Annotations for Serre's Course in Arithmetic

Martin H. Weissman, Jordan Fassler, Filix Maisch, and...

E-mail address: weissman@ucsc.edu, jfassler@math.ucsc.edu, fmaisch@ucsc.edu

Contents

Background

0.1. Project Description. During the fall quarter, 2006, a graduate course in algebraic number theory is being held at the University of California, Santa Cruz. For approximately one hour per week, the participants in this course discuss the first part of Serre's book "A Course in Arithmetic" in great detail. In addition, the participants take turns preparing annotations to accompany this book, in order to aid this discussion. Herein lie the annotations.

0.2. Notation and references. All notation will be the same as Serre's notation, unless otherwise specified. References to Serre will refer to the chapter, section, and subsection. For example, referring to I.1.1 of Serre refers to the first chapter (Finite Fields), the first section (Generalities), and the first subsection (Finite Fields). When referring to theorems, the chapter, section, and subsection will also be mentioned so that the theorem can easily be found. For example, Theorem 6 of I.3.3 is Gauss's theorem of quadratic reciprocity.

We will label chapters, sections, and subsections, in these notes, to precisely mirror Serre's divisions.

0.3. Authorship of these notes. Since there are many authors of these notes, we will write the author's name at the beginning of each section he or she has responsibility for writing.

CHAPTER 1

Finite Fields

1. Generalities

Notes by: M.H. Weissman

In this section, Serre proves the basic structural results for finite fields. This includes their construction, complete classification, and essentially their Galois theory. It also includes the very fundamental theorem, that their multiplicative groups are cyclic - this result is not obvious at all, and can be thought of as a huge generalization and strengthening of Fermat's little theorem.

1.1. Finite Fields. A ring will always mean a commutative ring with unit. Ring homomorphisms are always assumed to take the unit element to the unit element.

Remarks on: The characteristic subring

For any ring R, there is a unique ring homomorphism ϕ from $\mathbb{Z}$ to R. The image of ϕ is a subring of R, and a quotient ring of $\mathbb{Z}$. Thus R contains a subring isomorphic to $\mathbb{Z}/N\mathbb{Z}$ for some integer $N \geq 0$.

If R is an integral domain, then the image $\phi(\mathbb{Z})$ is an integral domain. Hence $N = 0$ or $N = p$ for some positive prime integer p, since the principal ideals $< 0 >$ and $< p >$ are the only prime ideals of $\mathbb{Z}$. In particular, if R is a field, then $\phi(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$ or $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Moreover, if R is a field, and $\phi(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$, then R contains $\mathbb{Q}$.

Remarks on: The Lemma

Suppose that K is a field, of characteristic p (a prime). Let $\sigma(x) = x^p$ be the resulting isomorphism of K onto its subfield K^p. There are examples when $K^p \neq K$. For example, consider the field $K = \mathbb{F}_p(X) = Quot(\mathbb{F}_p[X])$. Elements of K are "rational functions" (i.e. quotients of polynomials) in a variable X with coefficients in $\mathbb{F}_p$. Raising such a quotient to the p-power raises the numerator and denominator to the p-power. Since σ is a ring homomorphism, a polynomial raised to the p-power becomes a polynomial in the variable X^p. Hence, one can see that $K^p = \mathbb{F}_p(X^p)$ (rational functions in the variable X^p).

It should be remarked that the binomial formula (for expanding $(a + b)^n$) is valid in any (commutative) ring – the typical inductive proof uses only the ring axioms.

Every homomorphism of fields is injective (the zero-ring is not considered a field by us, though perhaps Deitmar and others would disagree!). This explains why "σ is clearly injective".

Remarks on: Theorem 1

Supposing that K is a finite field, it contains $\mathbb{F}_p$ for some prime number p. Thus K is naturally an $\mathbb{F}_p$-vector space. It is finite-dimensional, since its cardinality is p^f, where f denotes its dimension as an $\mathbb{F}_p$-vector space. This also implies that the additive structure of K (as an abelian group) is $(\mathbb{Z}/p\mathbb{Z})^f$. Of course, this is not the ring structure of K, unless $f = 1$.

When Ω is an algebraically closed field of characteristic p, the automorphism σ is often called "Frobenius". In general, if α is an automorphism of a field F, the elements of F fixed by α form a subfield. Applied to Ω, one arrives at subfields $\mathbb{F}_q$ containing $\mathbb{F}_p$, fixed by σ^f.

It's a general fact from field theory, that if P is a polynomial in $F[X]$, in an algebraically closed field F, then r is a repeated root of P (when P is factored (uniquely) into linear factors, $X - r$ occurs at least twice) if and only if $F(r) = 0$ and $F'(r) = 0$. Thus the polynomial $X^q - X$ has no repeated roots, as Serre says, in Ω. The basic assertions of Theorem 1 are:

- The subfield $\mathbb{F}_q$ of Ω is precisely the set of elements of Ω which are fixed by the automorphism σ^f (when $q = p^f$).
- The subfield $\mathbb{F}_q$ is also equal to the set of roots of the polynomial $X^q - X$ in Ω.
- If F is a subfield of Ω with q elements, then $F = \mathbb{F}_q$.

1.2. The multiplicative group of a finite field. Remarks on: Theorem 2

Serre's proof that $\mathbb{F}_q^*$ is cyclic reduces to a counting argument. His proof can be somewhat simplified, it seems, if one is willing to use the structure theorem for finite abelian groups. Serre is certainly aware of this structure theorem - perhaps he resists using it because the proof of the structure theorem itself is quite involved, and he is trying to assume minimal prerequisites.

We provide a proof of Lemma 2, in the abelian case:

LEMMA 1.1. *Let H be a finite* abelian *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.*

PROOF. Since H is a finite abelian group, there is an isomorphism of abelian groups:

$$H \cong \frac{\mathbb{Z}}{e_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{e_k\mathbb{Z}}.$$

Moreover, we can assume that if $k > 1$, then $GCD(e_i, e_j) > 1$ for all $i \neq j$. In other words, we make k as small as possible in the decomposition. Thus, if $k > 1$, there exists an integer d dividing both e_1 and e_2. Let E_1 and E_2 denote the subgroups of $\mathbb{Z}/e_1\mathbb{Z}$ and $\mathbb{Z}/e_2\mathbb{Z}$, consisting of elements of order dividing d. Then the cardinality of E_1 is at least d, and the cardinality of E_2 is at least d. Finally, we see that H contains a subgroup E isomorphic to $E_1 \times E_2$, all of whose elements have order dividing d. There are at least d^2 elements in this subgroup E - a contradiction.

Hence $k = 1$, and H must be cyclic. □

Examples on: Theorem 2

Since the multiplicative group of a finite field is cyclic, one may immediately deduce facts about perfect powers. If q is odd, then $q-1$ is even. Hence there are $(q-1)/2$ perfect squares in $\mathbb{F}_q^\times$, when q is odd. Moreover, multiplying two non-squares always

yields a square. When q is even, every element of $\mathbb{F}_q$ is a perfect square (squaring is an automorphism of the field!).

Similarly, when $q-1$ is divisible by 3, there are $(q-1)/3$ perfect cubes in $\mathbb{F}_q^\times$. When $q-1$ is not divisible by 3, every element of $\mathbb{F}_q$ is a perfect cube!

Most generally, when $q-1$ is relatively prime to k (k a positive integer), for every element x of $\mathbb{F}_q$, there exists a unique element $y \in \mathbb{F}_q$, such that $y^k = x$.

2. Equations over a finite field

Notes by: M.H. Weissman

In this section, Serre applies some computations over a finite field to problems involving counting solutions to polynomial equations. This culminates in the Chevalley-Warning theorem, which has applications to Diophantine equations.

2.1. Power sums. Remarks on: The Lemma

The proof of this Lemma may seem a bit ad-hoc. It relies on the following three properties of functions from K to K (when K is a finite field):

- $$\sum_{x \in K} 1 = 0.$$
- $$\sum_{x \in K^\times} 1 = -1.$$
- $$\sum_{x \in K} f(xy) = \sum_{x \in K} f(x),$$
  when $y \in K^\times$, and $f\colon K \to K$ is any function.

2.2. Chevalley theorem. Remarks on: Theorem 3

The proof of the Chevalley-Warning theorem follows the general plan for studying the vanishing locus V of a system of polynomials f_α in n variables over a finite field K.

- Remarkably, it is possible to "cook up" a single polynomial P in n variables over K, such that P is the characteristic function of V ($P(\vec{v}) = 1$ if $\vec{v} \in V$, and $P(\vec{v}) = 0$ if $\vec{v} \notin V$).
- The cardinality of V, mod p, is equal to the summation of P over the domain K^n. This reduces the counting problem to a fact about power sums.
- By construction, $deg(P) < n(q-1)$. This means that for each monomial M in P, there exists a variable X_i such that the degree of X_i in M is less than $q-1$. Thus the power sum for that monomial vanishes (mod p, of course).

The Chevalley theorem is an extremely useful way to prove that a system of polynomial equations over a finite field has a *nontrivial* solution. The general idea is:

- Prove that the system of polynomial equations has at least one solution (usually a "trivial solution").

- Prove that the the total number N of solutions to the system is divisible by p, a prime number.
- Since $N \geq 1$, and $N \equiv 0 \mod p$, we must have $N \geq p$. Thus there are at least $p-1$ nontrivial solutions.

Examples on: Theorem 3

The requirements of the Chevalley theorem are that the number of variables is large compared to the degree of the equations. The Chevalley theorem is quite easy to use when one is working with a homogeneous equation (so that a trivial solution exists). We focus on some illustrative examples here.

Suppose first that we have a single polynomial $f \in K[X_1, \ldots, X_n]$. Define the vanishing locus:

$$V = \{\vec{x} \in K^n \text{ such that } f(\vec{x}) = 0\}.$$

If $n > deg(f)$, then $Card(V) \equiv 0 \mod p$, by the Chevalley theorem.

The Chevalley theorem applies if f is quadratic in at least 3 variables, cubic in at least 4 variables, quartic in at least 5 variables, etc... If $f(0, \ldots, 0) = 0$ (for example, if f is homogeneous, or more generally, if f does not have a constant term), then the Chevalley theorem implies that $Card(V) > 1$.

There is an important way to convert an inhomogeneous equation into a homogeneous equation, to apply Chevalley's theorem. Consider the following example: let $f(X, Y) = X^2 + 2Y^2 + Y + 1$. We might ask if there exist $x, y \in K$ such that $f(x, y) = 0$. Unfortunately, Chevalley's theorem does not apply, and even if it did, we might not be able to find a "trivial solution" to begin with.

The trick is to homogenize the polynomial f by putting in a new variable Z:

$$F(X, Y, Z) = X^2 + 2Y^2 + YZ + Z^2.$$

Here, we multiply each term by a suitable power of Z, so that each resulting term has degree 2.

Now, we have an quadratic equation in 3 variables, with an obvious solution $(0, 0, 0)$. Hence the number of solutions to the equation $F(X, Y, Z) = 0$ is divisible by p . There are two types of solutions: those with $Z = 0$, and those with $Z \neq 0$. When $Z = 0$, $F(X, Y, Z) = 0$ if and only if $X^2 + 2Y^2 = 0$. If $2 = u^2$ in K, and $p \neq 2$, then $X = \pm uY$ (if $p \neq 2$). Thus there are $2p - 1$ such solutions. Hence there must be one at least one solution to $F(X, Y, Z) = 0$, when $Z \neq 0$. Dividing through by Z yields: if 2 is a square in K, and $p \neq 2$, then there exists a solution to $f(X, Y) = 0$ in K.

3. Quadratic reciprocity law

In this section, Serre gives a proof of quadratic reciprocity. Although conjectured before, the first proof of this theorem is due to Gauss (around 1799). During his lifetime, Gauss gave eight proofs of quadratic reciprocity.

The proof of Serre owes a great deal to proofs of Gauss, though it is probably slicker in places.

3.1. Squares in $\mathbb{F}_q$.

Remarks on: Theorem 4

The fact that all elements of $\mathbb{F}_q$ are squares when $q = 2^f$ makes the study of squares in $\mathbb{F}_q$ irrelevant. From a more advanced standpoint, this fact is suggestive. It suggests the question: what are the quadratic extensions of $\mathbb{F}_q$? In fact, every

quadratic extension of a field of characteristic 2 is obtained by adjoining a root of X^2+X+a, for some element a of the field. Therefore, one should ask the question: when does X^2+X+a have a root in $\mathbb{F}_q$?

Part (b) of Theorem 4 suggests the definition of the Legendre symbol. The fact that squares form a subgroup of index two relies essentially on the fact that $\mathbb{F}_q^\times$ is a cyclic group of even order. Moreover, every subgroup of a cyclic group is cyclic.

Let us prove part (b), just with basic group theory. If g is a generator of the cyclic group $\mathbb{F}_q^\times$, then $g^{2d}=1$ for some positive integer d, which we can choose minimally. In fact, the minimal d is $(q-1)/2$ It follows that the squares $\mathbb{F}_q^{\times 2}$ are the elements g^{2i} for $i=1,\dots,d$. If $x=g^{2i}$, then $x^{(q-1)/2}=g^{2di}=1$.

Conversely, if $x^d=1$, and $x=g^j$, then $g^{jd}=1$, so jd must be a multiple of $2d$, so j is even. Thus x is a square.

Finally, if $x=g^j$ for any j, we see that $x^d=g^{jd}$ and $x^{2d}=g^{2jd}=1$. Thus x^d is a square root of 1, and hence equals ± 1.

3.2. Legendre symbol (elementary case). The crucial fact to remember about the Legendre symbol is that it has a formulaic definition as well as an interpretation in terms of squares. Suppose that p is prime, and $x \not\equiv 0 \mod p$. Then $\left(\frac{x}{p}\right)$ is equal to 1 or -1, depending on whether x is a square or not in $\mathbb{F}_p$. When $x \equiv 0 \mod p$, we define $\left(\frac{x}{p}\right)=0$. Uniformly speaking, $\left(\frac{x}{p}\right)$ is equal to the number of square roots of x in $\mathbb{F}_p$, decreased by 1.

The formulaic definition of $\left(\frac{x}{p}\right)$ is that $\left(\frac{x}{p}\right) = x^{(p-1)/2}$ (in $\mathbb{F}_p$).

The multiplicativity of the Legendre symbol follows easily from the formulaic definition; and without too much difficulty from its interpretation in terms of squares, given the cyclicity of $\mathbb{F}_q^\times$.

Remarks on: Theorem 5

1 is always a square – nuff said.

The fact that $\left(\frac{-1}{p}\right)=(-1)^{\epsilon(p)}$ is based on the fact that $\epsilon(p)\equiv(p-1)/2 \bmod 2$. Thus the fact follows from the formulaic definition of the Legendre symbol. Again, one could approach this from the interpretation in terms of squares. -1 is a square in $\mathbb{F}_p$, if and only if there is a fourth root of unity in $\mathbb{F}_p$. This would require that $p-1$ is divisible by 4, by the cyclicity of $\mathbb{F}_p^\times$.

The proof that $\left(\frac{2}{p}\right)=(-1)^{\omega(p)}$ is quite slick here. There are, to be certain, other proofs out there, one using Wilson's theorem that is cute.

Consider a primitive eighth root of unity α in Ω, as Serre suggests. This means that $\alpha^8=1$, and if $\alpha^d=1$ for $1<d$, then d is divisible by 8. However, even a primitive eighth root of unity has degree at most 4 over $\mathbb{F}_q$, since $\alpha^4=-1$. Here, we note that α^4 must be a square root of unity, and cannot equal 1 since α is primitive.

