In this lecture we lay the groundwork needed to prove the Hasse-Minkowski theorem for \( \mathbb{Q} \), which states that a quadratic form over \( \mathbb{Q} \) represents 0 if and only if it represents 0 over every completion of \( \mathbb{Q} \) (as proved by Minkowski). The statement still holds if \( \mathbb{Q} \) is replaced by any number field (as proved by Hasse), but we will restrict our attention to \( \mathbb{Q} \).

Unless otherwise indicated, we use \( p \) throughout to denote any prime of \( \mathbb{Q} \), including the archimedean prime \( p = \infty \). We begin by defining the Hilbert symbol for \( p \).

### 10.1 The Hilbert symbol

**Definition 10.1.** For \( a, b \in \mathbb{Q}_p^\times \) the Hilbert symbol \( (a, b)_p \) is defined by

\[
(a, b)_p = \begin{cases} 
1 & \text{if } ax^2 + by^2 = 1 \text{ has a solution in } \mathbb{Q}_p, \\
-1 & \text{otherwise.}
\end{cases}
\]

It is clear from the definition that the Hilbert symbol is symmetric, and that it only depends on the images of \( a \) and \( b \) in \( \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \) (their square classes). We note that

\[
\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \simeq \begin{cases} 
\mathbb{Z}/2\mathbb{Z} & \text{if } p = \infty, \\
(\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \text{ is odd,} \\
(\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p = 2.
\end{cases}
\]

The case \( p = \infty \) is clear, since \( \mathbb{R}^\times = \mathbb{Q}_\infty^\times \) has just two square classes (positive and negative numbers), and the cases with \( p < \infty \) were proved in Problem Set 4. Thus the Hilbert symbol can be viewed as a map \( (\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}) \times (\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}) \to \{\pm 1\} \) of finite sets.

We say that a solution \( (x_0, \ldots, x_n) \) to a homogeneous polynomial equation over \( \mathbb{Q}_p \) is **primitive** if all of its elements lie in \( \mathbb{Z}_p \) and at least one lies in \( \mathbb{Z}_p^\times \). The following lemma gives several equivalent definitions of the Hilbert symbol.

**Lemma 10.2.** For any \( a, b \in \mathbb{Q}_p^\times \), the following are equivalent:

(i) \( (a, b)_p = 1 \).

(ii) The quadratic form \( z^2 - ax^2 - by^2 \) represents 0.

(iii) The equation \( ax^2 + by^2 = z^2 \) has a primitive solution.

(iv) \( a \in \mathbb{Q}_p \) is the norm of an element in \( \mathbb{Q}_p(\sqrt{b}) \).

**Proof.** (i)\( \Rightarrow \) (ii) is immediate (let \( z = 1 \)). The reverse implication is clear if \( z^2 - ax^2 - by^2 = 0 \) represents 0 with \( z \) nonzero (divide by \( z^2 \)), and otherwise the non-degenerate quadratic form \( ax^2 + by^2 \) represents 0, hence it represents every element of \( \mathbb{Q}_p \) including 1, so (ii)\( \Rightarrow \) (i).

To show (ii)\( \Rightarrow \) (iii), multiply through by \( p^r \), for a suitable integer \( r \), and rearrange terms. The reverse implication (iii)\( \Rightarrow \) (ii) is immediate.

If \( b \) is square then \( \mathbb{Q}_p(\sqrt{b}) = \mathbb{Q}_p \) and \( N(a) = a \) so (iv) holds, and the form \( z^2 - by^2 \) represents 0, hence every element of \( \mathbb{Q}_p \) including \( ax_0^2 \) for any \( x_0 \), so (ii) holds. If \( b \) is not square then \( N(z + y\sqrt{b}) = z^2 - by^2 \). If \( a \) is a norm in \( \mathbb{Q}(\sqrt{b}) \) then \( z^2 - ax^2 - by^2 \) represents 0 (set \( x = 1 \)), and if \( z^2 - ax^2 - by^2 \) represents 0 then dividing by \( x^2 \) and adding \( a \) to both sides shows that \( a \) is a norm. So (ii)\( \Leftrightarrow \) (iv). \( \square \)
Corollary 10.3. For all \( a, b, c \in \mathbb{Q}_p^\times \), the following hold:

(i) \( (1, c)_p = 1 \).
(ii) \( (-c, c)_p = 1 \).
(iii) \( (a, c)_p = 1 \implies (a, c)_p(b, c)_p = (ab, c)_p \).
(iv) \( (c, c)_p = (-1, c)_p \).

