Solutions Exercise sheet 7

1. Let $L : K$ be a splitting field of a separable polynomial $f(x) \in K[x]$ of degree n. Show that if f is irreducible then n divides $|\text{Gal}(L : K)|$.

Solution:

Let $\alpha \in$ be a root of f. Since f is irreducible, $[K(\alpha) : K] = n$. On the other hand since $L : K$ is a splitting field of f, $|\text{Gal}(L : K)| = [L : K]$. Together with $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ this implies $n||\text{Gal}(L : K)|$.

2. Let p be a prime and $\mathbb{F}_{p^n}$ be the finite field of p^n elements. Show that $\text{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and a generator is given by the Frobenius homomrphism $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ where $\varphi(x) = x^p$.

Solution:

We have seen that $\mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^x} - x$. Hence using Theorem 3.5 we have that $|\text{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Clearly the Frobenius homomorphism is in $\text{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$. We claim that the order of φ is equal to n. Suppose its order is $k \leqslant n$. Then $\varphi^k = \text{Id}_{\mathbb{F}_{p^n}}$. Since $\varphi^k(x) = x^{p^k}$, this means that every $x \in \mathbb{F}_{p^n}$ satisfies $x^{p^k} - x = 0$ Hence $p^n \leqslant p^k$ which in return implies that $k = n$.

3. For $p^r = 8, 9, 16$ find the minimal polynomial over $\mathbb{F}_p$ of a generator of $\mathbb{F}_{p^r}^\times$.

Solution: Let $p^r = 8$. By checking that none of the elements in $\mathbb{F}_2$ are a zero of $X^3 + X + 1$, we conclude that the polynomial is irreducible over $\mathbb{F}_2$, as it has degree 3.

Since $X^3 + X + 1$ is an irreducible polynomial of degree 3 over $\mathbb{F}_2$, $\mathbb{F}_8 \cong \mathbb{F}_2[X]/(X^3 + X + 1)$ follows. In addition, $\mathbb{F}_8^\times$ is cyclic of order 7, so every element different from 1 is a generating element. For example, we can choose the image of X in $\mathbb{F}_2[X]/(X^3 + X + 1)$ as a generating element. Its minimal polynomial is then $X^3 + X + 1$.

Let $p^r = 9$. Then $\mathbb{F}_9$ is isomorphic to $\mathbb{F}_3[X]/(X^2 + 1)$, since $X^2 + 1$ is an irreducible polynomial of degree 2 over $\mathbb{F}_3$. A $\mathbb{F}_3$-basis of $\mathbb{F}_9$ is therefore $\{1, a\}$ with $a^2 = -1$. Since $\mathbb{F}_9^\times$ is cyclic of order 8, we are looking for an element of order 8. The elements of orders 1, 2 and 4 are 1, -1 and $\pm a$ respectively. Thus, for example, $a + 1$ can only have the order 8. (We can also calculate this directly using $(a + 1)^2 = 2a$ and $(a + 1)^4 = (2a)^2 = -4 = -1 \neq 1$). Because $(a + 1)^2 + (a + 1) - 1 = 0$ and $a + 1 \notin \mathbb{F}_3$, $X^2 + X - 1$ is the minimal polynomial of $a + 1$ over $\mathbb{F}_3$.

Let $p^r = 16$. The polynomial $X^4 + X + 1$ is irreducible of degree 4 over $\mathbb{F}_2$: checking all zeros in $\mathbb{F}_2$ shows that there are no linear factors. The only irreducible polynomial of degree 2 in $\mathbb{F}_2[X]$ is $X^2 + X + 1$, and since $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq X^4 + X + 1$, we obtain that $X^4 + X + 1$ is irreducible over $\mathbb{F}_2$.

Hence $\mathbb{F}_{16} = \mathbb{F}_2(a)$ for an element a with minimal polynomial $X^4 + X + 1$ over $\mathbb{F}_2$. Since $\mathbb{F}_{16}^\times$ is cyclic of order $16 - 1 = 3 \cdot 5$, a itself is a generator unless $a^3 = 1$ or $a^5 = 1$. In this case, a would be a zero of $X^3 - 1$ or $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$, whereas, for degree reasons, the degrees of each of these polynomials is coprime to the degree of the irreducible polynomial $X^4 + X + 1$. So this cannot be the case, and a is a generator of $\mathbb{F}_{16}^\times$ with the minimum polynomial $X^4 + X + 1$.

