Galois theory - Problem Set 3 solutions

Solved on Thursday 07.03

Chapter 16.4

Problem 1. (Exercise 16.4.1 in the book.) If F is a finite field of characteristic p, show that each element α of F has a unique p-th root $\sqrt[p]{\alpha}$ in F.

Solution. Since F is a finite field of characteristic p, we may assume that $F = \mathrm{GF}(p^n)$ for some $n \geq 1$. Let $\alpha \in F$. If $\alpha = 0$, then $0^p = 0$ and for any other element $x \in F^* = F \setminus \{0\}$ we have $x^p \neq 0$ since F is a field. If $\alpha \neq 0$, then $\alpha^{p^n - 1} = 1$, since F^* is a multiplicative group with $p^n - 1$ elements. Then $\alpha^{p^n} = \alpha$. Let $\beta = \alpha^{p^{n-1}}$. Then

$$\beta^p = (\alpha^{p^{n-1}})^p = \alpha^{p^n} = \alpha,$$

and so β is a p-th root of α in F. Moreover it is unique since if $\gamma^p = \alpha$ for some element $\gamma \in F$, then

$$\gamma = \gamma^{p^n} = (\gamma^p)^{p^{n-1}} = \alpha^{p^{n-1}} = \beta.$$

Problem 2. (Exercise 16.4.3 in the book.) Find generators for the multiplicative groups of fields with 8, 13, and 17 elements.

Solution. Let $x \in \{8, 13, 17\}$ and $F = \mathrm{GF}(x)$, so that $|F^*| = x - 1$. Since F^* is a cyclic group by Theorem 10.11, we conclude that there are $\phi(x-1)$ generators of F^*, where ϕ is Euler's totient function.

If $x = 8$, then $|F^*| = 7$ is a prime number. Hence if $\alpha \in F^*$ with $\alpha \neq 1$, then $\langle \alpha \rangle = F^*$. Hence $\alpha \in F$ is a generator of the multiplicative group of F if and only if $\alpha \in F \setminus \{0, 1\}$.

If $x = 13$, then $|F^*| = 12$. Hence if $\alpha \in F^*$, then its order $o(\alpha)$ belongs to the set $\{1, 2, 3, 4, 6, 12\}$. We may identify F with $\mathbb{Z}_{13}$ and we compute

$$\begin{aligned}
\{\alpha \in \mathbb{Z}_{13}^* \mid o(\alpha) = 1\} &= \{1\}, \\
\{\alpha \in \mathbb{Z}_{13}^* \mid o(\alpha) = 2\} &= \{12\}, \\
\{\alpha \in \mathbb{Z}_{13}^* \mid o(\alpha) = 3\} &= \{3, 9\}, \\
\{\alpha \in \mathbb{Z}_{13}^* \mid o(\alpha) = 4\} &= \{5, 8\}, \\
\{\alpha \in \mathbb{Z}_{13}^* \mid o(\alpha) = 6\} &= \{4, 10\}, \\
\{\alpha \in \mathbb{Z}_{13}^* \mid o(\alpha) = 12\} &= \{2, 6, 7, 11\}.
\end{aligned}$$

Hence $\alpha \in F$ is a generator of the multiplicative group of F if and only if $\alpha \in \{2, 6, 7, 11\}$.

If $x = 17$, then $|F^*| = 16$. Hence if $\alpha \in F^*$, then its order $o(\alpha)$ belongs to the set $\{1, 2, 4, 8, 16\}$. We may identify F with $\mathbb{Z}_{16}$ and we compute

$$\begin{aligned}
\{\alpha \in \mathbb{Z}_{16}^* \mid o(\alpha) = 1\} &= \{1\}, \\
\{\alpha \in \mathbb{Z}_{16}^* \mid o(\alpha) = 2\} &= \{16\}, \\
\{\alpha \in \mathbb{Z}_{16}^* \mid o(\alpha) = 4\} &= \{4, 13\}, \\
\{\alpha \in \mathbb{Z}_{16}^* \mid o(\alpha) = 8\} &= \{2, 8, 9, 15\}, \\
\{\alpha \in \mathbb{Z}_{16}^* \mid o(\alpha) = 16\} &= \{3, 5, 6, 7, 10, 11, 12, 14\}.
\end{aligned}$$

Hence $\alpha \in F$ is a generator of the multiplicative group of F if and only if $\alpha \in \{3, 5, 6, 7, 10, 11, 12, 14\}$.

