Solutions of exercise sheet 13

The content of the marked exercises **(*)** should be known for the exam.

1. 1. Show that the polynomial
$$P = X^3 + 3X + 3$$
is irreducible in $\mathbb{F}_5[X]$.

2. Let α be a root of P in an algebraic closure L of $\mathbb{F}_5$, and $\mathbb{F}_{125} = \mathbb{F}_5(\alpha)$. Compute the matrix of the Frobenius automorphism $\phi : \mathbb{F}_{125} \to \mathbb{F}_{125}$ in the basis $(1, \alpha, \alpha^2)$.
3. Write the element
$$\beta = \frac{1}{1-\alpha} \in \mathbb{F}_{125}$$
as an $\mathbb{F}_5$-linear combination of 1, α and α^2.
4. Prove that α is a generator of the cyclic group $\mathbb{F}_{125}^\times$.

Solution: In the following, we will denote elements of $\mathbb{F}_5$ just with integer numbers, so that $5 = 0$.

1. Since the polynomial $P \in \mathbb{F}_5[X]$ has degree 3, every proper decomposition of P has a linear factor, which means that P is irreducible if and only if it has no root in $\mathbb{F}_5$. Since $P(0) = 3$, $P(1) = 2$, $P(2) = 2$, $P(3) = 4$ and $P(4) = 4$, we obtain that P has no root in $\mathbb{F}_5$, so that it is irreducible in $\mathbb{F}_5$.
2. Since α is a root of P, we have
$$\alpha^3 = -3\alpha - 3 = 2(\alpha+1) \text{ and}$$
$$(\alpha+1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 3(\alpha^2+1),$$
which implies in particular that
$$\alpha^9 = -\alpha^2 - 1.$$
To compute the matrix of $\phi : x \mapsto x^5$ with respect to the basis $(1, \alpha, \alpha^2)$, where α is a root of P, we write down the images of 1, α and α^2 as $\mathbb{F}_5$-linear combinations of 1, α and α^2. We get the following:
$$\begin{aligned}\phi(1) &= 1\\ \phi(\alpha) &= \alpha^5 = \alpha^2 \cdot 2 \cdot (\alpha+1) = 2\alpha^3 + 2\alpha^2 = -1 - \alpha + 2\alpha^2\\ \phi(\alpha^2) &= \alpha \cdot \alpha^9 = -\alpha^3 - \alpha = -2 + 2\alpha\end{aligned}$$

Please turn over!

Then the matrix associated to ϕ with respect to the basis $(1, \alpha, \alpha^2)$ is

$$M_\phi = \begin{pmatrix} 1 & -1 & -2 \\ 0 & -1 & 2 \\ 0 & 2 & 0 \end{pmatrix}.$$

3. Suppose that $\beta = \lambda + \mu\alpha + \nu\alpha^2$ for $\lambda, \mu, \nu \in \mathbb{F}_5$. Then the condition $1 = \beta(1-\alpha)$ gives

$$1 = \lambda + (\mu - \lambda)\alpha + (\nu - \mu)\alpha^2 - \nu\alpha^3 = \lambda + 3\nu + (3\nu + \mu - \lambda)\alpha + (\nu - \mu)\alpha^2,$$

which is equivalent to

$$\begin{cases} \lambda + 3\nu = 1 \\ 3\nu + \mu - \lambda = 0 \\ \nu - \mu = 0 \end{cases}.$$

Solving the equations backwards we obtain $\mu = \nu$, $\lambda = 4\nu$ and $7\nu = 1$, so that the unique solution is $(\lambda, \mu, \nu) = (2, 3, 3)$, and $\beta = 2 + 3\alpha + 3\alpha^2$.

4. We have that $|\mathbb{F}_{125}^\times| = 124 = 4 \cdot 31$, and by Lagrange's theorem applied to the subgroup $\langle \alpha \rangle$ we see that the order of α is a divisor of 124. We want to prove that indeed $\mathrm{ord}_{\mathbb{F}_{125}^\times}(\alpha) = 124$, and this can be done by checking that α^4 and α^{62} both differ from 1, since every proper divisor of 124 divides either 4 or 62. Of course, $\alpha^4 = 2(\alpha^2 + \alpha) \neq 1$, so that we are left to check that $\alpha^{62} \neq 1$. We have

