J.-P. Serre

A Course in Arithmetic

J.-P. Serre

A Course in Arithmetic

Springer-Verlag New York · Heidelberg · Berlin

Jean-Pierre Serre
Professor of Algebra and Geometry, Collège de France, Paris

Title of the French Original Edition: Cours d' Arithmétique
Publisher: Presses Universitaires de France, Paris 1970.

AMS Subject Classification (1970)
10 B 05, 10 C 05, 10 C 20, 10 D 05, 10 H 10, 10 J 05, 30 A 16

Library of Congress Catalog Card Number 70-190089.

Printed in the United States of America.

ISBN 0-387-90041-1 Springer-Verlag New York Heidelberg Berlin (soft cover)
ISBN 0-387-90040-3 Springer-Verlag New York Heidelberg Berlin (hard cover)
ISBN 3-540-90041-1 Springer-Verlag Berlin Heidelberg New York (soft cover)

Preface

This book is divided into two parts.

The first one is purely algebraic. Its objective is the classification of quadratic forms over the field of rational numbers (Hasse-Minkowski theorem). It is achieved in Chapter IV. The first three chapters contain some preliminaries: quadratic reciprocity law, p-adic fields, Hilbert symbols. Chapter V applies the preceding results to integral quadratic forms of discriminant ± 1. These forms occur in various questions: modular functions, differential topology, finite groups.

The second part (Chapters VI and VII) uses "analytic" methods (holomorphic functions). Chapter VI gives the proof of the "theorem on arithmetic progressions" due to Dirichlet; this theorem is used at a critical point in the first part (Chapter III, no. 2.2). Chapter VII deals with modular forms, and in particular, with theta functions. Some of the quadratic forms of Chapter V reappear here.

The two parts correspond to lectures given in 1962 and 1964 to second year students at the Ecole Normale Supérieure. A redaction of these lectures in the form of duplicated notes, was made by J.-J. Sansuc (Chapters I–IV) and J.-P. Ramis and G. Ruget (Chapters VI–VII). They were very useful to me; I extend here my gratitude to their authors.

J.-P. Serre

Table of Contents

Part I

Algebraic Methods

Chapter I

Finite Fields

All fields considered below are supposed commutative.

§1. *Generalities*

1.1. *Finite fields*

Let K be a field. The image of $\mathbf{Z}$ in K is an integral domain, hence isomorphic to $\mathbf{Z}$ or to $\mathbf{Z}/p\mathbf{Z}$, where p is prime; its field of fractions is isomorphic to $\mathbf{Q}$ or to $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. In the first case, one says that K is of *characteristic zero*; in the second case, that K is of *characteristic p*.

The characteristic of K is denoted by char(K). If char(K) $= p \neq 0$, p is also the smallest integer $n>0$ such that $n.1 = 0$.

Lemma.—*If* char(K) $= p$, *the map* $\sigma\colon x \mapsto x^p$ *is an isomorphism of* K *onto one of its subfields* K^p.

We have $\sigma(xy) = \sigma(x)\sigma(y)$. Moreover, the binomial coefficient $\binom{p}{k}$ is congruent to 0 (mod p) if $0<k<p$. From this it follows that

$$\sigma(x+y) = \sigma(x)+\sigma(y);$$

hence σ is a homomorphism. Furthermore, σ is clearly injective.

Theorem 1.—i) *The characteristic of a finite field* K *is a prime number* $p \neq 0$; *if* $f = [K\colon\mathbf{F}_p]$, *the number of elements of* K *is* $q = p^f$.

ii) *Let* p *be a prime number and let* $q = p^f (f \geqq 1)$ *be a power of* p. *Let* Ω *be an algebraically closed field of characteristic* p. *There exists a unique subfield* $\mathbf{F}_q$ *of* Ω *which has* q *elements. It is the set of roots of the polynomial* $X^q - X$.

iii) *All finite fields with* $q = p^f$ *elements are isomorphic to* $\mathbf{F}_q$.

If K is finite, it does not contain the field $\mathbf{Q}$. Hence its characteristic is a prime number p. If f is the degree of the extension $K/\mathbf{F}_p$, it is clear that Card(K) $= p^f$, and i) follows.