If $y=\alpha+\alpha^{-1}$, then $y^2=\alpha^2+\alpha^{-2}+2$; since $\alpha^4=-1$, we have $\alpha^2=-1/\alpha^2$, so $\alpha^{-2}=-\alpha^2$. Thus $y^2=2$ as Serre says.

If $p\equiv\pm 1 \mod 8$, then $\alpha^p=\alpha^{\pm 1}$. This is why $y^p\equiv y$ if $p\equiv\pm1 \mod 8$. Thus $\left(\frac{2}{p}\right)=\left(\frac{y^2}{p}\right)=y^{(p-1)}=1$ in this case. Note that computations are taking place in the algebraic closure Ω, though the results lie in $\mathbb{F}_p$!

When $p \equiv \pm 5 \mod 8$, we have $y^p = \alpha^5 + \alpha^{-5}$. We have $\alpha^5 = \alpha^4\alpha = -\alpha$, and $\alpha^{-5} = \alpha^{-4}\alpha^{-1} = -\alpha^{-1}$. Hence $y^p = -y$, and the proof follows.

3.3. Quadratic reciprocity law. Quadratic reciprocity, in addition to being a beautiful theorem, is also a very practical one. The formula, when p and ℓ are distinct odd primes, is:

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right)(-1)^{\epsilon(p)\epsilon(\ell)}.$$

To remember this, one can simply remember the following:

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right), \text{ unless } p \text{ and } \ell \text{ are } 3 \mod 4.$$

Of course, if both are $3 \mod 4$, then one switches the sign. It is a theorem worth memorizing!

Many proofs of quadratic reciprocity use "Gauss sums". Serre works with Gauss sums in the algebraic closure of $\mathbb{F}_p$, which slickens some proofs.

Remarks on: Lemma 1

Here $y = \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)w^x$, where w is a primitive l-th root of unity in an algebraic closure of $\mathbb{F}_p$. This is very confusing, because x is in $\mathbb{F}_\ell$ (a number mod ℓ), and w is in $\bar{\mathbb{F}}_p$. Thus we have an exponent and base that live in different worlds! It works precisely because of the choice of w as such a root of unity. More confusing still, is that $\left(\frac{x}{\ell}\right)$, though it equals 0, 1, or -1, it is being interpreted as an element of $\mathbb{F}_p$ in the formula for y.

The result that $y^2 = (-1)^{\epsilon(\ell)}\ell$ is somewhat deep; a similar fact is true if one works in $\mathbb{C}$, but the sign can be difficult to obtain. The computations are essentially "calculus tricks" transferred to this finite situation.

In the first step, summing over $x, z \in \mathbb{F}_\ell$ becomes summing over $t, u \in \mathbb{F}_\ell$ with the change of variables $x + z = u, x = t$.

The second step, computing $\left(\frac{t(u-t)}{\ell}\right)$ when $t \neq 0$ simply uses the property that the Legendre symbol is multiplicative, and the formula for $\left(\frac{-1}{\ell}\right)$. Of course, this Legendre symbol equals zero when $t = 0$.

The first and second steps together yield the new expression for $(-1)^{\epsilon(\ell)}y^2$. The rest is a direct computation and counting of squares and nonsquares.

Note that nowhere is the characteristic p nature of the Gauss sum being used! Only the fact that w is a primitive root of unity.

Remarks on: Lemma 2

Here the characteristic p nature of Serre's Gauss sum is exploited. There is a typo in the first equation of the proof; it should read:

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

Note that the first step is a simple change of variables, letting $x = zp^{-1}$ (in $\mathbb{F}_\ell$!). The second step uses only the multiplicativity of the Legendre symbol. The third step uses the fact that p is a square iff p^{-1} is a square (mod ℓ).

CHAPTER 2

p-Adic Fields

1. The ring $\mathbb{Z}_p$ and the field $\mathbb{Q}_p$

Notes by: J. Fassler

In this section, Serre defines the p-adic integers $\mathbb{Z}_p$ and proves several of their properties. These include a charicterization of the units in $\mathbb{Z}_p$ and a description of their topology. The p-adic numbers $\mathbb{Q}_p$ are introduced as the field of fractions of $\mathbb{Z}_p$.

1.1. Definitions. As usual p denotes a prime number. We let $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\phi_n : A_n \to A_{n-1}$ be the canonical homomorphism.

Remarks on: Definition 1

We use the following to define the p-adic integers:

DEFINITION 1.1. A *projective system* is a sequence of objects $\{C_n\}$ and maps $\{f_n\}$ such that $f_n : C_n \to C_{n-1}$ for $n \geq 1$. The *projective limit* (or *inverse limit*) of the system is defined to be

$$\varprojlim C_n = \{(c_n) \in \prod_{n\geq 1} C_n | c_{n-1} = f_n(c_n) \text{ for all } n\}$$

We then define $\mathbb{Z}_p = \varprojlim A_n$.

We can equivalently define the p-adic integers as infinite sums of the form $\sum_{k=0}^{\infty} a_k p^k$ where $a_k \in \{0, 1, \ldots, p-1\}$. Thus p-adic integers can be represented as infinite base p numbers. For example, $\ldots 44444. = \cdots + 4{\cdot}5^4 + 4{\cdot}5^3 + 4{\cdot}5^2 + 4{\cdot}5^1 + 4{\cdot}5^0$ is -1 in $\mathbb{Z}_5$. With this representation addition and multiplication is performed in the same way we add and multiply decimal numbers.

Examples on: Arithmetic in $\mathbb{Z}_p$

Addition:

$$\begin{array}{rr} & \ldots 333333. \\ + & \underline{\ldots 111112.} \\ & \ldots 000000. \end{array}$$

Multiplication

$$\begin{array}{rr} & \ldots 444444. \\ \times & \underline{\ldots 111111.} \\ & \ldots 444444 \\ & \ldots 444440 \\ & \ldots 444400 \\ + & \vdots \\ & \ldots 333334. \end{array}$$

Remarks on: The topology of $\mathbb{Z}_p$

The A_n are finite and thus with the discrete topology are compact. By Tychonoff's theorem the product ring is compact and since $\mathbb{Z}_p = f^{-1}(\{0\})$ where $f : x \in \mathbb{Z}_p \to y \in \mathbb{Z}_p$ is given by $(y_n) = (\phi_{n+1}(x_{n+1}) - x_n)$ thus $\mathbb{Z}_p$ is closed in the product ring and compact.

1.2. Properties of $\mathbb{Z}_p$. Remarks on: Proposition 1

For the proof that $ker(\varepsilon_n) \subset im(p^n)$, we let $x \in ker(\varepsilon_n)$ (note this is a typo in Serre), since $x_m \equiv x_n \pmod{p^n}$ we have that $x_m \equiv 0 \pmod{p^n}$ for all $m \geq n$. This implies that in A_m, $x_m \equiv p^n y_{m-n} \pmod{p^m}$ where $y_{m-n} \in A_{m-n}$ is well defined, since $p^n\mathbb{Z}/p^m\mathbb{Z} \cong A_{m-n}$. Since $x_m = p^n y_{m-n}$ and $x_m \equiv x_{m-1} \pmod{p^{m-1}}$ we have $p^n y_{m-n} \equiv p^n y_{m-n-1} \pmod{p^{m-1}}$ which implies $y_{m-n} \equiv y_{m-n-1} \pmod{p^{m-n-1}}$ and thus $y = (y_m) \in \mathbb{Z}_p$.

That ε_n is surjective is easy since for any $x_n \in A_n$ we can form the sequence $(\ldots, x_n, x_n, \ldots, x_n) \in \mathbb{Z}_p$.

Remarks on: Proposition 2

For part (a), if $x = (x_n) \in \mathbb{Z}_p$ is not divisible by p then, in particular, $x_1 \neq 0 \pmod{p}$ thus there exists $\alpha \in \mathbb{Z}$ such that $\alpha x_1 \equiv 1 \pmod{p}$. Let $z = 1 - \alpha x$, we can compute the inverse of x as follows:

$$\begin{aligned} \alpha x &= 1 - z \\ (1 - z)(1 + z + z^2 + \cdots) &= 1 \\ \text{Thus } x^{-1} &= \alpha(1 + z + z^2 + \cdots) \end{aligned}$$

We note that since z ends in at least one zero, z^k end in at least k zeros. Therefore, even though our expression for the inverse involves an infinite sum, it is well defined since there are only finitely many non-zero terms in any given position.

For part (b), the uniqueness follows from the fact that p^n is an injective map, which was shown in proposition 1.

We remark that, by part (a), $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus (p)$ which implies that $\mathbb{Z}_p$ is a local ring with maximal ideal (p).

Remarks on: The p-adic valuation

Let $x = p^n u$ and $y = p^m v$ where $u, v \in \mathbb{Z}_p$ and suppose $n \geq m$ then $\nu_p(x + y) = \nu_p(p^n u + p^m v) = \nu_p(p^m(p^{n-m}u + v) \geq m = \inf(\nu_p(x), \nu_p(y))$. With the metric defined by $d(x, y) = p^{-\nu_p(x-y)}$ the above inequality implies that the metric satisfies the ultrametric inequality $d(x, z) \leq \sup(d(x, y), d(x, z))$.

Remarks on: Proposition 3

Recall from point set topology that an open set in the product topology is a product of open sets such that only finitely many are not the whole space, thus an open neighborhood of zero in the product topology is of the form $\cdots \times A_{n+2} \times A_{n+1} \times 0 \times \cdots \times 0$. Hence, the ideals $p^n\mathbb{Z}_p$ form a basis of neighborhoods of 0. The addition and multiplication operations on the p-adics are continuous with this topology, which makes Z_p a topological ring.

1.3. The Field $\mathbb{Q}_p$. In our base-p notation the p-adic numbers are of the form $\sum_{n=k}^{\infty} a_n p^n$ where $a_n \in \{0, 1, \ldots, p-1\}$ and $k \in \mathbb{Z}$.

Remarks on: Proposition 4

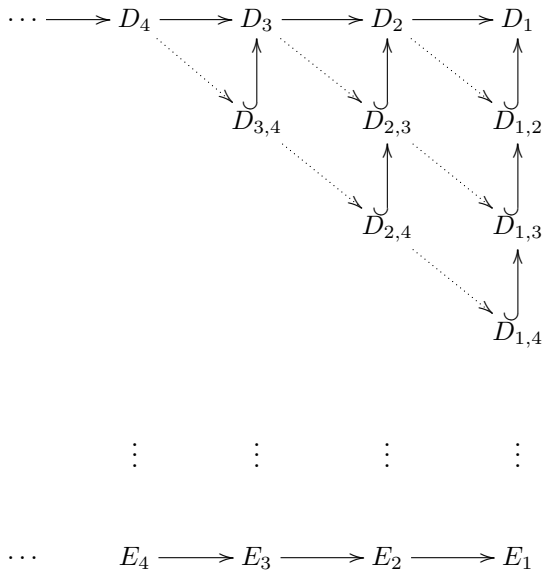
As before $p^n\mathbb{Z}_p$ form open neighborhoods of zero and are compact since $\mathbb{Z}_p$ is. Furthermore, we have the inclusions $\cdots \subset p^n\mathbb{Z}_p \subset p^{n-1}\mathbb{Z}_p \subset \cdots \subset p^0\mathbb{Z}_p \subset p^{-1}\mathbb{Z}_p \subset \cdots$, thus $\mathbb{Z}_p$ is an open subset of $\mathbb{Q}_p$. Finally, any element in $\mathbb{Q}_p$ is of the form $p^n u$ for $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$ thus since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ we have a sequence $y_n \in \mathbb{Z}$ converging to u and thus $p^n y_n \in \mathbb{Q}$ converges to x.

2. p-adic equations

2.1. Solutions. In this section, Serre discusses when polynomial equations over the p-adic numbers have solutions.

Remarks on: Lemma

We have the following picture in this proof:



Examples on: Proposition 5

We can use this proposition to prove that a polynomial has a solution in $\mathbb{Z}_p$ by proving it has a solution in each A_n. For example, we find $\sqrt{2}$ in $\mathbb{Z}_7$ by finding the roots of $f(x) = x^2 - 2$ in $\mathbb{Z}/7^n\mathbb{Z}$ for all n. We proceed by induction on n. Clearly $3^2 \equiv 2 \pmod 7$; we assume that $x_n^2 \equiv 2 \pmod{7^n}$ with $x_n \in A_n$ and find an element $x_{n+1} \in A_{n+1}$ satisfying the equation. Clearly, if $x_{n+1} \equiv x_n \pmod{p^n}$

then $x_{n+1} = x_n + 7^n h$ for some $h \in A_1$.

$$\begin{aligned}
(x_n + 7^n h)^2 &\equiv 2 \pmod{7^{n+1}} \\
x_n^2 + 2x_n h(7^n) &\equiv 2 \pmod{7^{n+1}} \\
2x_n h(7^n) &\equiv -(x_n^2 - 2) \pmod{7^{n+1}} \\
2x_n h(7^n) &\equiv k(7^n) \pmod{7^{n+1}} \text{ for some k in } A_n \\
\text{thus } 2x_n h &\equiv k \pmod 7
\end{aligned}$$

Since two and x_n are invertible in $\mathbb{Z}/7\mathbb{Z}$, we can find h and thus x_{n+1}. Finally, $\sqrt{2} = (x_n)$ in $\mathbb{Z}_p$.

2.2. Amerlioration of approximate solutions. Notes by: M. Weissman

Propositions 5 and 6 imply that in order to find a solution in $\mathbb{Z}_p$ to an equation (or system of equations) with integer coefficients, it suffices to find solutions in $\mathbb{Z}/p^n\mathbb{Z}$ for all n. It is (surprisingly) not necessary to find a compatible system of solutions, i.e., solutions for all n which form a compatible system with respect to the projection maps.

In this section, Serre discusses the "amelioration" process. The classic SAT vocabulary word "ameliorate" means "to make a situation better or more tolerable". When Serre speaks of ameliorating approximate solutions, he is thinking geometrically. Finding a solution to an equation mod p^n is the same as finding a value which is within radius p^{-n} of a solution, in the p-adic metric. When n is large, this could be thought of as an approximate solution. If one can successively increase n, and find better and better approximations, to any degree of precision, then a genuine solution exists.

Thus the amelioration process, when it works (as dictated by the Lemma), yields a genuine solution (as in Theorem 1 and its subsequent corollaries).

Serre remarks that the amelioration process is a p-adic version of Newton's method. In Newton's method, one begins with a polynomial $f \in \mathbb{R}[X]$, and a guess x_0, which may be close to a root. It is a recursive process, according to the rule:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Of course, this recursion fails, if $f'(x_n) = 0$; in general, the success of the method depends on $f'(x_n)$ being significantly larger than $f(x_n)$; obviously, this makes the change from x_n to x_{n+1} gradual. The same principles apply p-adically.

Remarks on: Lemma

Suppose that $f \in \mathbb{Z}_p[X]$, with derivative f'. The Lemma states that if $|f(x)| < p^{-n}$ $(n \geq 1)$, and $|f'(x)| > p^{-n/2}$, then there exists $y \in \mathbb{Z}_p$ such that $|f(y)| < p^{-n-1}$ (y is closer to being a root), and $|f'(y)| = |f'(x)|$. In addition, one finds such a y with $|y - x| < p^{k-n}$ where $k = v_p(f'(x)) = v_p(f'(y)) < n$.

Note that the conclusion that $|f'(y)| = |f'(x)|$ implies that:

$$|f'(y)| > p^{-n/2} > p^{(-n-1)/2}.$$

Hence, replacing x by y, one may apply the Lemma repeatedly to get a sequence $(x_i) in \mathbb{Z}_p$ with $|f(x_i)| < p^{-n-i}$ for all $i \geq 0$.