$$\alpha^{62} = \alpha^{-1}(\alpha^9)^7 = -\alpha^{-1}(\alpha^2 + 1)^7.$$

To proceed with the computation, notice that

$$\begin{aligned} (\alpha^2+1)^3 &= \alpha^6 + 3\alpha^4 + 3\alpha^2 + 1 = 4(\alpha+1)^2 + \alpha^2 + \alpha + 3\alpha^2 + 1 = 3\alpha^2 - \alpha, \\ (\alpha^2+1)^6 &= (3\alpha^2 - \alpha)^2 = -\alpha^4 - \alpha^3 + \alpha^2 = -\alpha^2 + \alpha - 2 \text{ and} \\ (\alpha^2+1)^7 &= (-\alpha^2 + \alpha - 2)(\alpha^2 + 1) = -\alpha^4 - \alpha^2 + \alpha^3 + \alpha - 2\alpha^2 - 2 = \alpha. \end{aligned}$$

Then

$$\alpha^{62} = -\alpha^{-1}\alpha = -1 \neq 1,$$

and we can conclude that α generates $\mathbb{F}_{125}^\times$.

2. Let p be an odd prime number, and denote by $\left(\frac{x}{p}\right)$ the Legendre symbol for $x \in \mathbb{F}_p^\times$.

1. Prove that

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} (\mathrm{mod}\ p),$$

and that this determines $\left(\frac{x}{p}\right) \in \{\pm 1\}$ uniquely.

2. Prove that the map $\mathbb{F}_p^\times \to \mathbb{C}^\times$ sending $x \mapsto \left(\frac{x}{p}\right)$ is a group homomorphism.

See next page!

3. Prove that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.
4. Let $s = (p-1)/2$. Prove that

$$s! \equiv 2^s s! (-1)^{\frac{s(s+1)}{2}} \pmod p.$$

[*Hint:* $s! = (-1)^{\frac{s(s+1)}{2}} \prod_{j=1}^{s} (-1)^j j$, and $-j \equiv p - j \pmod p$.]
5. Deduce that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

and find for which equivalence classes of p modulo 8 we have $\left(\frac{2}{p}\right) = 1$.
6. Find congruence conditions on p that are equivalent to 13 being a square modulo p.
7. Deduce that if $p \equiv 6 \pmod{13}$ is a prime number, then there exist only finitely many $n \in \mathbb{Z}_{>0}$ such that $n! + n^p - n + 13$ is a square in $\mathbb{Z}$.

Solution:

1. As seen in class, we have that for each $a \in \mathbb{F}_p$ one has $a^p = a$, so that for each $a \in \mathbb{F}_p^\times$ one has $a^{p-1} = 1$. This means that $\mathbb{F}_p^\times$ is the set of roots of the polynomial $f_p(X) = X^{p-1} - 1$. This polynomials factors (since $2|p-1$) as

$$f_p(X) = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1).$$

Suppose that $c \in \mathbb{F}_p^{\times 2}$, with $c = b^2$ and $b \neq 0$. Then

$$c^{\frac{p-1}{2}} = b^{p-1} = 1,$$

so that c is a root of the factor $(X^{\frac{p-1}{2}} - 1)$. As we have seen in Exercise 4.2 from Exercise sheet 12, $|\mathbb{F}_p^{\times 2}| = (p-1)/2$, and this implies that the for each $x \in \mathbb{F}_p^\times$ one has

$$\left(\frac{x}{p}\right) = 1 \iff x \in \mathbb{F}_p^{\times 2} \iff x^{\frac{p-1}{2}} = 1,$$
$$\left(\frac{x}{p}\right) = -1 \iff x \notin \mathbb{F}_p^{\times 2} \iff x^{\frac{p-1}{2}} = -1.$$

In both cases, we have that

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod p.$$

This of course determines uniquely the value of $\left(\frac{x}{p}\right)$ as p is odd so that $1 \neq -1$ in $\mathbb{F}_p$.
2. This follows immediately from the previous point, as for $x, y \in \mathbb{F}_p^\times$, one has $(xy)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} y^{\frac{p-1}{2}}$.

Please turn over!