On the other hand, if Ω is algebraically closed of characteristic p, the above lemma shows that the map $x \mapsto x^q$ (where $q = p^f$, $f \geqq 1$) is an automorphism of Ω; indeed, this map is the $f-$th iterate of the automorphism $\sigma\colon x \mapsto x^p$ (note that σ is surjective since Ω is algebraically closed). Therefore, the elements $x \in \Omega$ invariant by $x \mapsto x^q$ form a subfield $\mathbf{F}_q$ of Ω. The derivative of the polynomial $X^q - X$ is

$$qX^{q-1} - 1 = p.p^{f-1}X^{q-1} - 1 = -1$$

and is not zero. This implies (since Ω is algebraically closed) that $X^q - X$ has q distinct roots, hence $\text{Card}(\mathbf{F}_q) = q$. Conversely, if K is a subfield of Ω with q elements, the multiplicative group K^* of nonzero elements in K has $q-1$ elements. Then $x^{q-1} = 1$ if $x \in K^*$ and $x^q = x$ if $x \in K$. This proves that K is contained in $\mathbf{F}_q$. Since $\text{Card}(K) = \text{Card}(\mathbf{F}_q)$ we have $K = \mathbf{F}_q$ which completes the proof of ii).

Assertion iii) follows from ii) and from the fact that all fields with p^f elements can be embedded in Ω since Ω is algebraically closed.

1.2. *The multiplicative group of a finite field*

Let p be a prime number, let f be an integer $\geqq 1$, and let $q = p^f$.

Theorem 2.—*The multiplicative group $\mathbf{F}_q^*$ of a finite field $\mathbf{F}_q$ is cyclic of order $q-1$.*

Proof. If d is an integer $\geqq 1$, recall that $\phi(d)$ denotes the *Euler ϕ-function,* i.e. the number of integers x with $1 \leqq x \leqq d$ which are prime to d (in other words, whose image in $\mathbf{Z}/d\mathbf{Z}$ is a generator of this group). It is clear that the number of generators of a cyclic group of order d is $\phi(d)$.

Lemma 1.—*If n is an integer $\geqq 1$, then $n = \sum_{d|n} \phi(d)$.* (Recall that the notation $d|n$ means that d divides n).

If d divides n, let C_d be the unique subgroup of $\mathbf{Z}/n\mathbf{Z}$ of order d, and let Φ_d be the set of generators of C_d. Since all elements of $\mathbf{Z}/n\mathbf{Z}$ generate one of the C_d, the group $\mathbf{Z}/n\mathbf{Z}$ is the disjoint union of the Φ_d and we have

$$n = \text{Card}(\mathbf{Z}/n\mathbf{Z}) = \sum_{d|n} \text{Card}(\Phi_d) = \sum_{d|n} \phi(d).$$

Lemma 2.—*Let H be a finite group of order n. Suppose that, for all divisors d of n, the set of $x \in H$ such that $x^d = 1$ has at most d elements. Then H is cyclic.*

Let d be a divisor of n. If there exists $x \in H$ of order d, the subgroup $(x) = \{1, x, \ldots, x^{d-1}\}$ generated by x is cyclic of order d; in view of the hypothesis, all elements $y \in H$ such that $y^d = 1$ belong to (x). In particular, all elements of H of order d are generators of (x) and these are in number $\phi(d)$. Hence, the number of elements of H of order d is 0 or $\phi(d)$. If it were zero for a value of d, the formula $n = \sum_{d|n} \phi(d)$ would show that the number of elements in H is $<n$, contrary to hypothesis. In particular, there exists an element $x \in H$ of order n and H coincides with the cyclic group (x).

Theorem 2 follows from lemma 2 applied to $H = \mathbf{F}_q^*$ and $n = q-1$; it is indeed obvious that the equation $x^d = 1$, which has degree d, has at most d solutions in $\mathbf{F}_q$.

Remark. The above proof shows more generally that all finite subgroups of the multiplicative group of a field are cyclic.

§2. Equations over a finite field

Let q be a power of a prime number p, and let K be a field with q elements.

2.1. *Power sums*

Lemma.—*Let u be an integer >0. The sum $S(X^u) = \sum_{x \in K} x^u$ is equal to -1 if u is $\geqq 1$ and divisible by $q-1$; it is equal to 0 otherwise.*

(We agree that $x^u = 1$ if $u = 0$ *even if* $x = 0$.)

If $u = 0$, all the terms of the sum are equal to 1; hence $S(X^u) = q.1 = 0$ because K is of characteristic p.

If u is $\geqq 1$ and divisible by $q-1$, we have $0^u = 0$ and $x^u = 1$ if $x \neq 0$. Hence $S(X^u) = (q-1).1 = -1$.