The Lemma is most often applied in situations when $|f'(x)| = 1$. In this situation, one has Corollary 1 and 2. For simplicity, we go through the proof of Lemma 1, when $|f'(x)| = 1$.

In this case, we are given $|f(x)| < p^{-n}$ and $|f'(x)| = 1$, and we are looking for y such that $y = x + p^n z$, and $|f(y)| < p^{-n-1}$, and $|f'(y)| = 1$. Plugging in, we get:

$$f(y) = f(x) + f'(x)p^n z + f''(x)p^{2n}z^2 + \cdots .$$

This is simply the finite Taylor expansion of a polynomial, which works over any ring. Noting that only $f(x)$ and $f'(x)p^n z$ matter for our desired level of approximation, we are looking for z such that:

$$|f(x) + f'(x)p^n z| < p^{-n-1}.$$

In other words, we would like:

$$f(x) + f'(x)p^n z \equiv 0 \mod p^{n+1}.$$

Since $f'(x)$ has absolute value 1, it is invertible in $\mathbb{Z}_p$. Moreover, $f(x) = p^n q$, for some $q \in \mathbb{Z}_p$. Thus we can satisfy the above congruence by setting:

$$z \equiv -q(f'(x))^{-1} \mod p.$$

This yields a better approximation:

$$y = x - f(x)f'(x)^{-1},$$

for any choice of integer $f'(x)^{-1}$ which behaves as a reciprocal mod p. Notice the formal similarity with the real Newton's method. Here of course, we are only using a modular inverse.

Finally, note that $f'(y) = f'(x) + f''(x)p^n z + \cdots$. Since $f'(x)$ has absolute value 1, and p^n has absolute value p^{-n}, and higher terms are even smaller, the ultrametric inequality implies that $|f'(y)| = 1$. Thus the Lemma is proven in this simple case.

Examples on: Lemma

Suppose that $p \neq 2$, and $t \in \mathbb{Z}$. Then t has a square root in $\mathbb{Z}_p$ if and only if t has a square root in $\mathbb{F}_p$ and t is not divisible by p. For if $\bar{x}$ is a square root of t, mod p, then $\bar{x}$ yields an approximate solution $x \in \mathbb{Z}_p$. The equation $f(X) = X^2 - t$ has derivative $f'(X) = 2X$. As long as $2 \neq 0$, and $t \neq 0$, we see that $f'(\bar{x})$ is nonzero in $\mathbb{F}_p$. Hence $|f'(x)| = 1$. The Lemma applies, and we may successively approximate better solutions, yielding a solution in $\mathbb{Z}_p$.

However, if $p = 2$, and $t \in \mathbb{Z}$, and t is odd, then t has a square root in $\mathbb{Z}_2$ if and only if t has a square root in $\mathbb{Z}/8\mathbb{Z}$! Indeed, if t has a square root $\bar{x}$ in $\mathbb{Z}/8\mathbb{Z}$, then $\bar{x}$ yields an approximate solution $x \in \mathbb{Z}_2$ with $|f(x)| < 1/8 = 2^{-3}$. We have $f'(x) = 2x$, and since x is odd, $|f'(x)| > 1/2 > 2^{-3/2}$. The inequality in the Lemma applies, and we may "ameliorate" our approximate root to get a genuine square root in $\mathbb{Z}_2$.

3. The multiplicative group of $\mathbb{Q}_p$

Serre considers the structure of the abelian group $\mathbb{Q}_p^\times$ (nonzero elements of $\mathbb{Q}_p$ under multiplication). Serre's approach is completely algebraic, but it is possible and useful to consider a more analytic approach. We describe this analytic approach here.

3.1. The filtration of the group of units. Serre defines U to be the group of p-adic units: $U = \mathbb{Z}_p^\times$. Note that $\mathbb{Z}_p$ is a local ring; the units are all elements of $\mathbb{Z}_p$ which are not multiples of p. For every $n \geq 1$, he puts:

$$U_n = 1 + p^n\mathbb{Z}_p.$$

In other words,

$$U_n = \{x \in \mathbb{Z}_p \text{ such that } |x-1| \leq p^{-n}\}.$$

It is closed under multiplication, by direct computation. It is also closed under inverses, as can be seen from direct computation with a bit more trouble.

While Serre analyzes the structure of U_n algebraically, we work analytically instead. Then we claim the following:

PROPOSITION 3.1. *Define the formal power series:*

$$exp(X) = 1 + X + X^2/2! + X^3/3! + \cdots \in \mathbb{Q}_p[[X]].$$

If $p \neq 2$, then, for all $x \in p\mathbb{Z}_p$, the series $exp(x)$ converges to an element of U_1. If $p = 2$, then for all $x \in 4\mathbb{Z}_2$, the series $exp(x)$ converges to an element of U_2.

PROOF. The proposition follows if $|x^n/n!| \to 0$, under the given conditions. When $x \in p\mathbb{Z}_p$, we see that $|x^n| < p^{-n}$. Moreover, counting multiples of p, p^2, p^3, et cetera, in $n!$, yields:

$$v_p(n!) < n/p + n/p^2 + n/p^3 + \cdots \leq n\left(\frac{1}{p-1}\right).$$

Hence we compute:

$$|x^n/n!| < p^{n(2-p)/(p-1)} \to 0,$$

as $n \to \infty$ if $p > 2$. This yields convergence. Every partial sum is in U_1, so the limit is in U_1, since U_1 is compact.

When $p = 2$, and $x \in 4\mathbb{Z}_2$, we have:

$$|x^n/n!| < 2^{n(3-2p)/(p-1)} \to 0.$$

Again, convergence is guaranteed. Every partial sum is in U_2, so the limit is in U_2, since U_2 is compact. □

PROPOSITION 3.2. *Define the formal power series:*

$$log(X) = (X-1) - (X-1)^2/2 + (X-1)^3/3 - (X-1)^4/4 \cdots \in \mathbb{Q}_p[[X-1]].$$

If $p \neq 2$, then for all $x \in U_1$, the series $log(x)$ converges to an element of $p\mathbb{Z}_p$. If $p = 2$, then for all $x \in U_2$, the series $log(x)$ converges to an element of $4\mathbb{Z}_2$.

PROOF. When $p \neq 2$, and $x \in U_1$, we have $x - 1 \in p\mathbb{Z}_p$. It follows that:

$$|(x-1)^n/n| \leq np^{-n} \to 0.$$

It is also true that every term is in $p\mathbb{Z}_p$ in this case. Hence the sum converges to an element of $p\mathbb{Z}_p$. The case $p = 2$ is similar; □

One can check, using partial sums and continuity, the following facts about *exp* and *log* in this setting:

- *exp* is a homomorphism from $p\mathbb{Z}_p$ (or $4\mathbb{Z}_2$), under addition, to U_1 (or U_2) under multiplication.
- *log* is a homomorphism from U_1 (or U_2) to $p\mathbb{Z}_p$ (or $4\mathbb{Z}_2$).
- $log \circ exp = Id$ and $exp \circ log = Id$, on the appropriate domains.
- Both *log* and *exp* are continuous functions.

These yield the isomorphisms discussed by Serre:

THEOREM 3.3. *The group U_1 is topologically isomorphic to $p\mathbb{Z}_p$, when $p \neq 2$. The group U_2 is topologically isomorphic to $4\mathbb{Z}_2$, when $p = 2$.*

3.2. Structure of the group U_1. In the Corollary of Serre, he notes that the field $\mathbb{Q}_p$ contains the $(p-1)^{th}$ roots of unity (when $p \neq 2$ to make this meaningful). This can be seen by "amelioration" as follows: the polynomial $f(X) = X^{p-1} - 1$ has $p-1$ distinct roots in $\mathbb{F}_p$. Since these roots are not repeated, they are not roots of the derivative. Hence every root may be lifted to a distinct root in $\mathbb{Z}_p$. Thus we get a map: $\omega \colon \mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$. Note that only the root $1 \in \mathbb{F}_p^\times$ maps to an element of U_1. It follows that:

- $\omega(\mathbb{F}_p^\times) \cap U_1 = 1$.
- $\omega(\mathbb{F}_p^\times) \cdot U_1 = \mathbb{Z}_p^\times$. Indeed, every element of $\mathbb{Z}_p^\times$ can be multiplied by ω of the inverse of its units digit, to arrive at an element of U_1.

Hence, there is a group isomorphism:

$$\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times U_1 \cong \mathbb{F}_p^\times \times p\mathbb{Z}_p \cong \mathbb{F}_p^\times \times \mathbb{Z}_p.$$

Here, the last isomorphism comes from the group isomorphism $\mathbb{Z}_p \cong p\mathbb{Z}_p$ via multiplication by p.

A similar argument yields an isomorphism:

$$\mathbb{Z}_2^\times \cong \{\pm 1\} \times U_2 \cong \{\pm 1\} \times 4\mathbb{Z}_2 \cong \{\pm 1\} \times \mathbb{Z}_2.$$

Finally, every element of $\mathbb{Q}_p^\times$ can be uniquely expressed as $p^n u$, for $u \in U = \mathbb{Z}_p^\times$. Theorem 2 of Serre follows immediately:

THEOREM 3.4. *If $p \neq 2$, then $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{F}_p^\times \times \mathbb{Z}_p$. If $p = 2$, then $\mathbb{Q}_2^\times \cong \mathbb{Z} \times \{\pm 1\} \times \mathbb{Z}_2$.*

3.3. Squares in $\mathbb{Q}_p^\times$. Knowing the structure of the groups $\mathbb{Q}_p^\times$, and having specific isomorphisms, allows us to identify the squares. We begin, as Serre does in Theorem 3, with the easier case when $p \neq 2$. In this case, we can identify $\mathbb{Q}_p^{\times 2}$ with the group

$$2\mathbb{Z} \times \mathbb{F}_p^{\times 2} \times 2\mathbb{Z}_p.$$

Note that $2\mathbb{Z}_p = \mathbb{Z}_p$, since 2 is invertible in $\mathbb{Z}_p$ (since $p \neq 2$). Thus, the squares are identified with $2\mathbb{Z} \times \mathbb{F}_p^{\times 2} \times \mathbb{Z}_p$. Thus the squares in $\mathbb{Q}_p^\times$ have the form $p^{2k} \cdot \omega(s) \cdot exp(z)$, where $k \in \mathbb{Z}$, and $s \in \mathbb{F}_p^{\times 2}$, and $z \in p\mathbb{Z}_p$ is arbitary.

Alternatively, since $exp(p\mathbb{Z}_p) = 1 + p\mathbb{Z}_p$, we can characterize the squares as follows:

PROPOSITION 3.5. *An element x of $\mathbb{Q}_p^\times$ is a square if $val(x)$ is even, and the final nonzero digit of x is a quadratic residue, mod p.*

In particular, we see a Corollary of Serre:

$$\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

In other words, there are two ways for an element of $\mathbb{Q}_p^\times$ to fail to be a square – its valuation could be odd, or it could have a nonsquare last digit (or both!)

Knowing the structure of the group $\mathbb{Q}_2^\times$ allows us to understand the squares here as well. The squares correspond to elements of the subgroup:

$$2\mathbb{Z} \times \{1\} \times 2\mathbb{Z}_2 \subset \mathbb{Z} \times \{\pm 1\} \times \mathbb{Z}_2.$$

In particular, the squares correspond to all elements of the form $2^{2k} \cdot exp(z)$, where $z \in 8\mathbb{Z}_2$. Since $exp(8\mathbb{Z}_2) = U_3 = 1+8\mathbb{Z}_2$, we can characterize the squares as follows:

PROPOSITION 3.6. *An element x of $\mathbb{Q}_2^\times$ is a square if $val(x)$ is even, and the final three digits of x are* 001.

This is another way of phrasing Theorem 4 of Serre.

As a Corollary, we get:

$$\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

In other words, there are three ways for an element of $\mathbb{Q}_2^\times$ to fail to be a square – its valuation could be odd, its second-to-last digit could be 1, or its third-to-last digit could be 1.

CHAPTER 3

Hilbert Symbol

1. Local Properties

This section describes the Hilbert symbol, on the fields $\mathbb{R}$ or $\mathbb{Q}_p$ when p is a prime number. We begin by describing "symbols" in more generality.

Suppose that k is a field, and $k^\times$ is the abelian group ($\mathbb{Z}$-module) of invertible elements in k. Then we may consider the group:

$$k^\times \otimes_{\mathbb{Z}} k^\times.$$

It is quite confusing to work in this group, since composition is denoted by multiplication in $k^\times$, but usually by addition in $\mathbb{Z}$-modules. We give a sample of some identities in $k^\times \otimes_{\mathbb{Z}} k^\times$:

- $x^2 \otimes y = x \otimes y^2$.
- $x^{-1} \otimes y = -(x \otimes y)$.
- $x_1 \otimes y + x_2 \otimes y = (x_1 x_2) \otimes y$.

Within the group $k^\times \otimes_{\mathbb{Z}} k^\times$, we consider the subgroup generated by all elements $u \otimes (1-u)$, where $u \neq 0, 1$. The quotient is called $K_2(k)$:

$$K_2(k) = \frac{k^\times \otimes_{\mathbb{Z}} k^\times}{\langle u \otimes (1-u) \rangle_{u \neq 0,1}}.$$

A degree d *symbol* on k is a homomorphism $\sigma\colon K_2(k) \to \mathbb{Z}/d\mathbb{Z}$. In particular, we think of a quadratic symbol as a homomorphism from $K_2(k)$ to $\mathbb{Z}/2\mathbb{Z}$, or equivalently to $\{1, -1\}$. Since a symbol is determined by its values on simple tensors, we are really interested in:

$$(a, b)_\sigma = \sigma(a \otimes b),$$

for $a, b \in k^\times$. Any quadratic symbol satisfies the following basic properties:

- $(a, b^2) = 1$ and $(a^2, b) = 1$, for all $a, b \in k^\times$.
- $(a, 1-a) = 1$ for all $a \in k^\times$.
- $(ab, c) = (a, c)(b, c)$ for all $a, b, c \in k^\times$.
- $(a, bc) = (a, b)(a, c)$ for all $a, b, c \in k^\times$.

Conversely, any function $(\cdot, \cdot)$ from $k^\times \times k^\times$ to ± 1, satisfying the above four properties (actually, the last three suffice), arises from a unique quadratic symbol.

In particular, note that any quadratic symbol depends only on the cosets of $k^\times / k^{\times 2}$. Thus, the symbol can be viewed as a function:

$$(\cdot, \cdot)\colon k^\times / k^{\times 2} \times k^\times / k^{\times 2} \to \{\pm 1\}.$$

For any field k, the abelian group $k^\times / k^{\times 2}$ can be viewed as an $\mathbb{F}_2$-vector space, since it is two-torsion. We call this vector space S_k. The abelian group $\{\pm 1\}$, can also be

viewed as the additive group of $\mathbb{F}_2$. The "bilinearity" relations $(ab, c) = (a, c)(b, c)$ and $(a, bc) = (a, b)(a, c)$ show that a quadratic symbol yields a bilinear form:

$$\langle \cdot, \cdot \rangle \colon S_k \otimes_{\mathbb{F}_2} S_k \to \mathbb{F}_2.$$

This captures almost all of the properties of the symbol - except the "strange" property that $(a, 1 - a) = 1$. The strange property somehow sees the interaction between addition and multiplication in the field k.