Problem 3. (Exam May 2013, Problem 7.) Let $[E : F] < \infty$ where E is an extension of the field F. (**Warning: I don't think that** $[E : F] < \infty$ **plays a role.)** If $M_1(\subseteq E)$ and $M_2(\subseteq E)$ are two normal extension of F show that M_1M_2 is a normal extension of F. (Here M_1M_2 denotes the subfield of E generated by M_1 and M_2.)

Solution. Let $K = M_1M_2 = F(M_1 \cup M_2)$. Let $\sigma : K \to \overline{F}$ be an F-embedding of K to $\overline{F}$. By Theorem 8.5 it is enough to show that $\sigma(K) \subseteq K$.

We have that $\sigma\big|_{M_1}$ is also an F-embedding of M_1 to $\overline{F}$. Since $F \subseteq M_1$ is normal, by Theorem 8.5 we have that $\sigma\big|_{M_1}(M_1) \subseteq M_1$. Similarly $\sigma\big|_{M_2}(M_2) \subseteq M_2$. Now let $\alpha \in K$. Since K is the field generated by $M_1 \cup M_2$ over F, an element $\alpha \in K$ is of the form

$$\alpha = (\alpha_1\beta_1 + \cdots + \alpha_k\beta_k)(\alpha_1'\beta_1' + \cdots + \alpha_m'\beta_m')^{-1}$$

for some $\alpha_i, \alpha_i' \in M_1$ and $\beta_i, \beta_i' \in M_2$. Since σ is a ring homomorphism, we have

$$\sigma(\alpha) = (\sigma(\alpha_1)\sigma(\beta_1) + \cdots + \sigma(\alpha_k)\sigma(\beta_k))(\sigma(\alpha_1')\sigma(\beta_1') + \cdots + \sigma(\alpha_m')\sigma(\beta_m'))^{-1}.$$

In particular, $\sigma\big|_{M_1}(M_1) \subseteq M_1$ implies that $\sigma(\alpha_i), \sigma(\alpha_i') \in M_1$. Similarly we have $\sigma(\beta_i), \sigma(\beta_i') \in M_2$. But then $\sigma(\alpha) \in F(M_1 \cup M_2) = K$. Hence $\sigma(K) \subseteq K$, as required.

Problem 4. (Exam May 2017, Problem 4.) Let $K_1 = F(\alpha)$ and $K_2 = F(\beta)$ be two finite and normal extensions of F. Show that $K = F(\alpha, \beta)$ is a finite and normal extension of F.

Solution. Since $F \subseteq F(\beta)$ is finite, it follows that it is algebraic. Hence β is algebraic over F. Similarly, α is algebraic over F. Then $F \subseteq F(\alpha, \beta)$ is a finitely generated extension and α and β are algebraic over F and so, by Theorem 5.8, it is a finite extension. On the other hand, we have $F \subseteq K_1 \subseteq F(\alpha, \beta)$ and $F \subseteq K_2 \subseteq F(\alpha, \beta)$ with $F \subseteq K_1$ normal and $F \subseteq K_2$ normal. By Problem 3 we have that $K_1K_2 = F(K_1 \cup K_2)$ is a normal extension of F. But clearly we have

$$F(K_1 \cup K_2) = F(F(\alpha) \cup F(\beta)) = F(\alpha, \beta) \tag{1}$$

and so $F(\alpha, \beta)$ is a normal extension of F.

(For a formal proof of (1), we can argue like this. As sets we have

$$F(\alpha) \cup F(\beta) \subseteq F(\alpha, \beta)$$

and so

$$F(F(\alpha) \cup F(\beta)) \subseteq F(F(\alpha, \beta)) = F(\alpha, \beta).$$

On the other hand, we have

$$\{\alpha, \beta\} \subseteq F(\alpha) \cup F(\beta)$$

and so

$$F(\alpha, \beta) \subseteq F(F(\alpha) \cup F(\beta)),$$

which shows the other inclusion.)

Problem 5. (Exercise 16.4.6 in the book.) If F is a field and $f : F \to F$ is a mapping defined by

$$f(x) = \begin{cases} x^{-1}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0, \end{cases}$$

show that f is an automorphism of F if and only if F has at most four elements.

