Solution 22

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 $(\alpha_1, \dots, \alpha_n)$ be a K_1-basis of L_1, so that $n = [L_1 : K_1]$. Since φ is injective, $(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$ consists of n different elements of L_2. We want to prove that $(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$ 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 $\lambda_i \in K_1$. 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 $(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$ is a generating set.

   Now let $\mu_1, \dots, \mu_n \in K_2$ and assume that $\sum_{i=1}^n \mu_i \varphi(\alpha_i) = 0$. Since $K_2 = \varphi(K_1)$, there exist $\lambda_1, \dots, \lambda_n \in K_1$ 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 $\sum_{i=1}^n \lambda_i \alpha_i = 0$. Since $\alpha_1, \dots, \alpha_n$ are linearly independent, we obtain $\lambda_i = 0$ for each i, and so $\mu_i = \varphi(\lambda_i) = 0$ for each i. We conclude that the elements $\varphi(\alpha_1), \dots, \varphi(\alpha_n) \in L_2$ are K_2-linearly 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. Assume 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 $X - x$ divides $X^{p-1} - 1$ in $\mathbb{F}_p[X]$. Since $\mathbb{F}_p[X]$ is a UFD and $\#\mathbb{F}_p^\times = p - 1 = \deg(X^{p-1} - 1)$, 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

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

4. Let $E/F/k$ be field extensions such that E/F and F/k are finite Galois extensions.
   (a) Give an example where the extension E/k is Galois.
   (b) Is E/k necessarily Galois? If not, provide a counterexample.

   Solution: Let $k = \mathbb{Q}$.

   (a) Set $F = \mathbb{Q}(\sqrt{2})$ and $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Then E/F is Galois because it is a degree 2 extension, and E/F is Galois because E is a splitting field of the polynomial

$$\begin{aligned}
&(X - i - \sqrt[4]{2})(X + i + \sqrt[4]{2})(X - i + \sqrt[4]{2})(X + i - \sqrt[4]{2})\\
&\qquad\qquad = X^4 + 2(1-\sqrt{2})X + 3 + 2\sqrt{2} \in F[X].
\end{aligned}$$

   The extension E/k is Galois because it is a splitting field of $X^4 - 2 \in k[X]$.

   (b) This is not true. Set, for example $E' = \mathbb{Q}(\sqrt[4]{2})$: The extensions E'/F and F/k are of degree 2, thus Galois. But E'/k is not, because E' does not contain all roots of the minimal polynomial $X^4 - 2$ of $\sqrt[4]{2}$ over k.