1.1. Definition and first properties. The Hilbert symbol for $k = \mathbb{Q}_p$ or $\mathbb{R}$ is given by Serre as follows:

$$(a, b) = 1, \text{ if } z^2 - ax^2 - by^2 = 0 \text{ has a solution } (x, y, z) \neq (0, 0, 0) \in k^3,$$

and $(a, b) = -1$ otherwise. We only consider (a, b) when $a, b \in k^\times$. In fact, this is the definition of the Hilbert symbol for finite extensions of $\mathbb{Q}_p$, or $\mathbb{C}$ as well. Of course, for $\mathbb{C}$, we have $(a, b) = 1$ for all a, b.

When a or b is a square, it is clear that $(a, b) = 1$. Indeed, if $c^2 = b$, then we have $x = 0, y = 1, z = c$ as a solution. Thus, it suffices to consider the Hilbert symbol when neither a nor b is a square.

Remarks on: Proposition 1

Proposition 1 states that $(a, b) = 1$ if and only if $a \in N(k(\sqrt{b})^\times)$, where N denotes the norm map. Of course, when $b = 1$, $k(\sqrt{b}) = k$, and the norm map is trivial, so $(a, b) = 1$ without any further consideration.

When b is not a square, $k_b = k(\sqrt{b})$ is a quadratic extension of k. Every element of $k(\sqrt{b})$ can be written as $z + \beta y$, where $\beta = \sqrt{b}$. The norm is given by: $N(z + \beta y) = z^2 - by^2$. If a is such a norm, then we have:

$$a = z^2 - by^2.$$

It follows that $x = 1, y, z$ is a solution to the Diophantine equation. Thus if $a \in N(k_b^\times)$, then $(a, b) = 1$.

Conversely, if $(a, b) = 1$, we have a solution $z^2 - ax^2 - by^2 = 0$, with x, y, z not all zero. If $x = 0$, then b would be a square, contradicting our initial assumption. Dividing through by x^2, yields $z^2 - a - by^2 = 0$, and $a = z^2 - by^2$, a norm.

Note that the nature of the field k was used nowhere in this proof, except perhaps that $char(k) \neq 2$.

Remarks on: Proposition 2

The properties of the Hilbert symbol are the following:

- The Hilbert symbol is a quadratic symbol.
- The Hilbert symbol is symmetric (as a bilinear form over $\mathbb{F}_2$). In other words, $(a, b) = (b, a)$.
- $(a, -a) = 1$.
-

These properties are proven in a somewhat weird (but perhaps unavoidable) order in Serre.

(1) The definition of the Hilbert symbol is symmetric. It is thus clear that $(a, b) = (b, a)$ for all $a, b \in k^\times$.
(2) We have already seen that $(a, b^2) = (a^2, b) = 1$, for all $a, b \in k^\times$.
(3) We have $(a, -a) = 1$, since the equation $z^2 - ax^2 + ay^2$ has the solution $x = 1, y = 1, z = 0$.

(4) We have $(a, 1-a) = 1$, since the equation $z^2 - ax^2 + ay^2 - y^2$ has the solution $x = 1, y = 1, z = 1$.

Weak bilinearity If $(a, b) = 1$, then $(aa', b) = (a', b)$. Indeed, if $(a, b) = 1$, then a is a norm from k_b. Hence aa' is a norm from k_b if and only if a' is a norm from k_b, since these norms form a group.

Bilinearity will follow from explicit formulae later. It can almost be seen from looking at norms. We would like to show that $(aa', b) = (a, b)(a', b)$. If both a, a' are norms from k_b, then $a \cdot a'$ is also a norm from k_b. Similarly, if a is a norm, and a' is not a norm, then $a \cdot a'$ is not a norm. These facts follow from the fact that $N(k(\sqrt{b})^\times)$ is a group. The only thing remaining is to show that if a, a' are both *not* norms from k_b, then aa' *is* a norm. We will be done showing bilinearity if we can prove:

PROPOSITION 1.1. *The index of $Nk_b^\times$ in $k^\times$ is equal to two.*

1.2. Computation of (a, b). Explicit computation of (a, b) will show that the Hilbert symbol is bilinear and non-degenerate. When $k = \mathbb{R}$, it is easy to compute. For, if we consider the equation $z^2 = ax^2 + by^2$, the graph is a double-cone, unless both a, b are negative. In particular, there are nonzero solutions (x, y, z), unless a, b are negative. Hence:

$$(a, b) = 1 \text{ if } a > 0 \text{ or if } b > 0,$$

and $(a, b) = -1$ if both $a, b < 0$.

Remarks on: Theorem 1

We begin by proving the formula for the Hilbert symbol when p is an odd prime:

PROPOSITION 1.2. *If p is an odd prime, and $a = p^\alpha u$, and $b = p^\beta v$, where $\alpha, \beta \in \mathbb{Z}$, and $u, v \in \mathbb{Z}_p^\times$, then:*

$$(a, b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

PROOF. Since (a, b) depends only on a, b modulo $\mathbb{Q}_p^{\times 2}$, there are four cases to consider for a, b. We must consider four cases each for a and b:

$$a, b \in \{1, p, u, up\},$$

where $0 < u \leq p - 1$ is any fixed non-square, mod p. Since the Hilbert symbol is symmetric, and $(1, x) = (x, 1) = 1$ for all $x \in \mathbb{Q}_p^\times$, this reduces to the following cases:

$$(p, p), (p, u), (p, up), (u, u), (u, up), (up, up).$$

We compute these cases, like Serre does:

- Consider the equation $z^2 - ux^2 - uy^2 = 0$. Modulo p, it has a solution $(x, y, z) \in \mathbb{F}_p$, since it is a homogeneous quadratic in 3 variables, by the Chevalley-Waring theorem. Since $p \neq 2$, at least one of the partial derivatives of $f(x, y, z) = z^2 - ux^2 - uy^2$ does note vanish; this implies that the solution lifts to a solution in $\mathbb{Z}_p$. Hence $(u, u) = 1$.
- Consider the symbol (u, up). Since $(u, u) = 1$, we have $(u, up) = (u, p)$ by "weak bilinearity". Thus, computing (u, up) and (u, p) can be done at once. To compute (u, p), we consider the Diophantine equation:

$$z^2 - px^2 - uy^2 = 0$$

. If it has a solution, it has a solution where x, y, z are in $\mathbb{Z}_p$, and not all are divisible by p. In this case, y is not divisible by p, since otherwise, z would be divisible by p, and px^2 would necessarily be divisible by p^2, so x would be divisible by p, a contradiction.

Hence, $(u, p) = 1$ if and only if there exists a solution to $z^2 - px^2 - uy^2 = 0$, with y and z not divisible by p. But in this case, reducing mod p yields $z^2 = uy^2$, so u would have to be a square, mod p. This is a contradiction. Hence $(u, p) = -1$.

- Consider (up, up). We have:

$$(up, up) = (up, -up)(up, up) = (up, -u^2p^2) = (up, -1).$$

If -1 is a square, mod p, then $(up, up) = 1$. Otherwise, by the previous item, $(up, -1) = (up, u) = -1$.

- Consider (p, p). We have:

$$(p, p) = (p, -p)(p, p) = (p, -p^2) = (p, -1).$$

Again, if -1 is a square, mod p, then $(p, p) = 1$. Otherwise, $(p, -1) = (p, u) = -1$.

- Finally, consider (p, up). We have:

$$(p, up) = (p, -p)(p, up) = (p, -up^2) = (p, -u).$$

If -1 is a nonsquare, mod p, then $(p, -u) = (p, 1) = 1$. Otherwise, if -1 is a square, then $(p, -u) = (p, u) = -1$.

One may check directly that the formula in Theorem 1 holds. We also can write the Hilbert symbol as a bilinear form, using the above computations.

We fix a $\mathbb{F}_2$-vector space structure on $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ as follows. A basis will be given by $\{\bar{u}, \bar{p}\}$. Note that vector space addition of $\bar{u}$ and $\bar{p}$ corresponds to the product $\overline{up}$, where "bar" denotes the map from $\mathbb{Q}_p^\times$ to the $\mathbb{F}_2$ vector space $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

With respect to the basis $\{\bar{u}, \bar{p}\}$, the matrix of the bilinear form is:

$$Hil_p = \begin{pmatrix} (u,u) & (u,p) \\ (p,u) & (p,p) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & (p-1/2) \mod 2 \end{pmatrix}.$$

Note that in the above matrix of numbers, we are replacing the group elements ± 1 by the additive group elements $0, 1$ in $\mathbb{F}_2$. The bilinear form is nondegenerate, since the determinant is equal to 1, regardless of p.

When $p = 2$, the computations are more complicated. The $\mathbb{F}_2$-vector space $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is three-dimensional. Thus, we must compute (a, b) for 8 possible values of a, and 8 possible values of b. After excluding $a = 1$ and $b = 1$, and using symmetry, we are left with "7 choose 2" or 21 pairs (a, b) to check. Weak bilinearity and the relation $(a, -a) = 1$ reduces this further – Serre performs such a reduction, but in the end, a case-by-case analysis is required.

2. Global Properties

Notes by: Filix Maisch This section makes use of the embedding of $\mathbb{Q}$ into $\mathbb{Q}_v$, where v is a prime or ∞, adopting the convention that $\mathbb{Q}_\infty$ is equal to $\mathbb{R}$. For $a, b \in \mathbb{Q}^\times$ we let $(a, b)_v$ denote the Hilbert symbol on the images of a,b in $\mathbb{Q}_v$. We shall let V (set of places) denotes the set of primes union the infinity symbol.

THEOREM 2.1. *If $a, b \in \mathbb{Q}^\times$, then $(a,b)_v = 1$ for all but finitely many $v \in V$ and*

$$\prod_{v \in V} (a,b)_v = 1.$$

Remarks on: Theorem 2.1
In the following proof it is good to note that we have explicit formulas for the Hilbert symbol through the Legendre symbol. For any two a,b in the form $p^\alpha u$, $p^\beta v$ respectively, where u and v are p-adic units we have the following:

- $(a,b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$ if $p \neq 2$
- $(a,b)_p = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}$ if $p = 2$

PROOF. The Hilbert symbol is bilinear, which implies that it suffices to show the theorem for a,b equal to -1 or a prime. This is done via cases:

(1) $(a = b = -1)$ Then $(-1,-1)_\infty = -1 = (-1,-1)_2$ and $(-1,-1)_v = 1$ for all $v \neq 2, \infty$.
(2) $(a = -1, b = l$ with l a prime) If $l = 2$, then $(-1,2)_v = 1$ for all $v \in V$. If $l \neq 2$, then $(-1,l)_v = 1$ for all $v \neq 2, l$ and $(-1,l)_2 = (-1,l)_l = (-1)^{\epsilon(l)}$
(3) $(a = l, b = l'$ with both l and l' primes) If $l = l'$, then proposition 2.2 (iv) implies $(l,l')_v = (-1,l')_v$ for all $v \in V$ and so that brings us back to case number 2. If $l \neq l' = 2$, then $(l,2)_v = 1$ for all $v \neq 2, l$ while $(l,2)_2 = (-1)^{\omega(l)}$ and $(l,2)_l = \left(\frac{2}{l}\right) = (-1)^{\omega(l)}$. If $l \neq l'$ and both are not 2, then one has $(l,l')_v = 1$ for all $v \neq 2, l, l'$ and moreover we have that $(l,l')_2 = (-1)^{\epsilon(l)\epsilon(l')}; (l,l')_l = \left(\frac{l'}{l}\right); (l,l')_{l'} = \left(\frac{l}{l'}\right)$. By quadratic reciprocity, we have that $\left(\frac{l}{l'}\right)\left(\frac{l'}{l}\right) = (-1)^{\epsilon(l)\epsilon(l')}$ which implies that the product is one.

□

Note that quadratic reciprocity is equivalent to this theorem about the global Hilbert symbol. The next theorem considers the existence of rational numbers with given Hilbert symbols. The theorem will follow from three lemmas, including the Chinese remainder theorem.

2.1. Existence of rational numbers with given Hilbert symbols.

THEOREM 2.2. *Let $(a_i)_{i \in I}$ be a finite family in $\mathbb{Q}^x$ and let $(\epsilon_{i,v})_{i \in I, v \in V}$ be a family of numbers equal to ± 1. In order that there exists $x \in \mathbb{Q}^x$ such that $(a_i, x)_v = \epsilon_{i,v}$ for every i,v it is necessary and sufficient that*

(1) *All but finitely many $\epsilon_{i,v} = 1$.*
(2) *For all $i \in I$,*

$$\prod_{v \in V} \epsilon_{i,v} = 1$$

(3) *For all $v \in V$ there exists $x_v \in \mathbb{Q}_v^x$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all $i \in I$.*

Remarks on: Theorem 2.2
The necessity of (1) follows from theorem 2.1 and is clear, because otherwise the product would not be well-defined, it could simply alternate forever. The necessity of (2) also follows from theorem 2.1, and (2) is really the important global condition. In other words, (2) is a parity condition, revealing that for a given i, the finite

number of $\epsilon_{i,v} = -1$ is precisely even. The necessity of (3) is easy, just set $x_v = x$ for every v, after all (3) is really just the local version of the theorem. It is to prove sufficiency of these conditions that requires the three lemmas.

The first lemma is the Chinese remainder theorem. Remarks on: First lemma We use the form of this theorem that states that for any list of integers $a_i, i = 1, ..., n$ and any list of pairwise relatively prime integers $m_i, i = 1, ..., n$ there exists an integer a, such that $a \equiv a_i (mod\ m_i)$ for all $i = 1, ..., n$.

The second lemma is the so-called Approximation theorem. Remarks on: Second lemma and its proof
This lemma basically states that for any finite set of places, that is a finite subset S of V, the of image of the rational numbers is dense in the product of the p-adics for p in S. To prove this, we simply suppose that

$$S = \{\infty, p_1, ..., p_n : \text{ such that } p_i \text{ are distinct primes}\}.$$

This is without loss of generality, since if the rational numbers are dense over a larger product space, then they are dense over any subset of that space. So we may enlarge S and assume the above.

Next we pick a point in the product space over S, say $(x_\infty, x_1, ..., x_n)$, and via multiplication by some integer, we may assume that the $x_i \in \mathbb{Z}_{p_i}$ for $i = 1, .., n$. We let ϵ be any positive real number and N be any natural number. By lemma 1 (Chinese remainder theorem) there exists some $x_0 \in \mathbb{Z}$ such that $\nu_{p_i}(x_0 - x_i) \geq N$ for all i. This follows from the existence of $x_0 \in \mathbb{Z}$ such that $x_0 \equiv x_i \pmod{p_i^N}$. Now an integer $q \geq 2$ is chosen relatively prime to all the p_i. Rational numbers of the form $\frac{a}{q^m}$ with $a \in \mathbb{Z}$ and m some non-negative number are dense among the real numbers. This follows from the divergence of q^m as m goes to infinity. So we find a number $u = \frac{a}{q^m}$ such that $|x_0 - x_\infty + up_1^N ... p_n^N| \leq \epsilon$. So if we set $x = x_0 + up_1^N ... p_n^N$ we have the desired effects:

$$|x - x_\infty| \leq \epsilon, \text{ and,}$$
$$\nu_{p_i}(x - x_i) \geq N$$

The next lemma is called the Dirichlet theorem, and Serre postpones the proof until chapter 4. This lemma gives us, for relatively prime integers greater than or equal to one, a and m, there exists infinitely many primes such that the prime is congruent to $a \pmod{m}$.