4. Let n be a positive integer. Let p be a prime number and let K be a finite field of order p^n. Prove:

(a) If $p = 2$, then each element of K is a square. (*Hint:* Consider the Frobenius homomorphism)

(b) Each element of K can be written as a sum of two squares.

(c) For $p > 2$, we have that -1 is a square in K if and only if $p^n \equiv 1 \pmod 4$.

Solution:

(a) For $p = 2$ consider the Frobenius endomorphism $\mathrm{Frob}_p : x \mapsto x^2$ on the finite field K. Since any finite field extension over a finite field is separable, Frob_p is injective. Since k is finite, it is moreover bijective, and we obtain our claim.

(b) Let $Q := \{a^2 \mid a \in K\}$ be the set of all squares in K. This is the union of $\{0\}$ with the image of the homomorphism $K^\times \to K^\times$, $x \mapsto x^2$. The kernel of this homomorphism is $\{\pm 1\}$ and therefore has order $\leqslant 2$. The image of the homomorphism therefore has order $\geqslant \frac{p^n-1}{2}$. Thus $|Q| \geqslant \frac{p^n+1}{2}$ applies.

For each $x \in K$ now consider the set $x - Q := \{x - q \mid q \in Q\}$. For this, $|x - Q| \geqslant \frac{p^n+1}{2}$ applies again, and we obtain

$$|Q \cap (x-Q)| \;=\; |Q| + |x-Q| - |Q \cup (x-Q)| \;\geqslant\; \tfrac{p^n+1}{2} + \tfrac{p^n+1}{2} - |K| \;\geqslant\; 1.$$

So $Q \cap (x - Q)$ is not empty. Thus $a, b \in K$ exist with $b^2 = x - a^2$, or in other words $x = a^2 + b^2$.

(c) Because $p > 2$, $-1 \neq 1$ is an element of K, and because $(-1)^2 = 1$, -1 is an element of order 2 in $K^\times$. Now, $K^\times$ is cyclic of order $p^n - 1$ and therefore isomorphic to $\mathbb{Z}/(p^n-1)\mathbb{Z}$. Moreover, the element $-1 \in K^\times$ corresponds to the residue class $[\frac{p^n-1}{2}] \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ for every isomorphism. Thus -1 is a square in K if and only if $[\frac{p^n-1}{2}] \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ is a multiple of 2. This is the case if $\frac{p^n-1}{2}$ is even, i.e. if $p^n \equiv 1 \mod 4$.

5. Let $p > 2$ be a prime number. Prove that p can be written as a sum of two squares in $\mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$.

Hint: Look at the prime factorization of p in $\mathbb{Z}[i]$. See also Exercise sheet 1, question 3.

Solution: We already know that $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z} \cdot i$, and according to Exercise sheet 1, this is a Euclidean ring with multiplicative norm function $N(a + bi) := a^2 + b^2$. In particular, it is factorial. Furthermore, the following holds:

$$\mathbb{Z}[i]^\times \;=\; \{x \in \mathbb{Z}[i] \mid N(x) = 1\} \;=\; \{\pm 1, \pm i\}.$$

First let $p \equiv 1 \pmod 4$. According to exercise **4**. (c) above, $-1 \in \mathbb{F}_p^\times$ is a square. Therefore $c \in \mathbb{Z}$ exists with $p|(c^2+1)$. On the other hand, $c \pm i \notin p \cdot \mathbb{Z}[i]$ and therefore $p \nmid (c \pm i)$. Because $c^2+1 = (c+i)(c-i)$, p is not a prime element in $\mathbb{Z}[i]$. Since it is also not a unit and $\mathbb{Z}[i]$ is factorial, p therefore has a prime factorization of length > 1.

Write $p = ef$ with non-units $e, f \in \mathbb{Z}[i]$. Then $N(e) \cdot N(f) = N(ef) = N(p) = p^2$ and $N(e), N(f) > 1$, which is only possible with $N(e) = p$. If we write $e = a+bi$ with $a, b \in \mathbb{Z}$, we now get $p = N(e) = a^2 + b^2$, so p is a sum of two squares as desired.

Now let $p \equiv 3 \pmod 4$. According to Exercise sheet 1, p is then prime in $\mathbb{Z}[i]$. If there existed $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, then $(a+ib)(a-ib) = p$ would be a factorization of p. Since $N(a+ib) = N(a-ib) = p$ would apply, both factors would not be units, which yields a contradiction.