Solution. Assume first that f is an automorphism of F. Let $x \in F \setminus \{0, -1\}$. Then $f(x) = x^{-1}$, $f(x + 1) = (x + 1)^{-1}$ and $f(1) = 1$. We have

$$(x + 1)^{-1} = f(x + 1) = f(x) + f(1) = x^{-1} + 1.$$

Hence for every $x \in F \setminus \{0, -1\}$, we have

$$x^{-1} + 1 = (x + 1)^{-1}.$$

Multiplying both sides by $x(x + 1)$ we obtain

$$x(x + 1)x^{-1} + x(x + 1) = x(x + 1)(x + 1)^{-1},$$

or after doing some calculation

$$x^2 + x + 1 = 0,$$

for every $x \in F \setminus \{0, 1\}$. But $x^2 + x + 1$ can have at most two roots in F, and so there can be at most two elements in $F \setminus \{0, 1\}$. Hence F can have at most 4 elements.

Assume now that F has at most four elements, that is, $F = \mathrm{GF}(2)$ or $F = \mathrm{GF}(4)$. If $F = \mathrm{GF}(2)$, then $f(x) = \mathrm{id}_F(x)$ is clearly an automorphism. If $F = \mathrm{GF}(4)$, then we may identify F with the field $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Indeed, $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$ (since it has no roots in $\mathbb{Z}_2$), and so if α is a root of $x^2 + x + 1$ in F, then $F = \mathbb{Z}_2(\alpha)$ and

$$[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = \deg(x^2 + x + 1) = 2.$$

Hence $\mathbb{Z}_2(a)$ has $2^2 = 4$ elements. Then $\alpha^2 + \alpha + 1 = 0$ in $\mathbb{Z}_2(\alpha)$ from which we obtain that $\alpha^{-1} = -(\alpha + 1) = \alpha + 1$ (since $\mathbb{Z}_2(\alpha)$ has characteristic 2). Hence $F = \{0, 1, \alpha, 1 + \alpha\}$ and $f(0) = 0$, $f(1) = 1$, $f(\alpha) = 1 + \alpha$, $f(1 + \alpha) = \alpha$. It follows that for all $x, y \in F$ we have $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ (using $\alpha^2 + \alpha + 1 = 0$) and so $f : F \to F$ is a ring homomorphism.

Problem 6. (Exercise 16.4.7 in the book.) Prove that in any finite field any element can be written as the sum of two squares.

Solution. Let $F = \mathrm{GF}(p^n)$ be a finite field where p is a prime number and $n \geq 1$. If $p = 2$, then for every $\alpha \in F^*$ we have $\alpha^{2^n - 1} = 1$. Hence for every $\alpha \in F$ we have $\alpha^{2^n} = \alpha$ (since this equation also holds for $\alpha = 0$). Hence $\alpha = (\alpha^{2^{n-1}})^2 + 0^2$ for every $\alpha \in F$.

Now assume that $p \geq 3$ and so p is odd. Consider the set

$$A = \{\alpha^2 \mid \alpha \in F\}.$$

The polynomial $x^2 - \alpha^2 \in F[x]$ has at most two roots, namely α and $-\alpha$. If $\alpha = -\alpha$, then $2\alpha = 0$ and since $p > 2$, we conclude that $\alpha = 0$. Hence the polynomial $x^2 - \alpha^2$ has exactly two roots if $\alpha \neq 0$ and exactly one root if $\alpha = 0$. Therefore the set A has

$$\frac{|F| - 1}{2} + 1 = \frac{p^n - 1}{2} + 1 = \frac{p^n + 1}{2}$$

elements. We may write

$$A = \{\alpha_1, \alpha_2, \ldots, \alpha_{\frac{p^n+1}{2}}\}.$$

Let $\alpha \in F$. Consider the set

$$B = \{\alpha - \alpha_i \mid 1 \leq i \leq \frac{p^n + 1}{2}\}.$$

Clearly B has also $\frac{p^n+1}{2}$ elements. Assume to a contradiction that $A \cap B = \varnothing$. Then

$$p^n = |F| \geq |A \cup B| = |A| + |B| = p^n + 1,$$

a contradiction. Hence there exists $\beta \in A \cap B$, so that $\beta = \alpha_i$ and $\beta = \alpha - \alpha_j$ for some $1 \leq i, j \leq \frac{p^n+1}{2}$. Then

$$\alpha_i = \beta = \alpha - \alpha_j$$

gives

$$\alpha = \alpha_i + \alpha_j.$$

Since $\alpha_i, \alpha_j \in A$, they are squares and so α is a sum of two squares. Since α was arbitrary, we are done.

Problem 7. (Exam May 2017, Problem 3(a)-(b).)

