obtained as

   $$E = \mathbb{F}_3[X]/(f) \cong \{a + b\rho + c\rho^2 : a, b, c \in \mathbb{F}_3\},$$

   where the sum on the set on the right is done by adding the coefficients of $1, \rho, \rho^2$, while the product is induced by the bijection $\mathbb{F}_3[X]/(f) \cong \{a + b\rho + c\rho^2 : a, b, c \in \mathbb{F}_3\}$ sending $X \mapsto \rho$. That means that we can multiply two expressions on the right as if they were polynomial in ρ, and then simplify the obtained expression to one of "degree two" by using the condition $\rho^3 + \rho + 1 =$

0, i.e., $\rho^3 = -\rho - 1$, which gives $\rho^4 = \rho(-\rho-1) = -\rho^2 - \rho$ as well. Hence the multiplication rule of $\{a + b\rho + c\rho^2 : a, b, c \in \mathbb{F}_3\}$ is given by

$$\begin{aligned}
&(a + b\rho + c\rho^2)(a' + b'\rho + c'\rho^2) \\
&= aa' + (ab' + a'b)\rho + (ac' + bb' + ca')\rho^2 + (bc' + cb')\rho^3 + cc'\rho^4 \\
&= aa' - bc' - cb' + (ab' + a'b - bc' - cb' - cc')\rho + (ac' + bb' + ca' - cc')\rho^2.
\end{aligned}$$

(d) Using the same setup as in c), we write an element $x \in E$ as $x = a + b\rho + c\rho^2$ for $a, b, c \in \mathbb{F}_3$. Since E is the splitting field of $X^3 - X + 1 \in \mathbb{F}_3[X]$, the group $\mathrm{Gal}(E/\mathbb{F}_3)$ has $|E : \mathbb{F}_3| = 3$ elements. The image of $\sigma \in \mathrm{Gal}(E/\mathbb{F}_3)$ is uniquely determined by $\sigma(\rho)$, which must be one of the three roots of $X^3 - X + 1 \in \mathbb{F}_3[X]$, which are $\rho, \rho + 1, \rho - 1$. This means that, aside the identity, there are two automorphisms ρ_+ and ρ_- in $\mathrm{Gal}(E/\mathbb{F}_3)$ sending $\rho \mapsto \rho + 1$ and $\rho \mapsto \rho - 1$ respectively.
For a general element $a + b\rho + c\rho^2 \in E$, we can hence write

$$\begin{aligned}
\rho_+(a + b\rho + c\rho^2) &= a + b(\rho + 1) + c(\rho + 1)^2 = a + b + c + (b - c)\rho + c\rho^2 \\
\rho_-(a + b\rho + c\rho^2) &= a + b(\rho - 1) + c(\rho - 1)^2 = a - b + c + (b + c)\rho + c\rho^2.
\end{aligned}$$

4. Let p be a prime number.

(a) Show that an element of order p in S_p is a p-cycle.

(b) Show that a transposition and a p-cycle generated S_p.

Solution:

(a) Each $\sigma \in S_p$ can be decomposed into a product of disjoint cycles $\sigma_1, \dots, \sigma_n$ of lengths $\ell_1, \dots, \ell_n$ with $\sum_{i=1}^n \ell_i = p$. Since disjoint cycles commute, for each $k \in \mathbb{N}$ we get

$$\sigma^k = \sigma_1^k \cdots \sigma_n^k.$$

The permutations $\sigma_1^k, \dots, \sigma_n^k$ have disjoint support (that is, the elements permuted by σ_i and not permuted by σ_j for $i \neq j$), so that $\sigma^k = \mathrm{id}$ if and only if $\sigma_i^k = \mathrm{id}$ for each $i = 1, \dots, n$. As the order of σ_i (which, we recall, is a ℓ_i-cycle) is ℓ_i, we see that $\sigma^k = \mathrm{id}$ if and only if $\ell_i | k$ for each i. This means that $p = \mathrm{ord}(\sigma) = \mathrm{lcm}(\ell_1, \dots, \ell_n)$. As $\ell_i \leqslant p$ for every i, we see that $\ell_i \in \{1, p\}$ for each i and that one of the ℓ_i is p. As $\sum_{i=1}^n \ell_i = p$, the only possibility is $n = 1$ with $\ell_1 = p$, which is equivalent to saying that σ is a p-cycle.

(b) See Assignment 10, Exercise 7(b).