Finally, if u is $\geqq 1$ and not divisible by $q-1$, the fact that K^* is cyclic of order $q-1$(th. 2) shows that there exists $y \in K^*$ such that $y^u \neq 1$. One has:

$$S(X^u) = \sum_{x \in K^*} x^u = \sum_{x \in K^*} y^u x^u = y^u S(X^u)$$

and $(1-y^u)S(X^u) = 0$ which implies that $S(X^u) = 0$.

(*Variant*—Use the fact that, if $d \geqq 2$ is prime to p, the sum of the d-th roots of unity is zero.)

2.2. *Chevalley theorem*

Theorem 3 (Chevalley–Warning).—*Let $f_\alpha \in K[X_1, \ldots, X_n]$ be polynomials in n variables such that $\sum \deg f_\alpha < n$, and let V be the set of their common zeros in K^n. One has*

$$\mathrm{Card}(V) \equiv 0 \pmod{p}.$$

Put $P = \prod_\alpha (1-f_\alpha^{q-1})$ and let $x \in K^n$. If $x \in V$, all the $f_\alpha(x)$ are zero and $P(x) = 1$; if $x \notin V$, one of the $f_\alpha(x)$ is nonzero and $f_\alpha(x)^{q-1} = 1$, hence $P(x) = 0$. Thus P is the *characteristic function* of V. If, for every polynomial f, we put $S(f) = \sum_{x \in K^n} f(x)$, we have

$$\mathrm{Card}(V) \equiv S(P) \pmod{p}$$

and we are reduced to showing that $S(P) = 0$.

Now the hypothesis $\sum \deg f_\alpha < n$ implies that $\deg P < n(q-1)$; thus P is a linear combination of monomials $X^u = X_1^{u_1} \ldots X_n^{u_n}$ with $\sum u_i < n(q-1)$. It suffices to prove that, for such a monomial X^u, we have $S(X^u) = 0$, and this follows from the lemma since at least one u_i is $<q-1$.

Corollary 1.—*If $\sum \deg f_\alpha < n$ and if the f_α have no constant term, then the f_α have a nontrivial common zero.*

Indeed, if V were reduced to $\{0\}$, Card(V) would not be divisible by p.

Corollary 1 applies notably when the f_α are *homogeneous*. In particular:

Corollary 2.—*All quadratic forms in at least 3 variables over K have a non trivial zero.*

(In geometric language: every conic over a finite field has a rational point.)

§3. *Quadratic reciprocity law*

3.1. *Squares in* $\mathbf{F}_q$

Let q be a power of a prime number p.

Theorem 4.—(a) *If $p = 2$, then all elements of $\mathbf{F}_q$ are squares.*

(b) *If $p \neq 2$, then the squares of $\mathbf{F}_q^*$ form a subgroup of index 2 in $\mathbf{F}_q^*$; this subgroup is the kernel of the homomorphism $x \mapsto x^{(q-1)/2}$ with values in $\{\pm 1\}$.*

(In other terms, one has an exact sequence:

$$1 \to \mathbf{F}_q^{*2} \to \mathbf{F}_q^* \to \{\pm 1\} \to 1.)$$

Case (a) follows from the fact that $x \mapsto x^2$ is an automorphism of $\mathbf{F}_q$.

In case (b), let Ω be an algebraic closure of $\mathbf{F}_q$; if $x \in \mathbf{F}_q^*$, let $y \in \Omega$ be such that $y^2 = x$. We have:

$$y^{q-1} = x^{(q-1)/2} = \pm 1 \text{ since } x^{q-1} = 1.$$

For x to be a square in $\mathbf{F}_q$ it is necessary and sufficient that y belongs to $\mathbf{F}_q^*$, i.e. $y^{q-1} = 1$. Hence $\mathbf{F}_q^{*2}$ is the kernel of $x \mapsto x^{(q-1)/2}$. Moreover, since $\mathbf{F}_q^*$ is cyclic of order $q-1$, the index of $\mathbf{F}_q^{*2}$ is equal to 2.

3.2. *Legendre symbol (elementary case)*

Definition.—*Let p be a prime number $\neq 2$, and let $x \in \mathbf{F}_p^*$. The Legendre symbol of x, denoted by $\left(\frac{x}{p}\right)$, is the integer $x^{(p-1)/2} = \pm 1$.*

It is convenient to extend $\left(\frac{x}{p}\right)$ to all of $\mathbf{F}_p$ by putting $\left(\frac{0}{p}\right) = 0$. Moreover, if $x \in \mathbf{Z}$ has for image $x' \in \mathbf{F}_p$, one writes $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.