(a) Let F, N and K be fields such that $N = F(\alpha)$, $K = F(\beta)$, and let $p(x) \in F[x]$, $q(x) \in F[x]$ be the minimal polynomials of α and β, respectively, over F. Assume $\deg(p(x)) = 17$ and $\deg(q(x)) = 16$. Show that $[F(\alpha, \beta) : F] = 17 \cdot 16 = 272$.

(b) Let E be the splitting field of $f(x) = x^{17} - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. Determine $[E : \mathbb{Q}]$. Explain your argument.

Solution.

(a) Let m_β be the degree of the minimal polynomial of β over $F(\alpha)$. Since $q(x) \in F(\alpha)[x]$ and $q(\beta) = 0$, we have that $m_\beta \leq 16$. From $F \subseteq F(\alpha) \subseteq F(\alpha, \beta)$ we obtain

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = m_\beta \cdot 17.$$

Similarly let m_α be the degree of the minimal polynomial of α over $F(\beta)$. Similarly we get

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = m_\alpha \cdot 16.$$

Hence

$$m_\alpha \cdot 16 = m_\beta \cdot 17$$

gives that 16 divides m_β. But $m_\beta \leq 16$ implies $m_\beta = 16$ and so $[F(\alpha, \beta) : F] = m_\beta \cdot 17 = 16 \cdot 17 = 272$ as required.

(b) Let $\omega = e^{\frac{2\pi i}{17}}$ be a primitive 17-th root of unity. Then the roots of $f(x)$ in $\mathbb{C}$ are

$$\sqrt[17]{2}, \omega \sqrt[17]{2}, \omega^2 \sqrt[17]{2}, \ldots, \omega^{16} \sqrt[17]{2}.$$

Hence the splitting field of $f(x)$ is $\mathbb{Q}(\omega, \sqrt[17]{2})$. The polynomial $f(x)$ has $\sqrt[17]{2}$ as a root and is irreducible (Eisenstein for $x = 2$) and monic, and hence it is the minimal polynomial of $\sqrt[17]{2}$ over $\mathbb{Q}$. On the other hand

$$x^{17} - 1 = (x - 1)(1 + x + \cdots + x^{16}) = (x - 1)\Phi_{17}(x).$$

The polynomial $\Phi_{17}(x)$ has ω as a root (since ω is a root of $x^{17} - 1$ but not of $(x - 1)$), is irreducible by Example 3.11(2) and is monic and hence it is the minimal polynomial of ω over $\mathbb{Q}$. Hence we are in the situation of part (a) for $\alpha = \sqrt[17]{2}$ and $\beta = \omega$ and so $[E : \mathbb{Q}] = 17 \cdot 16 = 272$.

Problem 8. (Exam May 2013, Problem 5.)

(a) Let $F = \mathrm{GF}(2)(\alpha)$, where $\alpha^4 + \alpha + 1 = 0$. Determine $a, b, c, d \in \mathrm{GF}(2)$ such that

$$\frac{1}{\alpha} = a + b\alpha + c\alpha^2 + d\alpha^3.$$

(b) Let $f(x)$ be an irreducible polynomial over $\mathrm{GF}(p)$ where p is a prime. Show that $f(x)$ divides the polynomial $g(x) = x^{p^n} - x$ in $\mathrm{GF}(p)[x]$ if and only if $\deg(f(x))$ divides n.

Solution.

(a) We have $\alpha^4 + \alpha + 1 = 0$ and so

$$1 = -\alpha - \alpha^4 = \alpha(-1 - \alpha^3),$$

and since F has characteristic 2, we conclude that

$$\alpha^{-1} = -1 - \alpha^3 = 1 + \alpha^3.$$

Hence $a = 1$, $b = 0$, $c = 0$, $d = 1$.

(b) Let $F = \mathrm{GF}(p)$ and let $f(x) \in F[x]$ be irreducible of degree d. Let E be a splitting field of $g(x)$ over F. By Theorem 10.6 we have that E has p^n elements and so

$$[E : F] = n.$$

Assume first that $f(x)$ divides $g(x) = x^{p^n} - x$. Every root of $g(x)$ exists in E. In particular, every root of $f(x)$ exists in E since $f(x)$ divides $g(x)$. Let $\alpha \in E$ be a root of $f(x)$. Then $F \subseteq F(\alpha) \subseteq E$ and $[F(\alpha) : F] = \deg(f(x)) = d$ since $f(x)$ is irreducible. We obtain

$$n = [E : F] = [E : F(\alpha)][F(\alpha) : F] = [E : F(\alpha)]d,$$

and so $d = \deg(f(x))$ divides n.

