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 $\mathbb{F}_{125}^\times$.

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

Please turn over!

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 $\mathbb{Z}$.

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 $\mathbb{F}_p$.

Due to: 18 December 2014, 3 pm.