Finally we can tie together these ideas to prove the sufficiency of the conditions of the theorem 2.2. We let $(\epsilon_{i,v})$ be a family of numbers satisfying (1),(2), and (3). Via multiplication by square of some integer (recall Hilbert symbol is trivial on squares) we may assume that the a_i are integers. So we let

$$S = \{\infty, 2\} \cup \{ \text{ prime factors of } a_i\},$$
$$T = \{v \in V : \exists i \in I, \epsilon_{i,v} = -1\}.$$

Note that both sets above are clearly finite. The argument now splits into two cases.

1) $S \cap T = \emptyset$: We set the following:

$$a = \prod_{l \in T, l \neq \infty} l \text{ and}$$
$$m = 8 \prod_{l \in S, l \neq 2, \infty} l.$$

Since the intersection of S and T is empty, clearly a and m are relatively prime. By lemma 3, there must exist a prime $p \notin S \cup T$ such that $p \equiv a(\mod m)$ – There are infinitely many such primes, so of course we can choose one outside of any finite set of places, like $S \bigcup T$. We want to show that $x = ap$ will have the desired property and satisfy theorem 2.2.

If $v \in S$ then $v \notin T$ implying that $\epsilon_{i,v} = 1$. So we must check that $(a_i, x)_v = 1$. If $v = \infty$, this follows from the fact $x > 0$. If $v = l$, a prime, then $x \equiv a^2(\mod m)$, and hence we have that $x \equiv a^2 \pmod 8$ if l=2 and $x \equiv a^2 \pmod l$ if $l \neq 2$. Since x and a are l-adic units this shows that x is a square in $\mathbb{Q}_l^x$ implying $(a_i, x)_v = 1$.

If $v = l \notin S$, a_i is an l-adic unit. Since $l \neq 2$,

$$(a_i, b)_l = \left(\frac{a_i}{l}\right)^{\nu_l(b)}.$$

If $l \notin T \cup \{p\}$, x is an l-adic unit, hence $\nu_l(x) = 0 \implies (a_i, x)_l = 1$. On the other hand we have that $\epsilon_{i,l} = 1$ because l is not in T. If $l \in T$ then $\nu_l(x) = 1$. (3) $\implies \exists x_l \in \mathbb{Q}_l^x$ such that $(a_i, x_l)_l = \epsilon_{i,l}$ for all i; since one of the $\epsilon_{i,l} = -1$ for some i, $\nu_l(x_l) = 1 \pmod 2 \implies (a_i, x)_l = \left(\frac{a_i}{x_l}\right) = (a_i, x_l)_l = \epsilon_{i,l}$ for all i. If l=p then we deduce using the product formula that:

$$(a_i, x)_p = \prod_{v \neq p} (a_i, x)_v = \prod_{v \neq p} \epsilon_{i,v} = \epsilon_{i,p}$$

and so we have shown the sufficiency of (1),(2), and (3) when the intersection of S and T is empty.

2) General case.

We have from chapter 2 that the $(\mathbb{Q}_v^x)^2$ form an open subgroup of $\mathbb{Q}_v^x$. By lemma 2, there exists some $x' \in \mathbb{Q}^x$ such that x'/x_v is a square in $\mathbb{Q}_v^x$ for all v. So we have that $(a_i, x')_v = (a_i, x_v)_v = \epsilon_{i,v}$ for all v. If we set $\eta_{i,v} = \epsilon_{i,v}(a_i, x')_v$ the family $(\eta_{i,v})$ verifies (1),(2), and (3) and is equal to one if v is in S. Now by the first case we have that there exists $y \in \mathbb{Q}^x$ such that $(a_i, y)_v = \eta_{i,v}$ for all i and for all v. If we set $x = yx'$ it is clear we are done.

CHAPTER 4

Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

1. Quadratic Forms

1.1. Definitions. Serre begins by discussing quadratic forms over an arbitrary commutative ring. If 2 is invertible in a commutative ring A, then quadratic forms are essentially interchangable with symmetric bilinear forms. But if 2 is not invertible, then there is an important distinction. We emphasize that this subtlety arises, not only in the case of a field of characteristic 2, but also for rings, such as $\mathbb{Z}$, in which 2 is not invertible!

Following Serre, we recall the definitions of quadratic modules, symmetric bilinear forms, and the connection between the two:

DEFINITION 1.1. A quadratic module (over a commutative ring A) is a pair (V, Q), where V is a module over A, and $Q\colon V \to A$ is a function satisfying $Q(ax) = a^2Q(x)$, for all $a \in A, x \in V$, and such that $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.

If 2 is invertible in A, and (V, Q) is a quadratic module over A, we write B_Q for the associated symmetric bilinear form on V:

$$B_Q(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)).$$

Note the important factor $1/2$ in the definition of B_Q. Conversely, if B is a symmetric bilinear form on an A-module V, we write

$$Q_B(x) = B(x, x).$$

This establishes a bijection between symmetric bilinear forms and quadratic modules. In fact, this bijection is *functorial*. One may define two categories, $\mathfrak{QMod}_A$ and $\mathfrak{SBil}_A$, whose objects are quadratic modules and symmetric bilinear forms over A, respectively, and whose morphisms are A-module homomorphisms preserving the quadratic form or symmetric bilinear form.

In this chapter, Serre works over a field k, with $char(k) \neq 2$. This implies that we may pass freely between quadratic modules and symmetric bilinear forms. Moreover, this implies that "modules" are vector spaces, and hence are determined up to isomorphism by their dimension. We also assume that these vector spaces are finite-dimensional.

Working over a vector space V, over such a field k, we may always choose a basis $\{e_i\}$. If Q is a quadratic form on V, then we let $q_{ij} = B_Q(e_i, e_j)$ be the associated matrix. This is called the matrix of Q, corresponding to the basis e_i. Changing basis changes the matrix in a non-trivial way. Namely, if $g \in GL(V)$ denotes a change of basis matrix, then the matrix of Q corresponding to the new basis is $g \cdot (q_{ij}) \cdot {}^t g$.

In particular, the *square-class* of the determinant of q_{ij} depends only on Q, and not on the choice of basis. This square-class is called the discriminant: Either $disc(Q) = 0$ or else, $disc(Q) \in k^\times/k^{\times 2}$.

1.2. Orthogonality. Serre continues discussing basic facts about quadratic forms, over fields k with $char(k) \neq 2$. As before, V will be a vector space, with quadratic form Q. We write B_Q for the associated bilinear form (as opposed to Serre, who simply writes $x.y$ where we would write $B(x, y)$).

We also differ in notation from Serre. We write $x \perp y$ if $B_Q(x, y) = 0$, and we say that x and y are orthogonal (or perpindicular). If H is a subset of V, then we write $H^\perp$ for the set of elements orthogonal to every element of H. If V_1, V_2 are subspaces of V, we write $V_1 \perp V_2$ if $V_1 \subset V_2^\perp$ (or equivalently $V_2 \subset V_1^\perp$.

We write $rad(V) = V^\perp$. If $rad(V) = \{0\}$, then Q is called *non-degenerate*.

The bilinear form B_Q induces a k-linear map:

$$D_Q \colon V \to V' = Hom_k(V, k).$$

This is given by:

$$[D_Q(x)](y) = B_Q(x, y).$$

The following are equivalent:

- Q is non-degenerate.
- $disc(Q) \neq 0$.
- D_Q is an isomorphism of k-vector spaces.

In Definition 2, Serre discusses the direct sum of quadratic modules. In fact, there is also a tensor product of quadratic modules as well. We define both of these here:

Definition 1.2. Suppose that (V_1, Q_1) and (V_2, Q_2) are two quadratic modules over k. There are natural quadratic modules $(V_1 \oplus V_2, Q_1 \oplus Q_2)$, and $(V_1 \otimes V_2, Q_1 \otimes Q_2)$, where the quadratic forms are defined by:

- $(Q_1 \oplus Q_2)(v_1, v_2) = Q_1(v_1) + Q_2(v_2)$.
- $(Q_1 \otimes Q_2)(\sum_i v_1^i \otimes v_2^i) = \sum_{i,j} B_{Q_1}(v_1^i, v_1^j) B_{Q_2}(v_2^j, v_2^j)$.

When (V, Q) is a quadratic module, and U_1, U_2 are subspaces of V, we may decompose (V, Q) as a direct sum under the following conditions:

- $V = U_1 \oplus U_2$, as vector spaces. In other words, $U_1 + U_2 = V$ and $U_1 \cap U_2 = \{0\}$.
- $Q(u_1 + u_2) = Q(u_1) + Q(u_2)$, for all $u_1 \in U_1$, $u_2 \in U_2$.

Serre write $V = U_1 \hat{\oplus} U_2$, when V is the direct sum of U_1 and U_2, and the quadratic form satisfies the above conditions. In this case, (V, Q) is isomorphic to $(U_1, Q|_{U_1}) \oplus (U_2, Q|_{U_2})$.

Remarks on: Proposition 2

Proposition 2 discusses a number of consequences of non-degeneracy. If (V, Q) is non-degenerate, then:

(1) All morphisms ϕ from (V, Q) to another quadratic module (V', Q') are injective. Indeed, $ker(\phi)$ would clearly be in $Rad(V) = \{0\}$.
(2) If U is a vector subspace of V, then $U^{\perp\perp} = U$, and $dim(U) + dim(U^\perp) = dim(V)$, and $Rad(U) = Rad(U^\perp) = U \cap U^\perp$.

(3) If V is the orthogonal sum of two subspaces, then each of them is nondegenerate.

The first item is obvious. The second item follows from "playing with duality". Recall that we have an isomorphism $D_Q \colon V \to V'$, which is an isomorphism. When U is a subspace of V, there is a canonical projection $p_U \colon V' \to U'$. It is surjective, since functionals on U can always be extended to functionals on V. Thus we get a surjection $V \to U'$, given by $p_U \circ D_Q$. The kernel is easily seen to be $U^\perp$. Thus we have:

$$0 \to U^\perp \to V \to U' \to 0.$$

This yields the dimension identity

$$dim(U) + dim(U^\perp) = dim(U') + dim(U^\perp) = dim(V).$$

It is important to note that $V \neq U \oplus U^\perp$, in general! It follows that $dim(U) = dim(U^{\perp\perp})$. It is clear that $U \subset U^{\perp\perp}$, and hence $U = U^{\perp\perp}$. Since $rad(U) = U \cap U^\perp$ (by chasing the definition), we have

$$rad(U^\perp) = U^\perp \cap U^{\perp\perp} = U^\perp \cap U.$$

Hence $rad(U) = rad(U^\perp)$.

The third item is not particularly difficult. In fact, if $V = U_1 \hat{\oplus} U_2$, then:

$$Rad(V) = Rad(U_1) \oplus Rad(U_2).$$

Thus $Rad(V) = \{0\}$ if and only if the same is true of U_1 and U_2.

1.3. Isotropic Vectors. An isotropic vector in a quadratic module (V, Q) is simply a vector v satisfying $Q(v) = 0$. Such vectors form a "quadric hypersurface" in V. More generally, a subspace $U \subset V$ is called isotropic if all of its vectors are.

A "hyperbolic plane" is a quadratic module of rank two, which is isomorphic to (k^2, η), where $\eta(x, y) = xy$. Equivalently, a hyperbolic plane is a quadratic module (V, Q) of rank two, which has a basis of isotropic vectors v_1, v_2, satisfying $B_Q(v_1, v_2) \neq 0$. Its discriminant is -1.

Remarks on: Proposition 3

Proposition 3 essentially says that in a non-degenerate quadratic module, every nonzero isotropic vector is contained in a hyperbolic plane. It is proven by construction. If v is a nonzero isotropic vector, non-degeneracy yields a second vector w with $B_Q(v, w) = 1$. Note that non-degeneracy also implies that $dim(V) > 1$. The trick is to set:

$$y = 2w - Q(w)v.$$

Then:

$$Q(y) = 4Q(w) + Q(w)^2 Q(v) + 2B_Q(2w, -Q(w)v) = 4Q(w) - 4Q(w)B_Q(w, v) = 0.$$

Hence y is isotropic. The span of v and w is a hyperbolic plane.

Remarks on: Corollary

Hyperbolic planes "represent" every number. This corollary is the first about representations by a quadratic form. If $x \in k$, and (V, Q) is a quadratic module, we say that Q represents x if there exists $v \in V$ satisfying $Q(v) = x$. The quadratic module (k^2, eta), with $\eta(x, y) = xy$ clearly represents every element of k. Hence any quadratic module with an embedded hyperbolic plane represents every element of k. Hence every non-degenerate quadratic module, with at least one isotropic vector, represents every element of k.

1.4. Orthogonal Basis. The existence of an orthogonal basis for a quadratic module allows us to "get our hands dirty". A basis $e_1, \ldots, e_n$ is called an orthogonal basis of a quadratic module (V, Q), if it is a basis, and $e_i \perp e_j$ whenever $i \neq j$. In this case, $V = e_1 k \hat{\oplus} \cdots \hat{\oplus} e_n k$. Thus, the quadratic form Q is completely determined by its values $a_i = Q(e_i)$. In other words, the quadratic module can be identified with k^n, with the quadratic form:

$$Q(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2.$$

In this case, rather than writing (V, Q) and discussing quadratic modules, we write $[a_1, a_2, \ldots, a_n]$ for the associated quadratic form on k^n.

Remarks on: Theorem 1

This theorem says that every quadratic module has an orthogonal basis. It allows us to restrict our studies to quadratic forms $[a_1, \ldots, a_n]$, for various $a_i \in k$. Its proof is not difficult – in linear algebra classes, one usually uses the Gram-Schmidt process. The proof in Serre is somewhat slicker.

The proof is inductive on $dim(V)$, the theorem being trivial in dimension zero. We V is itself isotropic, then Q is the "zero-form", and every element of V is orthogonal to every other element of V. Hence any basis is an orthogonal basis. Otherwise, we choose $e_1 \in V$, with $Q(e_1) \neq 0$. Let $V' = (e_1 k)^\perp$. Since "pairing with e_1" is a nonzero linear functional on V, its kernel is $dim(V) - 1$-dimensional, and we see that $V' \oplus (e_1 k) = V$. Moreover, this sum is orthogonal, so $V = V' \hat{\oplus} (e_1 k)$. By induction, we may find an orthogonal basis of V', say $e_2, \ldots, e_n$, yielding an orthogonal basis $e_1, \ldots, e_n$ of V.

Remarks on: Theorem 2

The central question in our study of quadratic forms is: when are two quadratic forms isomorphic? Isomorphism can be expressed via a linear isomorphism from a quadratic module (V, Q) to another (V', Q'). But, after choosing orthogonal bases of V and V', this question reduces to: when is the quadratic form $[a_1, \ldots, a_n]$ equivalent to the quadratic form $[b_1, \ldots, b_n]$? Here equivalence can be thought of as a linear isomorphism from k^n to k^n, or equivalently, as a change of basis matrix.

The main theorem, Theorem 2, implies that if $[a_1, \ldots, a_n] \sim [b_1, \ldots, b_n]$ (the quadratic forms are equivalent), and the a_i and b_i are nonzero (so (V, Q) is non-degenerate), and $n \geq 3$, then the equivalence may be broken up in stages. In each stage, we have an equivalence:

$$[\alpha_1, \ldots, \alpha_n] \sim [\beta_1, \ldots, \beta_n],$$

in which at least one of the α_i is equal to one of the β_j.

In terms of changing basis, this means that we change at most $n - 1$ basis elements at each stage. We give an example here:

EXAMPLE 1.3. *Consider the quadratic forms* $[2, 1, 6]$ *and* $[3, 5, 5]$ *over* $\mathbb{F}_7$. *These are equivalent, but perhaps not obviously so. The theorem implies that there exists a chain of equivalences such as:*

$$[2, 1, 6] \sim [3, 5, 6] \sim [3, 5, 5].$$

Note that at every stage, we leave at least one number fixed.