For the other direction assume that d divides n. Since $f(x)$ is irreducible, the quotient ring $K = F[x]/(f(x))$ is a field extension of F. Moreover, we have $[K : F] = \deg(f(x)) = d$. Hence K has p^d elements and so for every $\alpha \in K$ we have $\alpha^{p^d} = \alpha$. We claim that $\alpha^{p^{dk}} = \alpha$ for all $\alpha \in K$ and $k \geq 1$. We show this by induction. The base case $k = 1$ is clear, while for the induction step we have

$$\alpha^{p^{dk}} = \left(\alpha^{p^{d(k-1)}}\right)^{p^d} = \alpha^{p^d} = \alpha,$$

where the penultimate equality follows by the induction assumption. Now, since d divides n we have that $n = dm$ for some $m \in \mathbb{Z} \geq 1$. Then $\alpha^{p^n} = \alpha^{p^{dm}} = \alpha$ for every $\alpha \in K$. In particular, every element in K is a root of $g(x)$. Let $\beta = x + (f(x)) \in K$. Then β is a root of $f(x)$ and a root of $g(x)$. But since $f(x)$ is irreducible in $GF(p)[x]$, it follows that $f(x)$ divides $g(x)$ in $GF(p)[x]$.

Problem 9. (Exercise 16.4.9 in the book.) Show that $x^p - x - 1$ is irreducible over $\mathbb{Z}_p$. Let K be the splitting field of degree p over $\mathbb{Z}_p$. Show that $K = \mathbb{Z}_p(\omega)$, where ω is a root of $x^p - x - 1$. For $p \in \{2, 3, 5\}$ show that the order of ω in the group $K \setminus \{0\}$ is $1 + p + p^2 + \cdots + p^{p-1}$.

Solution. Let $\omega \in \overline{\mathbb{Z}_p}$ be a root of $f(x) = x^p - x - 1$ in the algebraic closure of $\mathbb{Z}_p$. Then for any $a \in \mathbb{Z}_p$ we have

$$f(\omega + a) = (\omega + a)^p - (\omega + a) - 1 = \omega^p + a^p - \omega - a - 1 = f(\omega) + a^p - a = 0,$$

since $f(\omega) = 0$ and since $a^p = a(\mod p)$ by Fermat's little theorem. Hence $\omega + a$ is a root of $f(x)$ for every $a \in \mathbb{Z}_p$. In particular, we have that $\omega \notin \mathbb{Z}_p$, since $0 = \omega + (-\omega)$ is not a root of $f(x)$. Since the set

$$S = \{\omega, \omega + 1, \ldots, \omega + p - 1\}$$

has p elements and $\deg(f(x)) = p$, we conclude that S is the set of roots of $f(x)$. Thus

$$f(x) = \prod_{0 \leq k \leq p-1} (x - (\omega + k)) \tag{2}$$

in $\overline{\mathbb{Z}_p}$. Now assume to a contradiction that $f(x)$ is not irreducible over $\mathbb{Z}_p$. Then $f(x) = p(x)q(x)$ with $\deg(p(x)) \geq 1$ and $\deg(q(x)) \geq 1$. In particular, there exist $k_1, k_2, \ldots, k_t \in \mathbb{Z}_p$ such that

$$p(x) = (x - (\omega + k_1))(x - (\omega + k_2)) \cdots (x - (\omega + k_t)).$$

But then

$$p(x) = x^t - [(\omega + k_1) + (\omega + k_2) + \cdots + (\omega + k_t)]x^{t-1} + \text{lower degree terms}$$

and so

$$(\omega + k_1) + (\omega + k_2) + \cdots + (\omega + k_t) = t\omega + \sum_{i=1}^{t} k_i \in \mathbb{Z}_p.$$

Since $\sum_{i=1}^{t} k_i \in \mathbb{Z}_p$ we obtain that $t\omega \in \mathbb{Z}_p$. But since $\omega \notin \mathbb{Z}_p$ and $p \geq t = \deg(p(x)) \geq 1$, we conclude that $t = p$. But then

$$\deg(f(x)) = \deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = p + \deg(q(x)) \geq p + 1,$$

a contradiction. So $p(x)$ is irreducible over $\mathbb{Z}_p$. Since $S \subseteq \mathbb{Z}_p(\omega)$, and since $f(x)$ factors into linear factors in $\mathbb{Z}_p(\omega)$, it follows that the splitting field of $f(x)$ is $K = \mathbb{Z}_p(\omega)$.