We have $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$: The Legendre symbol is a "character" (cf. chap. VI, §1). As seen in theorem 4, $\left(\frac{x}{p}\right) = 1$ is equivalent to $x \in \mathbf{F}_p^{*2}$; if $x \in \mathbf{F}_p^*$ has y as a square root in an algebraic closure of $\mathbf{F}_p$, then $\left(\frac{x}{p}\right) = y^{p-1}$.

Computation of $\left(\frac{x}{p}\right)$ *for* $x = 1, -1, 2$:

If n is an *odd* integer, let $\varepsilon(n)$ and $\omega(n)$ be the elements of $\mathbf{Z}/2\mathbf{Z}$ defined by:

$$\varepsilon(n) \equiv \frac{n-1}{2} \pmod 2 = \begin{cases} 0 \text{ if } n \equiv 1 \pmod 4 \\ 1 \text{ if } n \equiv -1 \pmod 4 \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \pmod 2 = \begin{cases} 0 \text{ if } n \equiv \pm 1 \pmod 8 \\ 1 \text{ if } n \equiv \pm 5 \pmod 8 \end{cases}$$

[The function ε is a homomorphism of the multiplicative group $(\mathbf{Z}/4\mathbf{Z})^*$ onto $\mathbf{Z}/2\mathbf{Z}$; similarly, ω is a homomorphism of $(\mathbf{Z}/8\mathbf{Z})^*$ onto $\mathbf{Z}/2\mathbf{Z}$.]

Theorem 5.—*The following formulas hold*:

i) $\left(\frac{1}{p}\right) = 1$

ii) $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$

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

Only the last deserves a proof. If α denotes a primitive 8th root of unity in an algebraic closure Ω of $\mathbf{F}_p$, the element $y = \alpha+\alpha^{-1}$ verifies $y^2 = 2$ (from $\alpha^4 = -1$ it follows that $\alpha^2+\alpha^{-2} = 0$). We have

$$y^p = \alpha^p+\alpha^{-p}.$$

If $p \equiv \pm 1 \pmod 8$, this implies $y^p = y$, thus $\left(\frac{2}{p}\right) = y^{p-1} = 1$. If $p \equiv \pm 5 \pmod 8$, one finds $y^p = \alpha^5+\alpha^{-5} = -(\alpha+\alpha^{-1}) = -y$. (This again follows from $\alpha^4 = -1$.) We deduce from this that $y^{p-1} = -1$, whence iii) follows.

Remark. Theorem 5 can be expressed in the following way:

-1 is a square (mod p) if and only if $p \equiv 1 \pmod 4$.
2 is a square (mod p) if and only if $p \equiv \pm 1 \pmod 8$.

3.3 *Quadratic reciprocity law*

Let l and p be two distinct prime numbers different from 2.

Theorem 6 (Gauss).— $\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}$.

Let Ω be an algebraic closure of $\mathbf{F}_p$, and let $w \in \Omega$ be a primitive l-th root of unity. If $x \in \mathbf{F}_l$, the element w^x is well defined since $w^l = 1$. Thus we are able to form the "Gauss sum":

$$y = \sum_{x \in \mathbf{F}_l} \left(\frac{x}{l}\right) w^x.$$

Lemma 1.—$y^2 = (-1)^{\varepsilon(l)} l$.
(By abuse of notation l denotes also the image of l in the field $\mathbf{F}_p$.)

We have

$$y^2 = \sum_{x,z} \left(\frac{xz}{l}\right) w^{x+z} = \sum_{u \in \mathbf{F}_l} w^u \left(\sum_{t \in \mathbf{F}_l} \left(\frac{t(u-t)}{l}\right)\right).$$

Now if $t \neq 0$:

$$\left(\frac{t(u-t)}{l}\right) = \left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right) = (-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right),$$

and

$$(-1)^{\varepsilon(l)} y^2 = \sum_{u \in \mathbf{F}_l} C_u w^u,$$

where

$$C_u = \sum_{t \in \mathbf{F}^*} \left(\frac{1-ut^{-1}}{l}\right).$$

If $u = 0$, $C_0 = \sum_{t \in \mathbf{F}_l^*} \left(\frac{1}{l}\right) = -1$; otherwise $s = 1-ut^{-1}$ runs over $\mathbf{F}_l - \{1\}$, and we have

$$C_u = \sum_{s \in \mathbf{F}_l} \left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) = -\left(\frac{1}{l}\right) = -1,$$

since in $\mathbf{F}_l^*$ there are as many squares as non squares. Hence $\sum_{u \in \mathbf{F}_l} C_u w^u = l-1-\sum_{u \in \mathbf{F}_l^*} w^u = l$, which proves the lemma.

