

Exercise sheet n°1

**Exercise 1 – (Legendre symbol)** Let  $p \geq 3$  be an odd prime number. For  $a \not\equiv 0 \pmod{p}$ , we consider the congruence

$$X^2 \equiv a \pmod{p}.$$

We say that  $a$  is a quadratic residue modulo  $p$  if the above congruence has a solution. Otherwise we say that  $a$  is a quadratic nonresidue. Let  $\bar{a}$  denote the class of  $a$  in  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . Note that  $a$  is a quadratic residue modulo  $p$  if and only if the polynôme  $X^2 - \bar{a}$  has a root in  $\mathbb{F}_p$ . The Legendre symbol is defined as follows :

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{otherwise} \end{cases}$$

Sometimes one also sets  $\left(\frac{a}{p}\right) = 0$  if  $a \equiv 0 \pmod{p}$ , but this convention will not be used in the exercices below.

- 1) Show that the polynomial  $X^{p-1} - \bar{1}$  has  $p-1$  distinct roots in  $\mathbb{F}_p$ .
- 2) Show that there exist exactly  $\frac{p-1}{2}$  classes of residues and  $\frac{p-1}{2}$  classes of nonresidues modulo  $p$ .
- 3) Show that  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .
- 4) Show that  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$  for all  $a, b \not\equiv 0 \pmod{p}$ .

**Exercise 2 – (Gauss' lemma)** We keep notation and conventions of Exercise 1. Set  $R = \{1, 2, \dots, \frac{p-1}{2}\}$ . Let  $a \not\equiv 0 \pmod{p}$ .

- 1) Show that for each integer  $i \in R$  there exist a unique  $r_i \in R$  and  $\varepsilon_i \in \{1, -1\}$  such that  $a \cdot i \equiv \varepsilon_i r_i \pmod{p}$ . Show that  $r_i \neq r_j$  if  $i \neq j$ .
- 2) Show that  $a^{\frac{p-1}{2}} \equiv \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \pmod{p}$  and deduce the formula  $\left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i$ .
- 3) Show that  $\varepsilon_i = (-1)^{\left[\frac{2ai}{p}\right]}$ , where  $[x]$  denotes the floor function (the biggest integer less than or equal to  $x$ ). (Hint : write the Euclidian division  $ai = pb_i + c_i$ . Then  $\varepsilon_i = 1$  if  $1 \leq c_i < p/2$  and  $\varepsilon_i = -1$  if  $p/2 \leq c_i \leq p-1$ . Write

$$\left[\frac{2ai}{p}\right] = 2 \left[\frac{ai}{p}\right] + \left[2 \left\{\frac{ai}{p}\right\}\right],$$

where  $\{x\}$  denotes the fractional part of  $x$ .)

- 4) Deduce the formula

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{2ai}{p}\right]}.$$

**Exercice 3 – (Gauss' quadratic reciprocity law)** We keep notation and conventions of Exercises 1 and 2.

- 1) Assume that  $a$  is odd. Show that  $\left(\frac{2a}{p}\right) = \left(\frac{(a+p)/2}{p}\right)$  and deduce the formula

$$\left(\frac{2a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ai}{p}\right] + \frac{p^2-1}{8}}.$$

- 2) Show that

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

- 3) Let  $p$  and  $q$  be two distinct odd prime numbers. Let

$$S = \{(pj, qi) \mid 1 \leq j \leq \frac{q-1}{2}, 1 \leq i \leq \frac{p-1}{2}\}.$$

Set  $S_1 = \{(pj, qi) \in S \mid pj < qi\}$  and  $S_2 = \{(pj, qi) \in S \mid pj > qi\}$ . Show that  $S$  is the disjoint union of  $S_1$  and  $S_2$  and that

$$\text{card}(S_1) = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right], \quad \text{card}(S_2) = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right].$$

- 4) Show that  $\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$

**Exercice 4 –** Let  $p$  be an odd prime number. Show that 3 is a quadratic residue modulo  $p$  if and only if  $p \equiv \pm 1 \pmod{12}$ .

**Exercice 5 – (Roots in  $\mathbb{Z}_p$ )** Let  $p$  be a prime number such that  $p \nmid m$ .

- 1) Assume that the congruence  $x^m \equiv a \pmod{p}$  has a solution  $x_0$ . Show that for any  $n \geq 1$  there exists  $x_n \in \mathbb{Z}$  such that  $x_n^m \equiv a \pmod{p^{n+1}}$  and  $x_n \equiv x_0 \pmod{p}$ . Show that  $x_n$  is unique modulo  $p^{n+1}$ . Deduce that the equation  $X^m = a$  has a unique solution  $x \in \mathbb{Z}_p$  such that  $x \equiv x_0 \pmod{p}$ .
- 2) Show that  $\mathbb{Z}_p$  contains  $p-1$  distinct  $(p-1)$ th roots of unity.

**Exercice 6 – (The ring of formal power series)** Let  $k$  be a field and let  $k[[X]] = \{f = \sum_{n=0}^{\infty} a_n X^n \mid a_n \in k\}$ . Then  $k[[X]]$  is equipped with a natural structure of a commutative unitary ring.

- 1) Show that  $f = \sum_{i=0}^{\infty} a_i X^i$  is invertible if and only if  $a_0 \neq 0$ .
- 2) Show that each nonzero  $f \in k[[X]]$  can be written in a unique way in the form  $f = X^n u$  with  $u \in k[[X]]^*$ .
- 3) Show that  $k[[X]]$  is an integral domain and that its field of fractions is isomorphic to the field of Laurent power series

$$k((X)) = \{f = \sum_{i=i_0}^{\infty} a_i X^i \mid i_0 \in \mathbb{Z}, a_i \in k\}.$$

- 4) Show that each nonzero  $f \in k((X))$  can be written in a unique way in the form  $f = X^n u$  with  $n \in \mathbb{Z}$  and  $u \in k[[X]]^*$ . Set  $v_X(f) = n$ . Show that  $v_X$  is a discrete valuation on  $k((X))$  and that  $k[[X]]$  is the associated DVR.

**Exercise 7** – Show that the following rings are not discrete valuation rings :

$$\mathbf{Z}; \quad k[[X^2, X^3]].$$

**Exercise 8** – Let  $A$  be a local noetherian ring such that its maximal ideal  $\mathfrak{m}$  is generated by a non-nilpotent element  $\pi$ . The goal of this exercise is to prove that  $A$  is a principal ideal domain.

- 1) Verify that  $I = \{x \in A \mid \exists m \in \mathbf{N} : \pi^m x = 0\}$  is an ideal of  $A$  and that there exists  $N \in \mathbf{N}$  such that  $\pi^N I = \{0\}$ .
- 2) Show that  $\bigcap_{n \geq 1} \mathfrak{m}^n = \{0\}$ . Hint : if  $y = \pi^n x_n$  for every  $n \in \mathbf{N}$ , then the chain of ideals  $(I + x_n A)_{n \in \mathbf{N}}$  is ascending.
- 3) Prove that any element  $y \in A \setminus \{0\}$  can be written in a unique way in the form  $y = \pi^{v(y)} u$  with  $v(y) \in \mathbf{N}$  and  $u \in A^*$ , and that  $A$  is an integral domain.