In proving Theorem 2, we fix a quadratic module (V, Q), and two orthogonal bases $\vec{e}, \vec{e}'$ of V. Here we use vector notation, to abbreviate $\vec{e} = (e_1, \ldots, e_n)$ and $\vec{e}' = (e'_1, \ldots, e'_n)$. Given that these are two orthogonal bases, we wish to find a chain

$\vec{e}^{(i)}$ of orthogonal bases, with $\vec{e}^{(0)} = \vec{e}$, and $\vec{e}^{(m)} = \vec{e}'$, such that $\vec{e}^{(i)}$ is *contiguous* to $\vec{e}^{(i+1)}$ for all $0 \leq i \leq m-1$.

When e_1 and e_1' have the property $Q(e_1)Q(e_1') - B_Q(e_1, e_1')^2 \neq 0$, one can find a chain of length two (i.e. $m = 2$) linking $\vec{e}$ and $\vec{e}'$. This is the "easy case". In this case, we let $P = ke_1 \oplus ke_2$. The aforementioned property implies that Q, restricted to P, is non-degenerate. Hence e_1, and e_1' may be completed to orthogonal bases of P, yielding:

$$P = e_1 k \hat{\oplus} \epsilon 2k = e_1' k \oplus \epsilon_2' k.$$

Let $f_3, \ldots, f_n$ be an orthogonal basis of $P^\perp$. We have $V = P \hat{\oplus} P^\perp$, since P is non-degenerate. Thus we have a chain of orthogonal bases:

$$\vec{e} \to (e_1, \epsilon 2, f_3, \ldots, f_n) \to (\epsilon_1, e_2, f_3, \ldots, f_n) \to \vec{e}'.$$

The hard case in the proof is when one can not find two basis elements e_i, e_j' which span a nondegenerate plane. In particular, $ke_1 \oplus ke_1'$ is degenerate, and $ke_1 \oplus ke_2'$ is degenerate. But in this case, the Lemma implies that there exists $x \in k$ such that $e_x' = e_1' + xe_2'$ generates a nondegenerate plane with e_1, and is nonisotropic.

Indeed, to have e_x' be nonisotropic, we must have:

$$Q(e_x') = Q(e_1') + x^2 Q(e_2') \neq 0 \text{ since } e_1' \perp e_2'.$$

Thus as long as $x^2 \neq -Q(e_1')/Q(e_2')$, this will be satisfied. For e_1 and e_x' to generate a nondegenerate plane, we must have:

$$\begin{aligned}
0 &\neq Q(e_1)Q(e_x') - B_Q(e_1, e_x')^2 \\
&= Q(e_1)Q(e_1') + x^2 Q(e_1)Q(e_2') - \left(B_Q(e_1, e_1') + xB_Q(e_1, e_2')\right)^2 \\
&= Q(e_1)Q(e_1') + x^2 Q(e_1)Q(e_2') - B_Q(e_1, e_1')^2 - 2xB_Q(e_1, e_1')B_Q(e_1, e_2') - x^2 B_Q(e_1, e_2')^2 \\
&= Q(e_1)Q(e_1') + x^2 Q(e_1)Q(e_2') - Q(e_1)Q(e_1') - 2xB_Q(e_1, e_1')B_Q(e_1, e_2') - x^2 Q(e_1)Q(e_2') \\
&= -2xB_Q(e_1, e_1')B_Q(e_1, e_2').
\end{aligned}$$

Nondegeneracy, together with the fact that $B_Q(e_1, e_1')^2 = Q(e_1)Q(e_1')$ and $B_Q(e_1, e_2')^2 = Q(e_1)Q(e_2')$ implies that for $x \neq 0$, the above condition is satisfied. The existence of e_x' such that e_x' is nondegenerate, and with e_1 it generates a nondegerate plane, follows from finding $x \in k$ with:

$$0 \neq x, \text{ and } x^2 \neq -Q(e_1')/Q(e_2')$$

. This eliminates at most three values of x. We don't consider $k = \mathbb{F}_2$, because we assume $char(k) \neq 2$. In $\mathbb{F}_3$, all squares are 0 or 1, and the condition $Q(e_1)Q(e_1') = B_Q(e_1, e_1')^2$ and $Q(e_1)Q(e_2') = B_Q(e_1, e_2')^2$ implies that $Q(e_1')/Q(e_2') = 1$. Thus, choosing $x^2 \neq -1$ does not place any condition on x. Such an x exists.

Now, in order to make the transition from $\vec{e}$ to $\vec{e}'$, we use the intermediate basis $\vec{e}_x'$ given by:

$$\vec{e}_x' = (e_x', e_2', e_3', \ldots, e_n').$$

This basis is contiguous to $\vec{e}'$. By the "easy case", we can find a chain linking $\vec{e}$ to $\vec{e}_x'$.

1.5. Witt's theorem. Notes by: Jordan Fassler

In this section, we consider metric morphisms between quadratic modules and when they can be extended. Specifically, given two nondegenerate quadratic modules (V_1, Q_1) and (V_2, Q_2), an injective morphism

$$s : U \to V_2$$

between $U \subset V_1$, a submodule, and V_2 which preserves the associated bilinear form, we try to extend s to all of V_1. An extension of s is a morphism from a larger space, containing U as a subspace, which is equal to s when restricted to U. Our main result is Witt's theorem which says that such an extension exists if V_1 and V_2 are isomorphic.

Remarks on: Lemma

This lemma takes care of the case when U is degenerate and says that given an s as above we can extend to an $s_1 : U_1 \to V_2$ where U is a subspace of U_1 of codimension one. Since U is degenerate, we can choose a nonzero $x \in \mathrm{rad}(U)$. Furthermore, since V is non-degenerate we can find a $y \in V$ such that $l_1(x) := [D_{Q_1}(y)](x) = 1$ (recall $[D_{Q_1}(y)](u) = B_{Q_1}(y, u)$). We can also assume that y is isotropic (if not replace y by $y - \frac{1}{2}Q_1(y)x$, which is clearly isotropic). We then set $U_1 = U \oplus ky$.

Let $U' = s(U)$. Since s is injective we can form a linear functional $l_2 :$ on U' by $l_2 = l_1(y) \circ s^{-1}$. As we've seen, V_2 being nondegenerate implies that there exists y_2 such that $l_2 = D_{Q_2}(y_2)$. Thus if we define the map $s_1 : U_1 \to V_2$ by letting s_1 equal s on U and $s_1(y) = y_2$ and extend linearly, then s_1 is a metric morphism.

Remarks on: Theorem 3

We construct our extension inductively on the dimension of U. If U is degenerate, we can apply the above lemma repeatedly until we arrive at a non-degenerate submodule, thus we can make the simplifying assumption that U is non-degenerate. Furthermore, since V_1 and V_2 are isomorphic, we can assume that $V = V_1 = V_2$.

dim $U = 1$: Since U is non-degenerate and one-dimensional, it is generated by a non-isotropic element x. Let $y = s(x)$, then we have $Q(x) = Q(y)$ and we can choose an $\varepsilon = \pm 1$ such that $x + \varepsilon y$ is not isotropic; if not we would have:

$$\begin{aligned} Q(x+y) &= 0 \\ Q(x-y) &= 0 \end{aligned}$$

expanding the left hand side:

$$\begin{aligned} B_Q(x,x) + B_Q(x,y) + B_Q(y,x) + B_Q(y,y) &= 0 \\ B_Q(x,x) - B_Q(x,y) - B_Q(y,x) + B_Q(y,y) &= 0 \end{aligned}$$

since $B_Q(x,x) = B_Q(y,y)$ and $B_Q(x,y) = B_Q(y,x)$ we have:

$$\begin{aligned} 2B_Q(x,x) + 2B_Q(x,y) &= 0 \\ 2B_Q(x,x) - 2B_Q(x,y) &= 0 \end{aligned}$$

which implies that $Q(x) = 0$. Given such an ε, we let H be the orthogonal complement of $z = x + \varepsilon y$; we have $V = kz \widehat{\oplus} H$. Define σ to be the automorphism of V which is the identity on H and which sends z to $-z$. Thus

$$\begin{aligned} \sigma(x + \varepsilon y) &= -x - \varepsilon y \\ \sigma(x - \varepsilon y) &= x - \varepsilon y \text{since } x - \varepsilon y \in H \end{aligned}$$

implying $\sigma(x) = -\varepsilon y$, thus $-\varepsilon\sigma$ extends s.

dim $U > 1$: We can decompose U as $U_1 \widehat{\oplus} U_2$ both not zero; restricting s to U_1 and extending by induction we get an automorphism, σ_1, of V which extends s when restricted to U_1. By substituting s with $\sigma_1^{-1} \circ s$ we can suppose s is the identity on U_1. Since s is the identity on U_1 and injective we have that U_2 is contained in the orthogonal complement of U_1, $U_1^{\perp}$, and thus it suffices to extend $s|_{U_2}$ to a $\sigma_2 : U_1^{\perp} \to U_1^{\perp}$ which we can do by the induction hypothesis. Thus our desired extension is σ which is σ_2 on $U_1^{\perp}$ and $\sigma_1^{-1} \circ s$ on U_1.

Remarks on: Corollary

Witt's Theorem and this corollary will give us a cancellation law for quadratic forms, which will be made more explicit in the next section. Essentially, if we have a nondegenerate quadratic module (V, Q) with subspaces U_1 and U_2 such that $U_1 \cong U_2$ then we extend the isomorphisms of the subspaces to an automorphism of V, since $V \cong U_1 \widehat{\oplus} U_1^{\perp} \cong U_2 \widehat{\oplus} U_2^{\perp}$ when we restrict the automorphism to the orthogonal complements we can "cancel" and get $U_1^{\perp} \cong U_2^{\perp}$

1.6. Translations. In this section Serre defines the translation of one quadratic form by another and then translates several of our previous results in terms of these translations. Let $X \in k^n$, we consider a quadratic form $f(X) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i>j} a_{ij} X_i X_j$ in n variables over k. Set $a_{ij} = a_{ji}$ for $i > j$, the matrix $A = (a_{ij})$ is symmetric and the pair (k^n, A) is a quadratic module, associated to f. Two quadratic forms f and f', in n variables, are equivalent, $f \sim f'$, if there is a an invertible matrix M such that $f(MX) = f'(X)$. This is equivalent to the definition given by Serre that the associated modules of f and f' are isomorphic.

Let $f(X_1, \ldots, X_n)$ and $g(X_1, \ldots, X_m)$ be two quadratic forms. The translation of a one quadratic form by another, denoted $f \dot{+} g$, is defined to be the quadratic form given by:

$$f \dot{+} g = f(X_1, \ldots, X_n) + g(X_{n+1}, \ldots, X_{n+m})$$

In terms of the associated modules, this operation corresponds to the orthogonal sum. We similarly define $f \dot{-} g$ for $f \dot{+} (-g)$.

We now translate several of our definitions and theorems in terms of translations. First notice that our hyperbolic plane has associated form $f(X) = X_1 X_2 \sim X_1^2 - X_2^2$ which is clearly a translation of two one variable forms. Furthermore we say that a form represents an element $a \in k$ if there exists a vectoer $x \in k^n$ such that $f(x) = a$.

Remarks on: Corollary 1

This corollary will be useful in our classification of quadratic forms.

$(i) \Rightarrow (ii)$: If g represents a then there exists a vector x such that $g(x) = a$ and thus we can find the orthogonal complement H of x and since our translation sum of forms corresponds to orthogonal sums of modules, if h is the quadratic form associated to H then since $G = H \widehat{\oplus} kx$ in quadratic form language this says $g \sim h \dot{+} aZ^2$.

$(ii) \Rightarrow (iii)$: Since $g \sim h \dot{+} aZ^2$ it clearly represents a (the vector $(0, \ldots, 0, 1)$ works on the right hand side). Thus $g \dot{-} aZ^2$ represents 0.

$(iii) \Rightarrow (i)$: If the form $f = g \dot{-} aZ^2$ represents zero, we have a nontrivial vector $x_0 = (x_1, ..., x_{n-1}, z)$ such that $f(x_0) = 0$. If $z = 0$ in this vector this implies that g represents zero and by proposition 3', g represents all of k. If $z \neq 0$ then $f(x_1/z, ..., x_{n-1}/z, 1) = g(x_1/z, ..., x_{n-1}/z) - a = 0$ and g represents a.

Remarks on: Corollary 2

We discuss just the implication $(a) \Rightarrow (b)$, the other implications being clear from

the previous corollary. If f represents zero there is a vector (x, y) such that $f(x, y) = g(x) - h(y) = 0$ thus $g(x) = h(y)$. There are two cases, if $g(x) = a \neq 0$ we are done. If $g(x) = 0$ then from proposition 3' g represents all of k in particular g represents any nonzero value taken by h.

We return to our translations of previous results. From theorem 1 we know that a quadratic module has an orthogonal basis, in terms of our quadratic form this gives us the familiar "sums of squares" form of our quadratic form f:

$$f \sim a_1 X_1^2 + \cdots + a_n X_n^2$$

We define the rank of f to be the number of indices i such that $a_i \neq 0$. And clearly the rank is n if and only if discriminate of f $a_1 \cdots a_n \neq 0$.

Remarks on: Theorem 4

As was discussed before in the remark to the corollary of Witt's theorem, this theorem gives us a cancellation law for quadratic forms. The theorem is an immediate consequence of the corollary and is equivalent to Witt's Theorem.

Remarks on: Corollary

From proposition 3' $f \sim g_1 \dot{+} h_1$ with g_1 and h_1 nondegenerate. Repeatedly applying the proposition we get the claimed decomposition. For uniqueness, suppose $f \sim g_1 \dot{+} \cdots \dot{+} g_m \dot{+} h \sim g_1' \dot{+} \cdots \dot{+} g_k' \dot{+} h'$ then using the cancellation law, we see that $h \sim h'$ and $m = k$. The h is called the anisotropic part of f.

1.7. Quadratic forms over $\mathbb{F}_q$. In this section we completely classify the quadratic forms over the finite fields of characteristic different than two. With the tools we have developed, the classification is fairly straightforward. We let p be prime $\neq 2$ and $q = p^f$. Let $\mathbb{F}_q$ be the field with q elements.

Remarks on: Proposition 4

Recall that Chevalley's theorem states that if number of variables exceeds the degree of a polynomial in the finite field K then the cardinality of the set of zeros is congruent to 0 mod p. Thus if we consider a quadratic form f in three variables, by Chevalley's Theorem it represents zero. Similarly, if we consider a form g in two variables, the form $g \dot{-} aZ^2$ with $a \in \mathbb{F}_q^x$, represents 0 since it is in three variables and by corollary 1 from the previous section, that implies g represents a.

Remarks on: Proposition 5

This proposition along with it's corollary, completes our classification of quadratic forms over $\mathbb{F}_q$. We proceed by induction. Let f be a quadratic form over $\mathbb{F}_q$ of rank n. If $n = 1$, since the group $\mathbb{F}_q^x / \mathbb{F}_q^{x2}$ has two elements, any quadratic form in one variable is either of the form X^2 or aX^2. If $n \geq 2$ by proposition 4 the form represents 1 and thus $f \sim X_1^2 \dot{+} g$ and g is of lesser rank and by induction we are done.

We finally see that quadratic forms over $\mathbb{F}_q$ are completely determined (up to equivalence) by their rank and their discriminant.