Proof. Let \( N \) denote the norm map from \( \mathbb{Q}_p(\sqrt{c}) \) to \( \mathbb{Q}_p \). For (i) we have \( N(1) = 1 \). For (ii), \(-c = N(-c)\) for \( c \in \mathbb{Q}_p^\times \), so is \( -1 \). For (iii), If \( a \) and \( b \) are both norms in \( \mathbb{Q}(\sqrt{c}) \), then so is \( ab \), by the multiplicativity of the norm map; conversely, if \( a \) and \( ab \) are both norms, so is \( 1/a \), as is \((1/a)ab = b \). Thus if \( (a, c)_p = 1 \), then \( (b, c)_p = 1 \) if and only if \( (ab, c)_p = 1 \), which implies \( (a, c)_p(b, c)_p = (ab, c)_p \). For (iv), \( (-c, c)_p = 1 \) by (ii), so by (iii) we have \( (c, c)_p = (-c, c)_p(c, c)_p = (-c^2, c)_p = (-1, c)_p \). \( \Box \)

Theorem 10.4. \((a, b)_\infty = -1 \) if and only if \( a, b < 0 \)

Proof. We can assume \( a, b \in \{\pm 1\} \), since \( \{\pm 1\} \) is a complete set of representatives for \( \mathbb{R}^\times / \mathbb{R}^\times \). If either \( a \) or \( b \) is 1 then \((a, b)_\infty = 1 \), by Corollary 10.3.(i), and \((-1, -1)_\infty = -1 \), since \(-1 \) is not a norm in \( \mathbb{C} = \mathbb{Q}_\infty(\sqrt{-1}) \). \( \Box \)

Lemma 10.5. If \( p \) is odd, then \((u, v)_p = 1 \) for all \( u, v \in \mathbb{Z}_p^\times \).

Proof. Recall from Lecture 3 (or the Chevalley-Warning theorem on problem set 2) that every plane projective conic over \( \mathbb{F}_p \) has a rational point, so we can find a non-trivial solution to \( z^2 - ux^2 - vy^2 = 0 \) modulo \( p \). If we then fix two of \( x, y, z \) so that the third is nonzero, Hensel's lemma gives a solution over \( \mathbb{Z}_p \). \( \Box \)

Remark 10.6. Lemma 10.5 does not hold for \( p = 2 \); for example, \((3, 3)_2 = -1 \).

Theorem 10.7. Let \( p \) be an odd prime, and write \( a, b \in \mathbb{Q}_p^\times \) as \( a = p^\alpha u \) and \( b = p^\beta v \), with \( \alpha, \beta \in \mathbb{Z} \) and \( u, v \in \mathbb{Z}_p^\times \). Then

\[
(a, b)_p = (-1)^{\alpha \beta \frac{p-1}{2}} \left( \frac{u}{p} \right)^\beta \left( \frac{v}{p} \right)^\alpha,
\]

where \( \left( \frac{z}{p} \right) \) denotes the Legendre symbol \( \left( \frac{z \mod p}{p} \right) \).

Proof. Since \( (a, b)_p \) depends only on the square classes of \( a \) and \( b \), we assume \( \alpha, \beta \in \{0, 1\} \).

Case \( \alpha = 0, \beta = 0 \): We have \((u, v)_p = 1 \), by Lemma 10.5, which agrees with the formula.

Case \( \alpha = 1, \beta = 0 \): We need to show that \((pu, v)_p = \left( \frac{u}{p} \right) \).

Case \( \alpha = 1, \beta = 1 \): We must show \((pu, pv)_p = (-1)^{\frac{p-1}{2}} \left( \frac{u}{p} \right) \left( \frac{v}{p} \right) \).

Applying Corollary 10.3 we have

\[
(pu, pv)_p = (pu, pv)_p(-pv, pv)_p = (-p^2uv, pv)_p = (-uv, pv)_p = (pv, -uv)_p.
\]

Applying the formula in the case \( \alpha = 1, \beta = 0 \) already proved, we have

\[
(pv, -uv)_p = \left( \frac{-uv}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{u}{p} \right) \left( \frac{v}{p} \right) = (-1)^{\frac{p-1}{2}} \left( \frac{u}{p} \right) \left( \frac{v}{p} \right) \cdot \Box \]
Lemma 10.8. Let \( u, v \in \mathbb{Z}_2^\times \). The equations \( z^2 - ux^2 - vy^2 = 0 \) and \( z^2 - 2ux^2 - vy^2 = 0 \) have primitive solutions over \( \mathbb{Z}_2 \) if and only if they have primitive solutions modulo 8.