Lemma 2.—$y^{p-1} = \left(\frac{p}{l}\right)$

Since Ω is of characteristic p, we have

$$y^p = \sum_{x \in \mathbf{F}_l} \left(\frac{x}{p}\right) w^{xp} = \sum_{z \in \mathbf{F}_l} \left(\frac{zp^{-1}}{l}\right) w^z = \left(\frac{p^{-1}}{l}\right) y = \left(\frac{p}{l}\right) y;$$

hence $y^{p-1} = \left(\frac{p}{l}\right)$.

Theorem 6 is now immediate. Indeed, by lemmas 1 and 2,

$$\left(\frac{(-1)^{\varepsilon(l)}\, l}{p}\right) = y^{p-1} = \left(\frac{p}{l}\right)$$

and the second part of th. 5 proves that

$$\left(\frac{(-1)^{\varepsilon(l)}}{p}\right) = (1)^{-\varepsilon(l)\varepsilon(p)}.$$

Translation.—Write lRp if l is a square (mod p) (that is to say, if l is a "*quadratic residue*" modulo p) and lNp otherwise. Theorem 6 means that

$$lRp \Leftrightarrow pRl \quad \text{if } p \text{ or } l \equiv 1 \pmod 4$$

$$lRp \Leftrightarrow pNl \quad \text{if } p \text{ and } l \equiv -1 \pmod 4.$$

Remark. Theorem 6 can be used to compute Legendre symbols by successive reductions. Thus:

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Appendix

Another proof of the quadratic reciprocity law (G. EISENSTEIN, *J. Crelle*, *29*, 1845, pp. 177–184.)

i) *Gauss Lemma*

Let p be a prime number $\neq 2$, and let S be a subset of $\mathbf{F}_p^*$ such that $\mathbf{F}_p^*$ is the disjoint union of S and $-S$. In the following we take $S = \left\{1, \dots, \frac{p-1}{2}\right\}$.

If $s \in S$ and $a \in \mathbf{F}_p^*$, we write as in the form $as = e_s(a)s_a$ with $e_s(a) = \pm 1$ and $s_a \in S$.

Lemma (Gauss).—$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a)$.

Remark first that, if s and s' are two distinct elements of S, then $s_a \neq s'_a$ (for otherwise $s = \pm s'$ contrary to the choice of S). This shows that $s \mapsto s_a$ is a bijection of S onto itself. Multiplying the equalities $as = e_s(a)s_a$, we obtain

$$a^{(p-1)/2} \prod_{s \in S} s = \left(\prod_{s \in S} e_s(a)\right) \prod_{s \in S} s_a = \left(\prod_{s \in S} e_s(a)\right) \prod_{s \in S} s,$$

hence

$$a^{(p-1)/2} = \prod_{s \in S} e_s(a);$$

this proves the lemma since $\left(\frac{a}{p}\right) = a^{(p-1)/2}$ in $\mathbf{F}_p$.

Example.—Take $a = 2$ and $S = \left\{1, \dots, \frac{p-1}{2}\right\}$. We have $e_s(2) = 1$ if $2s \leqq \frac{p-1}{2}$ and $e_s(2) = -1$ otherwise. From this we get $\left(\frac{2}{p}\right) = (-1)^{n(p)}$ where $n(p)$ is the number of integers s such that $\frac{p-1}{4} < s \leqq \frac{p-1}{2}$. If p is of the form $1+4k$ (resp. $3+4k$), then $n(p) = k+1$. Thus we recover the fact that $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \pmod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 5 \pmod 8$, cf. th. 5.

ii) *A trigonometric lemma*

Lemma.—*Let m be a positive odd integer. One has*

$$\frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{1 \leq j \leq (m-1)/2} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m}\right).$$

This is elementary (for instance, prove first that $\sin(mx)/\sin(x)$ is a polynomial of degree $(m-1)/2$ in $\sin^2 x$, then remark that this polynomial has for roots the $\sin^2 \frac{2\pi j}{m}$ with $1 \leq j \leq (m-1)/2$; the factor $(-4)^{(m-1)/2}$ is obtained by comparing coefficients of $e^{i(m-1)x}$ on both sides).