Now we claim that for $0 \leq k \leq p-1$ we have

$$\omega^{p^k} = \omega + k \tag{3}$$

We use induction on k. For $k = 0$ the claim is true. Assume the claim is true for k and we show it for $k+1 \leq p-1$. We have

$$\omega^{p^{k+1}} = (\omega^{p^k})^p = (\omega + k)^p$$

using the induction step. But $\omega + k \in S$ is a root of $f(x)$ and so $(\omega + k)^p = \omega + k + 1$. Hence

$$\omega^{p^{k+1}} = \omega + (k+1),$$

as claimed.

Using $\omega^{p^k} = \omega + k$ we compute

$$\omega^{1+p+p^2+\cdots+p^{p^{p-1}}} = \omega\omega^p\omega^{p^2}\cdots\omega^{p^{p-1}} = \omega(\omega+1)(\omega+2)\cdots(\omega+p-1).$$

But by (2) we have that the constant term of $f(x)$ is

$$-\omega(-(\omega+1))(-(\omega+2))\cdots(-(\omega+p-1) = -\omega(\omega+1)\cdots(\omega+p-1),$$

where the sign follows since there are p terms (if p is odd, then there is an odd number of terms, while if $p = 2$ then $-1 = 1$). Since the constant term of $f(x)$ is -1, we obtain that

$$\omega(\omega+1)\cdots(\omega+p-1) = 1,$$

and so

$$\omega^{1+p+p^2+\cdots+p^{p^{p-1}}} = 1.$$

Hence the order of ω divides $1 + p + p^2 + \cdots + p^{p^{p-1}}$ (and clearly is not 1).

If $p = 2$, then the order of ω divides $1 + p^{2^{2-1}} = 1 + 2 = 3$. Since 3 is prime, the order of ω in this case is 3.

If $p = 3$, then the order of ω divides $1 + p + p^{3^{3-1}} = 1 + 3 + 9 = 13$. Since 13 is prime, the order of ω in this case is 13.

If $p = 5$, then the order of ω divides $1 + p + p^2 + p^3 + p^{5^{5-1}} = 1 + 5 + 25 + 125 + 625 = 781$. Since $781 = 11 \cdot 71$, it is enough to show that $\omega^{11} \neq 1$ and $\omega^{71} \neq 1$. Assume to a contradiction that $\omega^{11} = 1$. Recall by (3) that $\omega^5 = \omega + 1$. Then

$$1 = \omega^{11} = \omega\omega^5\omega^5 = \omega(\omega+1)^2 = \omega^3 + 2\omega^2 + \omega,$$

or $\omega^3 + 2\omega^2 + \omega - 1 = 0$. But this contradicts the fact that $\{1, \omega, \omega^2, \omega^3, \omega^4\}$ are linearly independent over $\mathbb{Z}_p$. Hence $\omega^{11} \neq 1$. Now assume to a contradiction that $\omega^{71} = 1$. Recall by (3) that $\omega^{25} = \omega + 2$. Then

$$\begin{aligned} 1 = \omega^{71} &= \omega^{-4}\omega^{75} = \omega^{-4}\omega^{25}\omega^{25}\omega^{25} = \omega^{-4}(\omega+2)^3 = \omega^{-4}(\omega^3 + 6\omega^2 + 12\omega + 8) \\ &= \omega^{-4}(\omega^3 + \omega^2 + 2\omega + 3) = \omega^{-1} + \omega^{-2} + 2\omega^{-3} + 3\omega^{-4} \end{aligned}$$

and so by multiplying both sides by ω^4 we obtain

$$\omega^4 = \omega^3 + \omega^2 + 2\omega + 3,$$

which again contradicts the fact that $\{1, \omega, \omega^2, \omega^3, \omega^4\}$ are linearly independent over $\mathbb{Z}_p$. Hence in this case the order of ω is neither 11 nor 71 and so it is 781.

Chapter 16.5

Problem 10. (Exercise 16.5.5 in the book.) Prove that a finite extension of a finite field is separable.

Solution. Let F be a finite field and $F \subseteq E$ be a finite extension. Since $F \subseteq E$ is finite, it follows that $F \subseteq E$ is algebraic. Let $\alpha \in E$ and let $f(x)$ be the minimal polynomial of α over F. Then $f(x)$ is irreducible and so by Theorem 10.15 all of its roots are simple. Hence $f(x)$ is separable and so α is separable over F. Since $\alpha \in E$ was arbitrary, we conclude that $F \subseteq E$ is a separable extension.