2. Quadratic forms over $\mathbb{Q}_p$

Notes by: Filix Maisch

Conventions for the section include that p is a prime number, k is the p-adic number field and quadratic modules and forms over k are assumed to be non-degenerate.

2.1. The two invariants. Here we let (V, Q) be a quadratic module of rank n and $d(Q) \in k^\times/(k^\times)^2$ its discriminant. If $e = (e_1, ..., e_n)$ is an orthogonal basis of V and we set $a_i = e_i \cdot e_i$, then

$$d(Q) = \prod_i^n a_i$$

Recall for $a, b \in k^\times$, the Hilbert symbol $(a, b) \in \{\pm 1\}$ is already defined. We define

$$\epsilon(e) := \prod_{i<j} (a_i, a_j) \in \{\pm 1\}$$

We shall show that this $\epsilon(e)$ is an invariant of (V, Q), that is, it does not depend on the choice of orthogonal basis e. This is the statement of theorem 5.

Remarks on: Theorem 5

The proof of this theorem is done via induction on the rank of V. If $n = 1$ then $\epsilon(e) = 1$ since the product is vacuous. So we need to do $n = 2$ as a base case. If $n = 2$ then we have that

$$\epsilon(e) = 1 \Leftrightarrow Z^2 - a_1X^2 - a_2Y^2 \text{ represents } 0 \Leftrightarrow a_1X^2 + a_2Y^2 \text{ represents } 1$$

$\Leftrightarrow \exists\ v \in V$ s.t. $Q(v) = 1$ and such a v is independent of any choice of basis

For $n \geq 3$, induction is used. By theorem 2 and transitivity it is enough to show that $\epsilon(e) = \epsilon(e')$ when e and e' are contiguous. Moreover the symmetry of the Hilbert symbol implies that we can assume that $e' = (e'_1, ..., e'_n)$ with $e_1 = e'_1$. So with $a'_i = e'_i \cdot e'_i$ it follows that $a_1 = a'_1$. We then write

$$\epsilon(e) = \prod_{k=2}^n (a_1, a_k) \prod_{2\leq i<j} (a_i, a_j) = (a_1, a_2 \cdots a_n) \prod_{2\leq i<j} (a_i, a_j) = (a_1, d(Q)a_1) \prod_{2\leq i<j} (a_i, a_j)$$

Similarly we have

$$\epsilon(e') = (a_1, d(Q)a_1) \prod_{2\leq i<j} (a'_i, a'_j)$$

and so the proof is done by induction. So given a quadratic form we immediately have two invariants, the discriminant and the epsilon sign invariant.

2.2. Representation of an element of k by a quadratic form. This section begins with a lemma. Part (a) of the lemma states that the number of elements in the $F_2 -$ v.s. $k^\times/(k^\times)^2$ is 2^r with $r = 2$ (resp. $r = 3$) if $p \neq 2$ (resp. $p = 2$). For parts (b) and (c) we need the following definition given $a \in k^\times/(k^\times)^2$ and $\epsilon = \pm 1$:

$$H_a^\epsilon := \{x \in k^\times/(k^\times)^2 : (x, a) = \epsilon\}$$

Part (b) states two cases. If $a = 1$, the H_a^1 has 2^r elements and $H_a^{-1} = \emptyset$. If $a \neq 1$, H_a^ϵ has 2^{r-1} elements. Consider $a, a' \in k^\times/(k^\times)^2$ and $\epsilon, \epsilon' = \pm 1$. Assume that $H_a^\epsilon \neq \emptyset \neq H_{a'}^{\epsilon'}$. Part (c) states that for $H_a^\epsilon \bigcap H_{a'}^{\epsilon'} = \emptyset$ it is necessary and sufficient that $a = a', \epsilon = -\epsilon'$.

Remarks on: Lemma

Part (a) has been already shown, see section 3.3 in chapter 2. The assertion in (b) in trivial for $a = 1$ (1 is a square). For $a \neq 1$, we have the following surjective homomorphism, $\varphi : k^\times/(k^\times)^2 \twoheadrightarrow \{\pm 1\}$ given by $b \mapsto (a, b)$. Hence $\ker \varphi = H_a^\epsilon =$

hyperplane, and so has 2^{r-1} elements. Part (c) follows from (b) and the non-degeneracy of the Hilbert symbol since $2^{r-1} + 2^{r-1} = 2^r$ and $(x, a) = (x, a') \; \forall \; x$ implies that $a = a', \epsilon = -\epsilon'$.

For theorem 6, f is a quadratic form of rank n and $d = d(f)$ and $\epsilon = \epsilon(f)$ are the invariants as previously defined.

Remarks on: Theorem 6

This theorem states that for f to represent 0, it is necessary and sufficient that

(1) $n = 2$ and $d = -1 \in k^\times/(k^\times)^2$
(2) $n = 3$ and $(-1, -d) = \epsilon$
(3) $n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$
(4) $n \geq 5$ (Thus all quadratic forms in at least five variables represent zero)

Letting $a \in k^\times/(k^\times)^2$ and $f_a = f - aZ^2$ ("dot" above minus sign) we have f_a represents $0 \Leftrightarrow$ f represents a. Nothing this and $d(f_a) = -ad$ and $\epsilon(f_a) = (-a, d)\epsilon$ we get a corollary to theorem 6 which gives the necessary and sufficient conditions for f to represent any a, not just zero. This conditions depend only on the rank, discriminant and invariant epsilon.

2.3. Classification. Theorem 7 states that two quadratic forms over k are equivalent if and only if they have the same rank, discriminant and invariant epsilon.

Remarks on: Theorem 7

The forward direction follows directly from definitions. The converse is shown by induction on the rank n. The case $n = 0$ is trivial. If we let f and g be two quadratic forms of rank n, discriminant d and invariant ϵ then by the Corollary from section 2.2 of this chapter, both f and g represent the exact same elements from $k^\times/(k^\times)^2$ and so we can find some a that is represented by both which implies that $f \sim aZ^2 + f'$ and $g \sim aZ^2 + g'$ with f', g' quadratic forms of rank $n - 1$, $d(f') = ad(f) = ad(g) = d(g')$ and $\epsilon(f') = \epsilon(f)(a, d(f')) = \epsilon(g)(a, d(g')) = \epsilon(g')$, so the proof is complete by induction.

Remarks on: Proposition 6

Given an $n \geq 1$, $d \in k^\times/(k^\times)^2$ and $\epsilon = \pm 1$ the proposition states that in order that there exists a quadratic form with the above invariants, it is necessary and sufficient that $n = 1, \epsilon = 1$ or $n = 2, d \neq 1$ or $n = 2, \epsilon = 1$ or $n \geq 3$. This proposition has a consequential corollary, that gives the number of classes of quadratic forms of rank n over k. For $p \neq 2$ (resp. $p = 2$) that number is 4 (resp. 8) if $n = 1$ and 7 (resp. 15) if $n = 2$ and 8 (resp. 16) if $n \geq 3$.

2.4. The real case. In this subsection, we let f be a quadratic form of rank n over the real numbers. We know f is equivalent to

$$X_1^2 + ... + X_r^2 - Y_1^2 - ... - Y_s^2$$

where r,s are two non-negative integers whose sum is n. The pair r,s depend only on f and is called the signature of the form f. The form f is positive or negative definite if $s = 0$ or $r = 0$ and otherwise f is indefinite (f represents 0 in that case and only in that case). The invariant $\epsilon(f)$ is defined as before and due to $(-1, -1) = -1$ we have the following:

$$\epsilon(f) = (-1)^{s(s-1)/2} \text{ and } d(f) = (-1)^s$$

So if n is less than or equal to three, these two invariants determine f up to equivalence!

3. Quadratic Forms over $\mathbb{Q}$

Notes by: M. Weissman In this section, all quadratic forms have coefficients in $\mathbb{Q}$, and are non-degenerate. We use the following notation (which Serre does not): let $[a_1, \ldots, a_n]$ denote the quadratic form:

$$Q(X_1, \ldots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2.$$

Every quadratic module has an orthogonal basis, and thus is equivalent to some $[a_1, \ldots, a_n]$. In this section, we always assume that $0 \neq a_i \in \mathbb{Q}$ for all $1 \leq i \leq n$.

3.1. Invariants of a form. Recall that V is the set of places of $\mathbb{Q}$, and $\infty \in V$ is the "real place", with $\mathbb{Q}_\infty = \mathbb{R}$.

Two invariants of a nondegenerate quadratic form, over any field k of characteristic not equal to 2, are:

- The discriminant $d = \prod_{i=1}^n a_i$. It is interpreted in $k^\times / k^{\times 2}$
- The ϵ-invariant (essentially the Hasse invariant) is defined by:

$$\epsilon = \prod_{1 \leq i < j \leq n} (a_i, a_j) \in \{\pm 1\},$$

  where (a_i, a_j) denotes the (quadratic) Hilbert symbol.

If f is a quadratic form over $\mathbb{Q}$, we write $\epsilon_v = \pm 1$ for the Hasse invariant of f, viewed as a quadratic form over $\mathbb{Q}_v$, and we write $d_v \in \mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$ for the discriminant of f viewed as a quadratic form over $\mathbb{Q}_v$. We write r, s for the number of ones and negative ones, as invariants of f over $\mathbb{R}$.

We are interested in three similar problems involving a quadratic forms:

- Given two quadratic forms f, g over $\mathbb{Q}$, when is f equivalent to g over $\mathbb{Q}$?
- Given a quadratic form f, and $a \in \mathbb{Q}^\times$, does f represent a?
- Given a quadratic form f, does f represent zero?

We will see that answering the final question yields an answer for the previous two (seemingly more difficult) questions.

The Hasse-Minkowski Theorem answers the final question – it is Theorem 8 in Serre:

THEOREM 3.1. *In order that a nondegenerate quadratic form f over $\mathbb{Q}$ represent 0, it is necessary and sufficient that for all $v \in V$, f_v represents 0.*

Necessity is obvious. Sufficiency requires proof. The proof of the Hasse-Minkowski theorem will use almost every technique discussed previously in Serre's text. Following Serre's treatment, we handle these questions case-by-case based on the rank of quadratic forms.

Note that if $f = [a_1, \ldots, a_n]$, then f represents zero iff $a_1 f = [a_1^2, a_1 a_2, \ldots, a_1 a_n] \sim [1, a_1 a_2, \ldots, a_1 a_n]$ represents zero. Thus, we may assume hereafter that $f = [1, a_2, \ldots, a_n]$, in proving the Hasse-Minkowski theorem.

3.1.1. *Quadratic forms of rank* 2. In rank 2, we have the following principle (valid over any field): **Whether a binary quadratic form represents zero is equivalent to whether a related number is a square or not.**

Suppose that $f = [1, a]$ over $\mathbb{Q}$. Suppose also that f represents zero over every $\mathbb{Q}_v$. Since f represents zero over $\mathbb{R}$, we have $a < 0$. Thus it suffices to consider $f = [1, -a]$ with $0 < a \in \mathbb{Q}$. This represents zero if and only if $a \in \mathbb{Q}^{\times 2}$.

Since f represents 0 over $\mathbb{Q}_p$, for every p, we have $a \in \mathbb{Q}_p^{\times 2}$. Thus, $val_p(a)$ is even for all p; recall that $val_p(a)$ is the exponent of p in the prime factorization of a^{-1}. Since a is positive, we see that $a = \prod_p p^{e_p}$, for even integers e_p. Hence $a \in \mathbb{Q}^{\times 2}$ as desired.

3.1.2. *Quadratic Forms of Rank* 3. This is the most difficult case in the theorem. In rank 3, we have the following principle (valid over any field): **Whether a ternary quadratic form represents zero is equivalent to whether a related Hilbert symbol is** 1 **or** -1**.**

It suffices to consider quadratic forms $f = [1, -a, -b]$ – here, we use the signs for convenience. Thus, we may rephrase the Hasse-Minkowski theorem in Rank 3 as the following statement:

PROPOSITION 3.2. *Suppose that* $a, b \in \mathbb{Q}^\times$. *Then, if* $(a, b)_v = 1$ *for all places* $v \in V$, *then* $(a, b) = 1$.

Note that if $(a, b)_v = -1$ for even one place $v \in V$, then $(a, b) = -1$. This follows from the definition of the Hilbert symbol, and the fact that $\mathbb{Q}$ is a subfield of $\mathbb{Q}_v$ for all v.

By altering a and b by rational squares (using the fact that $(ac^2, b) = (a, b)$ for all $a, b, c \in \mathbb{Q}^\times$), we may assume that a and b are squarefree (positive or negative) integers.

So, suppose that a, b are squarefree nonzero integers, and that $(a, b)_v = 1$ for all $v \in V$. We prove that $(a, b) = 1$ by induction on $m = |a| + |b|$, following Serre's treatment.

Since a and b are nonzero, the base step is $m = 2$. Here there are three possibilities $(1, 1)$, $(1, -1)$, $(-1, -1)$. We have $(-1, -1)_{\mathbb{R}} = -1$, so this case is irrelevant. It is easy to see that $(1, 1) = 1$, and $(1, -1) = 1$ (since the quadratic form $X^2 + Y^2 - Z^2$ represents zero over any field). This finishes the base step.

Now, we treat the case $m > 2$ by induction. Without loss of generality, assume that $|a| \leq |b|$. Let $b = \pm p_1 \cdot \cdots \cdot p_k$ be the prime factorization of b (noting that b is squarefree). Note that we may assume $b \neq \pm 1$ since this is covered by the base step – hence there exists a prime $p = p_1$ in the factorization of b.

Serre proves the following:

LEMMA 3.3. *a is a square, modulo p.*

PROOF. If $a \equiv 0 \mod p$, then a is automatically a square, modulo p. Otherwise, $a \in \mathbb{Z}_p^\times$. Since $(a, b)_p = 1$, there exist $x, y, z \in \mathbb{Q}_p$ such that $z^2 - ax^2 - by^2 = 0$. We may assume that $(x, y, z) \in \mathbb{Z}_p^3$ by scaling by powers of p. We may assume also that (x, y, z) is primitive, in the sense that $(x, y, z) \notin (p\mathbb{Z}_p)^3$ by scaling carefully. Since $p|b$, we have $z^2 - ax^2 \equiv 0 \mod p$. If $x \equiv 0 \mod p$, then $z \equiv 0 \mod p$, which implies that $by^2 \equiv 0 \mod p^2$, which implies that $y \equiv 0 \mod p$, since b is squarefree, contradicting primitivity. Thus $x \not\equiv 0 \mod p$, so $a \equiv (z/x)^2 \mod p$. □

This lemma implies the following:

COROLLARY 3.4. *a is a square, modulo b.*

PROOF. The ring $\mathbb{Z}/b\mathbb{Z}$ is isomorphic to the ring $\prod(\mathbb{Z}/p_i\mathbb{Z})$. Thus, an element of $\mathbb{Z}/b\mathbb{Z}$ is a square if and only if it is a square modulo p_i for all i. The previous lemma applies. □

Now, we are ready to perform the reduction. Since a is a square modulo b, there exist integers t, b' such that:

$$t^2 = a + bb'.$$

Since $t^2 = (-t)^2 \equiv (b-t)^2 \mod b$, we may assume that $0 \leq |t| \leq |b|/2$. The above formula shows that $bb' = t^2 - a = N(t+\sqrt{a})$ is a norm from the extension $k(\sqrt{a})/k$ when $k = \mathbb{Q}$ or $\mathbb{Q}_v$. Thus we have:

$$(a,b) = (a,b'), \text{ globally, and locally, } (a,b)_v = (a,b')_v.$$

If b' is not squarefree, then $b' = b''u^2$, where $u \in \mathbb{Z}$, and in particular $|b''| \leq |b'| < |b|$, and finally,

$$(a,b) = (a,b''), \text{ globally, and locally, } (a,b)_v = (a,b'')_v.$$

By induction, since $|b''| < |b|$ and b'' is squarefree, and since $(a,b'')_v = (a,b)_v = 1$ for all v, we have $(a,b'') = 1$. Hence $(a,b) = (a,b'') = 1$, and this finishes the inductive argument.