3. Applying point 1 with $x = 1$, we have that $\left(\frac{-1}{p}\right) = 1$ if and only if $(p-1)/2$ is even, and this, considering that p is odd - so that $p \equiv 1$ or $p \equiv 3 \pmod 4$ - is easily seen to happen precisely when $p \equiv 1 \pmod 4$.
4. We have

$$\begin{aligned} s! &= \prod_{j=1}^{s}(-1)^j \prod_{j=1}^{s}(-1)^j j = (-1)^{\sum_{j=1}^{s} j} \prod_{k=1}^{\lfloor \frac{s}{2} \rfloor}(2k) \prod_{k=1}^{\lceil \frac{s}{2} \rceil}(-(2k-1)) \equiv \\ &\equiv (-1)^{\frac{s(s+1)}{2}} \prod_{k=1}^{\lfloor \frac{s}{2} \rfloor}(2k) \prod_{k=1}^{\lceil \frac{s}{2} \rceil}(p-2k+1). \end{aligned}$$

Notice that the factors in the two products are distinct positive even (since p is odd) integers which are strictly smaller than p. There is a total of $\lfloor \frac{s}{2} \rfloor + \lceil \frac{s}{2} \rceil = s = (p-1)/2$ factors in the product, so that we can conclude that those factors are the numbers $2, 4, \ldots, p-1$. Hence

$$s! \equiv (-1)^{\frac{s(s+1)}{2}} \prod_{j=1}^{s}(2j) = (-1)^{\frac{s(s+1)}{2}} 2^s \prod_{j=1}^{s} j = (-1)^{\frac{s(s+1)}{2}} 2^s s!,$$

which is exactly the equivalence modulo p that we wanted to prove.
5. From the previous point we have $s = (p-1)/2 < p$, and $p \nmid s!$, so that $s!$ is invertible modulo p and the equivalence we proved implies (considering that $s(s+1)/2 = (p^2-1)/8$) that

$$1 \equiv 2^s(-1)^{\frac{p^2-1}{8}} \pmod p,$$

which is equivalent to

$$2^s \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

Now we apply Point 1, which gives

$$\left(\frac{2}{p}\right) \equiv 2^s \equiv (-1)^{\frac{p^2-1}{8}}.$$

We have that $\left(\frac{2}{p}\right) = 1$ if and only if $\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8}$ is even, and this happens if and only if either $p+1$ or $p-1$ is divisible by 8, which is equivalent to saying that $p \equiv \pm 1 \pmod 8$. So we can write

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

6. Of course, if $p = 13$ we have that $13 = 0$ in $\mathbb{F}_p$, which is a square. Hence we will exclude this case. Then $13 \in \mathbb{F}_p^\times$, and we want to determine $\left(\frac{13}{p}\right)$. By the quadratic reciprocity law, we have

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) \cdot (-1)^{\frac{p-1}{2}\frac{13-1}{2}} = \left(\frac{p}{13}\right),$$

See next page!

so that we just need to find the squares in $\mathbb{F}_{13}$. In $\mathbb{F}_{13}$, one has

$$(\pm 1)^2 = 1,\ (\pm 2)^2 = 4,\ (\pm 3)^2 = -4,\ (\pm 4)^2 = 3,\ (\pm 5)^2 = -1,\ (\pm 6)^2 = -3.$$

In conclusion, we have that 13 is a square if $\mathbb{F}_p$ if and only if p is congruent to $0, \pm 1, \pm 3$ or ± 4 modulo 13.

7. Let $\gamma_p(n) := n! + n^p - n + 13$. If $\gamma_p(n)$ is a square in $\mathbb{Z}$, then it is a square also modulo p. For $n \geq p$, we have that $p|n!$, and that $n^p \equiv n$ by Fermat's little theorem. Hence for $n \geq p$ we get $\gamma_p(n) \equiv 13 \pmod p$, which by the previous point is not a square when $p \equiv 6 \pmod{13}$. Hence $\gamma_p(n)$ is not a square in $\mathbb{Z}$ for $n \geq p$. In particular, $\gamma_p(n)$ is a square for only finitely many values of n.

3. (*) Let K be a field of characteristic $p > 0$, containing $\mathbb{F}_p$. Let $a \in K$.

1. Show that the polynomial $f = X^p - X - a$ is separable in $K[X]$.
2. Show that if L is an algebraically closed extension of K and $\alpha \in L$ is a root of f, then
$$\{\text{roots of } f \text{ in } L\} = \{\alpha + x, x \in \mathbb{F}_p\}.$$
3. Show that if $a \notin \{y^p - y : y \in K\}$, then $K(\alpha)$ has degree p over K. What happens if $a = y^p - y$ for some $y \in K$?
4. Show that, when $K \neq K(\alpha)$, the set of field automorphisms of $K(\alpha)$ which fix all elements in K, endowed with composition, is a group, and that it is cyclic of order p.
5. Find a polynomial $Q_p \in \mathbb{F}_p[X]$ which defines $\mathbb{F}_{p^p}$, in the sense that $\mathbb{F}_{p^p} = \mathbb{F}_p(\alpha)$ for some root α of Q_p in an algebraic closure of $\mathbb{F}_p$.

