Galois theory - Problem Set 3

To be 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.

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

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 $M_1 M_2$ is a normal extension of F. (Here $M_1 M_2$ denotes the subfield of E generated by M_1 and M_2.)

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.

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.

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.

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.

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.

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

Chapter 16.5

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

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.

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 $\mathbb{Q}(a\sqrt{p} + b\sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

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

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 $[F : \phi(F)] \neq 1$.

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.)