Exercise sheet 4

p-adic numbers

Exercise 1. Let p be an odd prime.

(1) Using the Hensel lemma, show that any element $v \in \mathbb{Q}_p^\times$, written in the form $v = p^r u$ with $r \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$, is a square if and only if r is prime and u is a square modulo p.

(2) Deduce an isomorphism $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

(3) Show that $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

(4) What are the quadratic extensions of $\mathbb{Q}_p$?

Exercise 2. Let p be an odd prime. Show that the roots of units of $\mathbb{Q}_p$ are the $p-1$ roots of the polynomial $X^{p-1} - 1$.

Finite fields

Exercise 3. (1) Show that $X^2 + X + 1$ is irreducible over $\mathbb{F}_5$.

(2) Let $P \in \mathbb{F}_5[X]$ be a unitary irreducible polynomial of degree 2. Show that the quotient ring $\mathbb{F}_5[X]/(P)$ is isomorphic to the field $\mathbb{F}_{25}$ and that P has two roots in $\mathbb{F}_{25}$.

(3) Let α be a root of $X^2 + X + 1$ in $\mathbb{F}_{25}$. Show that every element of $\mathbb{F}_{25}$ is of the form $x\alpha + y$ with $x, y \in \mathbb{F}_5$.

(4) Let $P = X^5 - X + 1$. Show that P is irreducible over $\mathbb{F}_5$. Is it irreducible over $\mathbb{Q}$?

Exercise 4. Consider the polynomials $Q(X) = X^9 - X + 1$ and $P(X) = X^3 - X - 1$ with coefficients in $\mathbb{F}_3$.

(1) Show that Q has no root in $\mathbb{F}_3$, nor in $\mathbb{F}_9$.

(2) Show that $\mathbb{F}_3[X]/(P)$ is isomorphic to $\mathbb{F}_{27}$.

(3) Show that every root $\alpha \in \mathbb{F}_{27}$ of P is also a root of Q.

(4) Determine all the roots of Q in $\mathbb{F}_{27}$.

(5) Factor the polynomial Q over $\mathbb{F}_3$.

Exercise 5. (1) Give all the polynomials over $\mathbb{F}_2$ of degree at most 4.

(2) What is the factorization over $\mathbb{F}_4$ of an irreducible polynomial $\mathbb{F}_2[X]$ of degree 4 ?

(3) Deduce the number of unitary irreducible polynomials of degree 2 over $\mathbb{F}_4$. Then list them all.

Exercise 6. Let $n \in \mathbb{N}$ be a nonzero natural number.

(1) Let $P \in \mathbb{F}_p[X]$ be a polynomial of degree n and let m be a natural number. Give a necessary and sufficient condition for P to be irreducible over $\mathbb{F}_{p^m}$. In the case where P is irreducible over $\mathbb{F}_p$, precise the possible degrees of the irreducible factors of P over $\mathbb{F}_{p^m}$.

(2) What is the minimal m such that every polynomial of degree n with coefficients in $\mathbb{F}_p$ splits over (respectively admits a root in) $\mathbb{F}_{p^m}$.

Exercise 7. Show that $X^4 + 1$ is irreducible over $\mathbb{Z}$ and reducible modulo all primes.

Exercise 8. Consider the polynomial $P = X^3 + 2X + 1$ and the ring $K = \mathbb{F}_3[X]/(P)$. Show that K is a field of cardinal 27 and that X is a generator of the multiplicative group $K^\times$. Find an integer k such that $X^2 + X = X^k$.

Exercise 9 (Cyclotomic polynomials). Let p be a prime number and $n \in \mathbb{N}^*$ be an integer coprime with p. Let d denote the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.

(1) Show that $\Phi_{n,\mathbb{F}_p}$ is the product of $\varphi(n)/d$ irreducible factors of degree d.

(2) Deduce that this polynomial is irreducible if and only if p generates $(\mathbb{Z}/n\mathbb{Z})^\times$.

(3) Assume that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. Show that there exists infinitely many primes ℓ such that $\Phi_{n,\mathbb{F}_\ell}$ is irreducible.
Hint. *You can use* Dirichlet's theorem on arithmetic progressions *: for every positive coprime integers n and a, there exists infinitely primes congruent to a modulo n.*

Exercise 10 (Eisenstein's criterion). Let $P(X) = a_n X^n + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Z}$ and let p be a prime number such that

(1) p does not divide a_n,

(2) for all $i \in \{0, \ldots, n-1\}$, p divide a_i,

(3) p^2 does not divide a_0.

Show that P is irreducible over $\mathbb{Q}$.
Application. For q prime, show that Φ_q is irreducible over $\mathbb{Q}$.