Solution:

1. We have that $f'(X) = pX^{p-1} - 1 = -1$, so that f and f' are necessarily coprime in $K[X]$ and f is separable by a Criterion seen in class.
2. Suppose $\alpha \in L$ is a root of f. Since raising to the p-th power (i.e., computing the Frobenius automorphism) respects the sums, for $x \in \mathbb{F}_p$ we get
$$f(\alpha + x) = (\alpha + x)^p - (\alpha + x) - a = f(\alpha) + x^p - x = 0,$$
since $x^p = x$ for $x \in \mathbb{F}_p$ and α is a root of f. Since $|\alpha + \mathbb{F}_p| = p = \deg(f)$, there cannot be other roots, and we can conclude that
$$\{\text{roots of } f \text{ in } L\} = \{\alpha + x, x \in \mathbb{F}_p\}.$$
3. We start from the easy case: if $a = y^p - y$ for some $y \in K$, then $\alpha = y \in K$ is a root of f, and $\alpha + \mathbb{F}_p = \mathbb{F}_p \subseteq K$, so that any root of f is indeed in K. This means that $K(\alpha) = K$ in this case.

Please turn over!

Now assume that $a \notin \{y^p - y : y \in K\}$. Then all the roots $\alpha + x$ of f lie outside K, and we claim that f is irreducible. This claim implies then that $K(\alpha) \cong K[X]/(f(X))$, so that $K(\alpha)$ has degree p over K. To prove our claim, by previous point we have that f factors in $L[X]$ as

$$f(X) = \prod_{x \in \mathbb{F}_p} (X - \alpha - x),$$

so that if $f = gh$ in $K[X]$, unique factorization in $L[X]$ gives that g is, up to a multiplicative constant,

$$g = \prod_{x \in I} (X - \alpha - x),$$

where $I \subseteq \mathbb{F}_p$. Let $d = |I| = \deg(g)$, and suppose that $d > 0$ (else, the factorization is trivial and we are done). Then the coefficient of g of the term of degree $d-1$ is $-\sum_{x \in I}(\alpha + x) = -d\alpha + \sum_{x \in I} x$. This coefficient needs to lie in K, and since $\sum_{x \in I} x \in \mathbb{F}_p \subseteq K$, we get $-d\alpha \in K$. But $\alpha \notin K$, so that the unique remaining possibility is that $d = p$, in which case the decomposition $f = gh$ is trivial. This proves that f is irreducible, which was the remaining claim.

4. If $K \neq K(\alpha)$, by previous point we get that $K(\alpha)$ is a degree-p extension of K. Let us denote by $\mathrm{Aut}_K(K(\alpha))$ the set of field automorphisms of $K(\alpha)$ which fix K. It is clearly a group with respect to composition since automorphism are invertible and the identity $\mathrm{id}_{K(\alpha)}$ fixes K. Notice that any endomorphism of $K(\alpha)$ is injective as $K(\alpha)$ is a field. Moreover, if such an endomorphism fixes K, then it is also a K-linear map $K(\alpha) \to K(\alpha)$, and since those are K-vector spaces of same dimension p, we can conclude that every endomorphism of $K(\alpha)$ fixing K is an automorphism. Hence $\mathrm{Aut}_K(K(\alpha))$ coincides with the sets of endomorphisms of $K(\alpha)$ fixing K. We have that $K(\alpha) \cong K[X]/(X^p - X - 1)$, with $\alpha \leftrightarrow X$, so that to determine a ring homomorphism $K(\alpha) \to K(\alpha)$ fixing K is equivalent to choosing an image for α in $K(\alpha)$ which still satisfies the polynomial $X^p - X - 1$. By Point 2, this means that

$$\mathrm{Aut}_K(K(\alpha)) = \{\gamma : K(\alpha) \to K(\alpha) : \gamma|_K = \mathrm{id}_K, \gamma(\alpha) = \alpha + x, x \in \mathbb{F}_p\}.$$

Hence there are $|\mathbb{F}_p| = p$ elements in $\mathrm{Aut}_K(K(\alpha))$, and this implies automatically that $\mathrm{Aut}_K(K(\alpha))$ is a cyclic group.

5. By Point 3, we just need to take an element $a \notin \{y^p - y : y \in \mathbb{F}_p\}$. Since $y^p - y = 0$ for every $y \in \mathbb{F}_p$, we can just take $a = 1$, so that Q_p is a separable irreducible polynomial, and so it defines $\mathbb{F}_{p^p}$ as an extension of $\mathbb{F}_p$.