Proof. Without loss of generality we can assume that \( u \) and \( v \) are odd integers, since every square class in \( \mathbb{Z}_2^\times / \mathbb{Z}_2^{	imes 2} \) is represented by an odd integer (in fact one can assume \( u, v \in \{ \pm 1, \pm 5 \} \)). The necessity of having a primitive solution modulo 8 is clear. To prove sufficiency we apply the strong form of Hensel’s lemma proved in Problem Set 4. In both cases, if we have a non-trivial solution \( (x_0, y_0, z_0) \) modulo 8 we can fix two of \( x_0, y_0, z_0 \) to obtain a quadratic polynomial \( f(w) \) over \( \mathbb{Z}_2 \) and \( w_0 \in \mathbb{Z}_2^\times \) that satisfies \( v_2(f(w_0)) = 3 > 2 = 2v_2(f'(w_0)) \). In the case of the second equation, note that a primitive solution \( (x_0, y_0, z_0) \) modulo 8 must have \( y_0 \) or \( z_0 \) odd; if not, then \( z_0^2 \) and \( v_0^2 \), and therefore \( 2ux_0^2 \), are divisible by 4, but this means \( x_0 \) is also divisible by 2, which contradicts the primitivity of \( (x_0, y_0, z_0) \). Lifting \( w_0 \) to a root of \( f(w) \) over \( \mathbb{Z}_2 \) yields a solution to the original equation. \( \square \)

Theorem 10.9. Write \( a, b \in \mathbb{Q}_2^\times \) as \( a = 2^αu \) and \( b = 2^βv \) with \( α, β \in \mathbb{Z} \) and \( u, v \in \mathbb{Z}_2^\times \). Then
\[
(a, b)_2 = (-1)^{(uε(v)+αω(v)+βω(u))},
\]
where \( ε(u) \) and \( ω(u) \) denote the images in \( \mathbb{Z}/2\mathbb{Z} \) of \( (u - 1)/2 \) and \( (u^2 - 1)/8 \), respectively.

Proof. Since \( (a, b)_2 \) only depends on the square classes of \( a \) and \( b \), it suffices to verify the formula for \( (a, b)_2 \) with \( S = \{ ±1, ±3, ±2, ±6 \} \). By Lemma 10.8, to compute \( (a, b)_2 \) with \( a, b \) in \( \mathbb{Z}_2^\times \), it suffices to check for primitive solutions to \( z^2 - ax^2 - by^2 = 0 \) modulo 8, which reduces the problem to a finite verification which performed by 18.782 Lecture 10 Sage Worksheet.

We now note the following corollary to Theorems 10.4, 10.7, and 10.9.

Corollary 10.10. The Hilbert symbol \( (a, b)_p \) is a nondegenerate bilinear map. This means that for all \( a, b, c \in \mathbb{Q}_p^\times \) we have
\[
(a, c)_p(b, c)_p = (ab, c) \quad \text{and} \quad (a, b)_p(a, c)_p = (a, bc)_p,
\]
and that for every non-square \( c \) we have \( (b, c)_p = -1 \) for some \( b \).

Proof. Both statements are clear for \( p = \infty \) (there are only 2 square classes and 4 combinations to check). For \( p \) odd, let \( c = p^γw \) and fix \( ε = (-1)^{\frac{p-1}{2}} \). Then for \( a = p^αu \) and \( b = p^βv \), we have
\[
(a, c)_p(b, c)_p = ε^{αγ}(u \overline{w})^α(w \overline{p})^γ \overline{v}^β \overline{w}^β = ε^{α+β} \overline{u}^γ(w \overline{p})^{α+β} = (ab, c)_p.
\]