3.1.3. *Quadratic forms of rank* 4. In rank 4, there is again a general principle (over any field k of characteristic not equal to 2): **A quaternary quadratic form $[a,b,c,d]$ represents zero if and only if there exists some x represented by both $[a,b]$ and $[-c,-d]$.** This principle follows from Corollary 2 to Proposition 3', in IV.1.6 (essentially, from Witt cancellation, and the fact that hyperbolic planes represent everything).

Since we are given that $[a,b,-c,-d]$ represents zero over every $\mathbb{Q}_v$, there exists some $x_v \in \mathbb{Q}_v$ such that $[a,b]$ represents x_v, and $[c,d]$ represents x_v, over every v. Over $\mathbb{Q}_v$, $[a,b]$ represents x_v iff $[a,b,-x_v]$ represents zero, iff $[1,ab,-ax_v]$ represents zero, iff $(-ab,ax_v)_v = 1$, iff $(-ab,a)_v(-ab,x_v)_v = 1$, iff $(-a,a)_v(a,b)_v(-ab,x_v)_v = 1$, iff $(a,b)_v = (-ab,x_v)_v$.

Thus, we know that $(a,b)_v = (-ab,x_v)_v$ for all places v. Similarly, we know that $(c,d)_v = (-cd,x_v)_v$ for all v. Note moreover that $\prod_v (a,b)_v = \prod_v (c,d)_v = 1$. Thus, the constants $\epsilon_{1,v} = (-ab,x_v)_v$ and $\epsilon_{2,v} = (-cd,x_v)$ satisfy the conditions of Theorem 4 of Chapter III.2.2. Hence, there exists $x \in \mathbb{Q}^\times$ such that:

$$(a,b)_v = (-ab,x)_v, \text{ and } (c,d)_v = (-cd,x)_v \text{ for all } v \in V.$$

Thus $[a,b,x]$ represents zero in every $\mathbb{Q}_v$, and $[c,d,x]$ represents zero in every $\mathbb{Q}_v$. By the Hasse-Minkowski Theorem in rank 3, $[a,b,x]$ represents zero in $\mathbb{Q}$, and $[c,d,x]$ represents zero in $\mathbb{Q}$. Thus $[a,b]$ represents x in $\mathbb{Q}$, and $[c,d]$ represents x in $\mathbb{Q}$. Thus $[a,b,-c,-d]$ represents x in $\mathbb{Q}$.

3.2. Quadratic forms of rank $n \geq 5$. In rank $n \geq 5$, we apply induction on n. The base steps are provided by the previously proven cases. Suppose that we are given $f = [a_1, a_2, a_3, \ldots, a_n]$. Let $h = [a_1, a_2]$ and $g = [-a_3, \ldots, -a_n]$, so that $f = h \dot{-} g$, in Serre's notation.

We assume that f represents zero over every $\mathbb{Q}_v$. By a similar principle as the rank 4 case, there exists $x_v \in \mathbb{Q}_v$ such that h represents x_v, and g represents x_v

over $\mathbb{Q}_v$. In other words, there exist elements $z_1^v, \ldots, z_n^v \in \mathbb{Q}_v$, such that:

$$h(z_1^v, z_2^v) = x_v = g(z_3^v, \ldots, z_n^v).$$

Here Serre uses a topological argument. The topological facts that he uses are the following:

- If S is a finite set of places (a finite subset of V), then $\mathbb{Q}$ is dense in $\mathbb{Q}_S = \prod_{v \in S} \mathbb{Q}_v$.
- Multiplication and addition are continuous maps in $\mathbb{Q}_v$. In particular, h determines a continuous map from $\mathbb{Q}_v^2$ to $\mathbb{Q}_v$, and g determines a continuous map from $\mathbb{Q}_v^{n-2}$ to $\mathbb{Q}_v$.
- The subset $\mathbb{Q}_v^{\times 2}$ is an open subset of $\mathbb{Q}_v$. Indeed, if $z \in \mathbb{Q}_v^{\times 2}$, and $d \in \mathbb{Q}_v$, and $val(d) > 3 + val(z)$, then $z + d \in \mathbb{Q}_v^{\times 2}$ (since the valuations of z and $z + d$, and the last three digits of z and $z + d$ are the same).

Since $\mathbb{Q}_v^{\times 2}$ is open in $\mathbb{Q}_v$, and multiplication is continuous, we see that the translate $x_v \cdot \mathbb{Q}_v^{\times}$ is open in $\mathbb{Q}_v$. Since h, g are continuous, the pre-images $H_v = h^{-1}(x_v \cdot \mathbb{Q}_v^{\times})$ and $G_v = g^{-1}(x_v \cdot \mathbb{Q}_v^{\times})$ are open in $\mathbb{Q}_v^2$ and $\mathbb{Q}_v^{n-2}$, respectively.

Let S be the finite subset of V containing ∞, 2, and all primes p such that $val_p(a_i) \neq 0$ for some $i \geq 3$. Let H_S and G_S denote the product of the open subsets H_v and G_v, for $v \in S$, respectively. Then, since $\mathbb{Q}$ is dense in $\mathbb{Q}_S$, we have $\mathbb{Q}^m$ is dense in $\mathbb{Q}_S^m$ for all positive integers m. Therefore, we see that:

$$\mathbb{Q}^2 \cap H_S \neq \emptyset, \text{ and } \mathbb{Q}^{n-2} \cap G_S \neq \emptyset.$$

Tracing through the definitions, this implies that there exists $z_1, z_2 \in \mathbb{Q}$ such that $x = h(z_1, z_2) \in x_v \mathbb{Q}_v^{\times 2}$. Let $f_1 = [x, a_3, a_4, \ldots, a_n] = [x] \dot{-} g$. Then, we observe the following properties of f_1:

- If $v \in S$, then g represents x_v, and hence g represents x over $\mathbb{Q}_v$ (since x is equivalent to x_v modulo squares in $\mathbb{Q}_v$). Thus f_1 represents zero over $\mathbb{Q}_v$.
- If $v \notin S$, then $a_3, \ldots, a_n$ are v-adic units. Hence the discriminant is a v-adic unit and the Hasse invariant ϵ_v is trivial (note that the Hilbert symbol is trivial on units, away from the places $v = 2, \infty$). It follows that $(-1, -d)_v = \epsilon_v = 1$. Applying Theorem 6 of Section 2.2, g represents zero, and thus every element of $\mathbb{Q}_v$ (since g has rank at least 3). In particular, g represents x, so that f_1 represents zero over $\mathbb{Q}_v$.

Since f_1 represents zero over $\mathbb{Q}_v$ for $v \in S$ and for $v \notin S$, we see that f_1 represents zero over $\mathbb{Q}$ by induction (f_1 has rank one less that the rank of f). Since $f_1 = [x] \dot{-} g$, and f_1 represents zero over $\mathbb{Q}$, we see that g represents x over $\mathbb{Q}$. Since h represents x over $\mathbb{Q}$, and $f = h \dot{-} g$, this implies that f represents zero over $\mathbb{Q}$.

This concludes the proof of the Hasse-Minkowski Theorem.

Serre now presents a series of important corollaries:

COROLLARY 3.5. *Let $a \in \mathbb{Q}^{\times}$. In order that f represent a in $\mathbb{Q}$, it is necessary and sufficient that f represents a in every $\mathbb{Q}_v$.*

PROOF. Recall that f represents a (over a field k) iff $[a] \dot{-} f$ represents zero. □

COROLLARY 3.6. *A quadratic form of rank at least 5 represents zero iff it is indefinite (represents zero over $\mathbb{R}$).*

PROOF. Every quadratic form of rank at least 5 represents zero over $\mathbb{Q}_p$ for every p. Thus only the real place must be checked. □

COROLLARY 3.7. *Suppose that n is the rank of f, and that $n = 3$ (or $n = 4$ and $d(f) = 1$). If f represents zero at all $\mathbb{Q}_v$, except at most one place, then f represents zero.*

PROOF. When $n = 3$, we see that f represents zero over $\mathbb{Q}_v$ iff $(-1, -d)_v = \epsilon_v$. The product formula for the Hilbert symbol proves that if this equality is satisfied for all but at most one place, then it is satisfied for every place. Similarly, when $n = 4$, f represents zero over $\mathbb{Q}_v$ if and only if $d = 1$ (which is given) and $\epsilon_v = (-1, -1)_v$. Again, by the product formula for the Hilbert symbol, $\epsilon_v = (-1, -1)_v$ is true for all but at most one place iff it is true for all places. □

Serre remarks that for $n = 2$, if f represents zero over $\mathbb{Q}_v$ for all but a finite number of places, then f represents zero over $\mathbb{Q}$. It suffices to consider $f = [1, -a]$, where $a = -p_1, \ldots, p_k$ is a squarefree integer. For $f = [1, -a]$ to represent zero over k, it is necessary and sufficient for a to be a square in $k^\times$. Suppose that a is a square in $\mathbb{Q}_p^\times$ for all but finitely many places – since $a \in \mathbb{Z}$, this means that a is a square, modulo p, for all but finitely many primes.

Let P_i denote the set of primes p for which p_i is a square modulo p. Equivalently, P_i is the set of primes p in a finite set of congruence classes modulo p_i, by quadratic reciprocity. By the Chinese Remainder Theorem, we see that the set of primes p for which a is a non-square modulo p is a finite collection of congruence classes. The infinitude of primes in arithmetic progressions shows that if these congruence classes are nonempty, then they contain an infinite number of primes; thus a must be a square in at every finite place $\mathbb{Q}_p$.

3.3. Classification. Perhaps the most important formulation of the Hasse-Minkowski theorem is the following, Theorem 9 of Serre:

THEOREM 3.8. *Let f and f' be two quadratic forms over $\mathbb{Q}$. For f and f' to be equivalent over $\mathbb{Q}$, it is necessary and sufficient that they are equivalent over each $\mathbb{Q}_v$.*

PROOF. Necessity being trivial, we must show that if f and f' are equivalent over $\mathbb{Q}_v$ for all v, then they are equivalent over $\mathbb{Q}$. The proof is inductive, via Witt's cancellation theorem. The base step, in rank 0, is trivial. So suppose that f, f' have rank $n > 0$, and are equivalent over every $\mathbb{Q}_v$. Choose some $a \in \mathbb{Q}^\times$ represented by f. Then a is represented by f' (by a previous corollary to the Hasse-Minkowski Theorem). Thus we may write $f \sim [a] + g$ and $f' \sim [a] + g'$, for some quadratic forms g, g' over $\mathbb{Q}$. By Witt's cancellation theorem, this implies that $g \sim g'$ over every $\mathbb{Q}_v$, since $f \sim f'$ and $[a] \sim [a]$ over every $\mathbb{Q}_v$. By induction, $g \sim g'$ over $\mathbb{Q}$. Hence $f \sim f'$ over $\mathbb{Q}$ as well. □

In the corollary following this theorem, Serre uses the classification of quadratic forms over $\mathbb{Q}_v$ to classify quadratic forms over $\mathbb{Q}$. Namely, for f, f' quadratic forms over $\mathbb{Q}$ to be equivalent, it is necessary and sufficient for all of the local invariants of f, f' to be the same. Namely, one must have $rank(f) = rank(f')$, $d(f) = d(f')$ (the discriminants are equal in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$), $(r, s) = (r', s')$ (the real signatures are the same), and $\epsilon_v(f) = \epsilon_v(f')$ (the local Hasse invariants are the same).

On the surface, it seems that this result might be difficult to use – there are an infinite number of local invariants! However, if f is a quadratic form over $\mathbb{Q}$, then $f \sim [a_1, \ldots, a_n]$, where every a_i is a squarefree integer (by multiplying by squares). Let S denote the finite set of places, containing 2, ∞, and all primes dividing the a_i for some $1 \leq i \leq n$. Then the Hilbert symbol $(a_i, a_j)_v$ is trivial for $v \notin S$. Thus

the local invariants $\epsilon_v(f)$ are trivial outside of S. One only has to compute a finite collection of invariants to know the equivalence class of a quadratic form over $\mathbb{Q}$.

Since quadratic forms over $\mathbb{Q}$ are completely determined by the set of invariants $(n = rank, d, \epsilon_v, r, s)$, the final question is what invariants actually arise from quadratic forms. The list of conditions required is given by Serre:

(1) $\epsilon_v = 1$ for almost all $v \in V$, and $\prod_v \epsilon_v = 1$. Necessity of this condition follows from properties of the Hilbert symbol.
(2) $\epsilon_v = 1$ if $n = 1$, or if $n = 2$ and $-d \in \mathbb{Q}_v^{\times 2}$. For $n = 1$, necessity of this condition is obvious. For $n = 2$, $f = [a, b]$, $d = ab$, and if $-d \in \mathbb{Q}_v^{\times 2}$ then
$$(a, b)_v = (a, -ab)_v(a, -a)_v = (a, -d)_v(a, -a)_v = 1.$$
This proves the necessity in case $n = 2$ and $-d \in \mathbb{Q}_v^{\times 2}$.
(3) $r, s \geq 0$ and $r + s = n$. This is obviously necessary, since any quadratic form over $\mathbb{R}$ can be written in standard form: $f \sim [1, \ldots, 1]+[-1, \ldots, -1]$, with r ones and s negative ones.
(4) $d_\infty = sign(d) = (-1)^s$. Again this arises from the standard form over $\mathbb{R}$.
(5) $\epsilon_\infty = (-1)^{s(s-1)/2}$. Again, this follows from a computation over $\mathbb{R}$.

Proposition 7 shows that these five conditions are the only restrictions on the invariants of a quadratic form over $\mathbb{Q}$. In other words, for every collection $(0 \leq n \in \mathbb{Z}, d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}, \epsilon_v \in \pm 1, 0 \leq r, s \in \mathbb{Z})$, satisfying the above five conditions, there is a quadratic form (unique up to equivalence) over $\mathbb{Q}$ having that collection as its invariants. This completes the classification of quadratic forms over $\mathbb{Q}$.

Remarks on: On the Hasse Principle

Consider a set of polynomials $T \subset \mathbb{Q}[X_1, \ldots, X_n]$. For example, one might consider the set of degree 2 polynomials, or the set of polynomials of the form $X_1^2 = X_2^3 + aX_2 + b$ for arbitrary $a, b \in \mathbb{Q}$. We say that the set of polynomials T obeys the Hasse principle if the following holds: for every $f \in T$, for there to exist a solution to $f(X_1, \ldots, X_n) = 0$ over $\mathbb{Q}$, it is necessary and sufficient for there to exist a solution to $f(X_1, \ldots, X_n) = 0$ over every $\mathbb{Q}_v$.

We have now seen that the Hasse principle holds for homogeneous quadratic polynomials. By "homogenizing", it also holds for inhomogeneous quadratic polynomials. The Hasse principle is also known to hold for homogeneous *cubic* polynomials of degree at least 9 (under a non-singularity assumption, Hooley 1988) or 10 (under no assumption, Heath-Brown 1983). It is further known that, for every odd positive integer d, there exists a positive integer C_d, such that the Hasse principle holds for homogeneous polynomials, of degree d, in C_d variables (Birch, 1957). Perhaps one may take $C_d = d^2 + 1$? I believe that this problem is open.