iii) *Proof of the quadratic reciprocity law*

Let l and p be two distinct prime numbers different from 2. Let

$$S = \{1, \ldots, (p-1)/2\}$$

as above. From Gauss' lemma, we get

$$\left(\frac{l}{p}\right) = \prod_{s \in S} e_s(l).$$

Now the equality $ls = e_s(l)s_l$ shows that

$$\sin \frac{2\pi}{p} ls = e_s(l) \sin \frac{2\pi}{p} s_l.$$

Multiplying these equalities, and taking into account that $s \mapsto s_l$ is a bijection, we get:

$$\left(\frac{l}{p}\right) = \prod_{s \in S} e_s(l) = \prod_{s \in S} \sin \frac{2\pi ls}{p} / \sin \frac{2\pi s}{p}.$$

By applying the trigonometric lemma with $m = l$, we can rewrite this:

$$\left(\frac{l}{p}\right) = \prod_{s \in S} (-4)^{(l-1)/2} \prod_{t \in T} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{l}\right)$$

$$= (-4)^{(l-1)(p-1)/4} \prod_{s \in S,\, t \in T} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{l}\right),$$

where T denotes the set of integers between 1 and $(l-1)/2$. Permuting the roles of l and p, we obtain similarly:

$$\left(\frac{p}{l}\right) = (-4)^{(l-1)(p-1)/4} \prod_{s \in S,\, t \in T} \left(\sin^2 \frac{2\pi t}{l} - \sin^2 \frac{2\pi s}{p}\right).$$

The factors giving $\left(\frac{l}{p}\right)$ and $\left(\frac{p}{l}\right)$ are identical up to sign. Since there are $(p-1)(l-1)/4$ of these, we find:

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{(p-1)(l-1)/4}.$$

This is the quadratic reciprocity law, cf. th. 6.

Chapter II

p-Adic Fields

In this chapter p denotes a prime number.

§1. *The ring* $\mathbf{Z}_p$ *and the field* $\mathbf{Q}_p$

1.1. *Definitions*

For every $n \geqq 1$, let $A_n = \mathbf{Z}/p^n\mathbf{Z}$; it is the ring of classes of integers (mod p^n). An element of A_n defines in an obvious way an element of A_{n-1}; we thus obtain a homomorphism

$$\phi_n : A_n \to A_{n-1},$$

which is surjective and whose kernel is $p^{n-1}A_n$.

The sequence

$$\ldots \to A_n \to A_{n-1} \to \ldots \to A_2 \to A_1$$

forms a "projective system" indexed by the integers $\geqq 1$.

Definition 1.—*The ring of p-adic integers* $\mathbf{Z}_p$ *is the projective limit of the system* (A_n, ϕ_n) *defined above.*

By definition, an element of $\mathbf{Z}_p = \varprojlim (A_n, \phi_n)$ is a sequence $x = (\ldots, x_n, \ldots, x_1)$ with $x_n \in A_n$ and $\phi_n(x_n) = x_{n-1}$ if $n \geqq 2$. Addition and multiplication in $\mathbf{Z}_p$ are defined "coordinate by coordinate". In other words, $\mathbf{Z}_p$ is a *subring* of the product $\prod_{n \geqq 1} A_n$. If we give A_n the discrete topology and $\prod A_n$ the product topology, the ring $\mathbf{Z}_p$ inherits a topology which turns it into a *compact* space (since it is closed in a product of compact spaces).

1.2. *Properties of* $\mathbf{Z}_p$

Let $\varepsilon_n : \mathbf{Z}_p \to A_n$ be the function which associates to a p-adic integer x its n-th component x_n.

Proposition 1.—*The sequence* $0 \to \mathbf{Z}_p \xrightarrow{p^n} \mathbf{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ *is an exact sequence of abelian groups.*

(Thus we can identify $\mathbf{Z}_p/p^n\mathbf{Z}_p$ with $A_n = \mathbf{Z}/p^n\mathbf{Z}$.)

Multiplication by p (hence also by p^n) is injective in $\mathbf{Z}_p$; indeed, if $x = (x_n)$ is a p-adic integer such that $px = 0$, we have $px_{n+1} = 0$ for all n, and x_{n+1} is of the form $p^n y_{n+1}$ with $y_{n+1} \in A_{n+1}$; since $x_n = \phi_{n+1}(x_{n+1})$, we see that x_n is also divisible by p^n, hence, is zero.