To verify non-degeneracy, we note that if \( c \) is not square then either \( γ = 1 \) or \( (w \overline{p}) = -1 \). If \( γ = 1 \) we can choose \( b = v \) with \( (\overline{w} \overline{p}) = -1 \), so that \( (b, c)_p = (w \overline{p}) = -1 \). If \( γ = 0 \), then \( ε = 1 \) and \( (w \overline{p}) = -1 \), so with \( b = p \) we have \( (b, c)_p = (w \overline{p}) = -1 \).
For $p = 2$, we have
\[(a,c)_2(b,c)_2 = (-1)^{\epsilon(u)\epsilon(w) + \alpha\omega(w) + \gamma\omega(u)}(-1)^{\epsilon(v)\epsilon(w) + \beta\omega(w) + \gamma\omega(v)}
= (-1)^{\epsilon(u) + \epsilon(v) + \alpha\omega(w) + \beta\omega(w) + \gamma\omega(u) + \gamma\omega(v)}
= (-1)^{\epsilon(u)v\omega(w) + (\alpha + \beta)\omega(w) + \gamma\omega(u)v}
= (ab,c)_2,
\]
where we have used the fact that $\epsilon$ and $\omega$ are group homomorphisms from $\mathbb{Z}_2^\times$ to $\mathbb{Z}/2\mathbb{Z}$. To see this, note that the image of $\epsilon^{-1}(0)$ in $(\mathbb{Z}/4\mathbb{Z})^\times$ is $\{1\}$, a subgroup of index 2, and the image of $\omega^{-1}(0)$ in $(\mathbb{Z}/8\mathbb{Z})^\times$ is $\{\pm 1\}$, which is again a subgroup of index 2.

We now verify non-degeneracy for $p = 2$. If $c$ is not square then either $\gamma = 1$, or one of $\epsilon(w)$ and $\omega(w)$ is nonzero. If $\gamma = 1$, then $(5,c)_2 = -1$. If $\gamma = 0$ and $\omega(w) = 1$, then $(2,c)_2 = -1$. If $\gamma = 0$ and $\omega(w) = 0$, then we must have $\epsilon(w) = 1$, so $(-1,c)_2 = -1$. $\blacksquare$

We now prove Hilbert’s reciprocity law, which may be regarded as a generalization of quadratic reciprocity.

**Theorem 10.11.** Let $a, b \in \mathbb{Q}^\times$. Then $(a,b)_p = 1$ for all but finitely many primes $p$ and
\[
\prod_p (a,b)_p = 1.
\]

**Proof.** We can assume without loss of generality that $a, b \in \mathbb{Z}$, since multiplying each of $a$ and $b$ by the square of its denominator will not change $(a,b)_p$ for any $p$. The theorem holds if either $a$ or $b$ is 1, and by the bilinearity of the Hilbert symbol, we can assume that
\[a,b \in \{-1\} \cup \{q \in \mathbb{Z}_{>0} : q \text{ is prime}\}.
\]
The first statement of the theorem is clear, since $a,b \in \mathbb{Z}_p^\times$ for $p < \infty$ not equal to $a$ or $b$, and $(u,v)_p = 1$ for all $u,v \in \mathbb{Z}_p^\times$ when $p$ is odd, by Lemma 10.5. To verify the product formula, we consider 5 cases.

Case 1: $a = b = -1$. Then $(-1,-1)_\infty = (-1,-1)_2 = -1$ and $(-1,-1)_p = 1$ for $p$ odd.

Case 2: $a = -1$ and $b$ is prime. If $b = 2$ then $(1,1)$ is a solution to $-x^2 + 2y^2 = 1$ over $\mathbb{Q}_p$ for all $p$, thus $\prod_p (-1,2)_p = 1$. If $b$ is odd, then $(-1,b)_p = 1$ for $p \notin \{2,b\}$, while $(-1,b)_2 = (-1)^{\epsilon(b)}$ and $(-1,b)_b = (\frac{-1}{b})$, both of which are equal to $(-1)^{(b-1)/2}$.

Case 3: $a$ and $b$ are the same prime. Then by Corollary 10.3, $(b,b)_p = (-1,b)_p$ for all primes $p$, and we are in case 2.

Case 4: $a = 2$ and $b$ is an odd prime. Then $(2,b)_p = 1$ for all $p \notin \{2,b\}$, while $(2,b)_2 = (-1)^{\omega(b)}$ and $(2,b)_b = (\frac{2}{b})$, both of which are equal to $(-1)^{(b^2-1)/8}$.

Case 5: $a$ and $b$ are distinct odd primes. Then $(a,b)_p = 1$ for all $p \notin \{2,a,b\}$, while
\[
(a,b)_p = \begin{cases} 
(-1)^{\epsilon(a)\epsilon(b)} & \text{if } p = 2, \\
\left(\frac{a}{b}\right) & \text{if } p = b, \\
\left(\frac{b}{a}\right) & \text{if } p = a.
\end{cases}
\]

Since $\epsilon(x) = (x - 1)/2 \mod 2$, we have
\[
\prod_p (a,b)_p = (-1)^{\frac{a+1}{2} \frac{b+1}{2}} \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = 1,
\]
by quadratic reciprocity. $\blacksquare$