Problem 11. (Exercise 16.5.7 in the book.) Let α be a root of $x^p - x - 1$ over a field F of characteristic p. Show that $F(\alpha)$ is a separable extension of F.

Solution. By Example 11.5 it is enough to show that α is separable over F. Let $p(x)$ be the minimal polynomial of α over F. Then $p(x) \mid f(x) = x^p - x - 1$. Hence to show that $p(x)$ is separable, it is enough to show that $x^p - x - 1$ does not have multiple roots. Let β be a root of $f(x)$ with multiplicity m_β. Then $1 \leq m_\beta \leq p$. If $m_\beta = p$, then

$$x^p - x - 1 = f(x) = (x - \beta)^p = x^p - \beta^p$$

gives a contradiction. Hence $m_\beta < p$. Therefore by Theorem 9.3 we have that m_β is equal to the smallest number k such that $f^{(k)}(\beta) \neq 0$. But notice that $f'(x) = px^{p-1} - 1 = -1 \neq 0$, and so $k = 1 = m_\beta$. Hence every root of $f(x)$ is simple, as required.

Problem 12. (Exercise 16.5.2 in the book generalized.) Let p, q be prime numbers and let $a, b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Show that $\mathbb{Q}(a\sqrt{p} + b\sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Solution. If $p = q$ then the claim is clear. If $p \neq q$ we claim that $a\sqrt{p} + b\sqrt{q}$ is not zero. Indeed, assuming otherwise we obtain $a^2 p = b^2 q$ and so $p \mid b$ and $q \mid a$. Then $b = p^{k_p} r$ for some $k_p \geq 1$ such that p does not divide r. Similarly $a = q^{k_q} s$ for some $k_q \geq 1$ such that q does not divide s. Then $a^2 p = b^2 q$ gives

$$q^{2k_q} s^2 p = p^{2k_p} r^2 q,$$

or

$$q^{2k_q - 1} s^2 = p^{2k_p - 1} r^2.$$

But this is impossible since the right hand side has an odd number of factors of p while the left hand side can only have an even amount of factors (since p does not divide q).

Now we have $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ and so $a\sqrt{p} + b\sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Hence $\mathbb{Q}(a\sqrt{p} + b\sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$. It remains to show that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{Q}(a\sqrt{p} + b\sqrt{q})$. In particular, it is enough to show that $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})$. We have

$$(a\sqrt{p} + b\sqrt{q})(a\sqrt{p} - b\sqrt{q}) = a^2 p - b^2 q.$$

And since $a\sqrt{p} + b\sqrt{q} \neq 0$, we have that

$$a\sqrt{p} - b\sqrt{q} = \underbrace{(a^2 p - b^2 q)}_{\in \mathbb{Q}} \underbrace{(a\sqrt{p} + b\sqrt{q})^{-1}}_{\in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})} \in \mathbb{Q}(a\sqrt{p} + b\sqrt{q}).$$

Then

$$a\sqrt{p} = \frac{1}{2}\left(\underbrace{a\sqrt{p} + b\sqrt{q}}_{\in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})} + \underbrace{a\sqrt{p} - b\sqrt{q}}_{\in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})} \right)$$

and so $a\sqrt{p} \in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})$, and so $\sqrt{p} = a^{-1} a\sqrt{p} \in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})$. Then

$$b\sqrt{q} = \underbrace{a\sqrt{p} + b\sqrt{q}}_{\in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})} - \underbrace{a\sqrt{p}}_{\in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})}$$

and so $\sqrt{q} \in \mathbb{Q}(a\sqrt{p} + b\sqrt{q})$ as well.

Problem 13. Show that there exists an $s \in \mathbb{C}$ such that $\mathbb{Q}\left(\sqrt{5}, e^{\frac{2\pi i}{2018}}, \sqrt[3]{1+\sqrt[4]{7}}\right) = \mathbb{Q}(s)$.

Solution. Let us write $\alpha = \sqrt{5}$, $\beta = e^{\frac{2\pi i}{2018}}$ and $\gamma = \sqrt[3]{1+\sqrt[4]{7}}$. Then α is algebraic over $\mathbb{Q}$ since it is a root of $q_\alpha(x) = x^2 - 5 \in \mathbb{Q}[x]$, β is algebraic over $\mathbb{Q}$ since it is a root of $q_\beta(x) = x^{2018} - 1 \in \mathbb{Q}[x]$ and to see whether γ is also algebraic over $\mathbb{Q}$ we have

$$\gamma^3 = 1 + \sqrt[4]{7} \implies (\gamma^3 - 1) = \sqrt[4]{7} \implies (\gamma^3 - 1)^4 = 7 \implies \gamma^{12} - 4\gamma^9 + 6\gamma^6 - 4\gamma^3 - 6 = 0,$$

and so γ is also algebraic over $\mathbb{Q}$ since it is a root of $q_\gamma(x) = x^{12} - 4x^9 + 6x^6 - 4x^3 - 6 \in \mathbb{Q}[x]$. In particular, we have that

$$[\mathbb{Q}(\alpha,\beta,\gamma) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta,\gamma) : \mathbb{Q}(\alpha,\beta)][\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq \deg(q_\gamma)\deg(q_\beta)\deg(q_\alpha)$$

$$= 12 \cdot 2018 \cdot 2 = 48432 < \infty,$$

and so the field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha,\beta,\gamma)$ is algebraic. Since $\mathrm{char}(\mathbb{Q}) = 0$, it follows by Remark 10.16 that the field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha,\beta,\gamma)$ is separable. As it is also finite, it follows by Theorem 11.3 that it is simple, as required.

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 14. (Chapter 16.4) Find a field F and a field embedding $\phi : F \to F$ such that $[F : \phi(F)] \neq 1$.

Solution. Consider the field

$$F \coloneqq \mathbb{Q}(t) = \left\{ \frac{p(t)}{q(t)} \mid p(t), q(t) \in \mathbb{Q}[t], q(t) \neq 0 \right\},$$

with standard addition and multiplication. Let $\phi : F \to F$ be the field embedding defined by

$$\phi\left(\frac{p(t)}{q(t)}\right) = \frac{p(t^2)}{q(t^2)}.$$

Then

$$\phi(F) = \mathbb{Q}(t^2) = \left\{ \frac{p(t^2)}{q(t^2)} \mid p(t), q(t) \in \mathbb{Q}[t], q(t) \neq 0 \right\},$$

and so clearly $\phi(F) \neq F$. Hence $[F : \phi(F)] \neq 1$. In fact, we have

$$F = \mathbb{Q}(t) = \mathbb{Q}(t^2)(t) = \phi(F)(t),$$

and the irreducible polynomial of t over $\phi(F)$ is $f(x) = x^2 - t^2$ of degree 2. Hence $[F : \phi(F)] = 2$.

Problem 15. (Chapter 16.5) Let $F \subseteq E$ be a field extension such that $[E : F] = 2$. For every possible characteristic of F, determine whether $F \subseteq E$ is separable (i.e. prove that it is separable or provide a counterexample.)

Solution. Since $[E : F] < \infty$, the extension $F \subseteq E$ is algebraic. Let $\alpha \in E$ and let $f(x)$ be the minimal polynomial of α over F. If $\alpha \notin F$, then $F \subseteq F(\alpha) \subseteq E$ and $[E : F] = 2$ implies that $[F(\alpha) : F] = 2$. Hence $\deg(f(x)) = 2$ and so $f(x) = x^2 + ax + b$ with $a, b \in F$. We have $f'(x) = 2x + a$. If $\mathrm{char}(F) \neq 2$, then $f'(\alpha) = 2\alpha + a \neq 0$ (since $\alpha \notin F$). Hence in this case by Theorem 9.3 we conclude that α is a simple root of $f(x)$ and so the other root of $f(x)$ is also simple. Hence α is separable over F and so, in the case $\mathrm{char}(F) \neq 2$, the extension $F \subseteq E$ is separable.

Assume now that $\mathrm{char}(F) = 2$. Let $F = \mathrm{GF}(2)(t)$ and let $f(x) = x^2 - t \in F[x]$. We claim that $f(x)$ is irreducible. To show this it is enough to show that it has no roots in F, that is, that there exist no polynomials $p(t), q(t) \in \mathrm{GF}(2)[t]$ such that

$$\left(\frac{p(t)}{q(t)}\right)^2 - t = 0.$$

But this follows by the Solution of Problem 9 in Problem Set 2. Hence $f(x)$ is irreducible. Let α be a root of $f(x)$ in $\overline{F}$. Then $F \subseteq F(\alpha)$ is an extension of degree 2 since $f(x)$ is the minimal polynomial of α over F. But $\alpha^2 - t = 0$ and the fact that $\mathrm{char}(F) = 2$ imply that

$$(x - \alpha)^2 = x^2 - \alpha^2 = x^2 - t = f(x)$$

and so α is not a simple root of $f(x)$. Hence the extension $F \subseteq F(\alpha)$ is not separable.