Serre 2.2: Existence of Rationals with given Hilbert Symbols

Alek Westover

February 27, 2024

1 Review of Important Theorems

In this section we briefly review some relevant theorems and notation introduced in recent lectures. For integers a, b we write $a \perp b$ to denote that a, b are coprime. For set A and element x we write xA to denote $\{a \cdot x \mid a \in A\}$. We use $[n]$ to denote $\{1, 2, \ldots, n\}$. We define $\mathbb{Q}_\infty = \mathbb{R}$, and let V denote the set of primes union $\{\infty\}$. For $v \in V$, $a, b \in \mathbb{Q}_v^*$ the ***hilbert symbol*** $(a, b)_v$ is $+1$ if the equation $z^2 - ay^2 - bw^2 = 0$ has a nontrivial solution and is -1 otherwise. Some useful trivial properties of the Hilbert Symbol are $(a, b)_v = (b, a)_v$ and $(a, c^2)_v = 1$. We will also use the following theorems about the Hilbert Symbol.

Theorem 1.1 (Computing the Hilbert Symbol)**.** If p is an odd prime, u, v are units in $\mathbb{Q}_p$, and α, β are integers, then

$$(up^\alpha, vp^\beta)_p = (-1)^{\alpha\beta(p-1)/2} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

Theorem 1.2 (Properties of the Hilbert Symbol)**.** Fix $v \in V$. The Hilbert Symbol is bilinear, i.e., satisfies $(aa', b)_v = (a, b)_v (a', b)_v$. The Hilbert Symbol is non-degenerate, i.e., for any b which is not a perfect square in $\mathbb{Q}_v^*$, there is some a such that $(a, b)_v = -1$.

Theorem 1.3 (Hilbert Product Formula)**.** For any $a, b \in \mathbb{Q}^*$, for each $v \in V$, $\{(a, b) \mid (a, b)_v = -1\}$ is finite, and $\prod_{v \in V} (a, b)_v = 1$.

2 Lemmas for the Main Theorem

Lemma 2.1 (Classification of Squares)**.** Fix prime $p \neq 2$. Let $x = p^n u \in \mathbb{Q}_p$ where u is a unit in $\mathbb{Q}_p$, and $n \in \mathbb{Z}$. Then x is a square in $\mathbb{Q}_p$ if and only if both n is even and $u \mod p$ is a square in $\mathbb{F}_p$.

Let $y = 2^n u \in \mathbb{Q}_2$ where $n \in \mathbb{Z}$ and u is a unit in $\mathbb{Q}_2$. Then x is a square if and only if both n is even and $u \equiv 1 \mod 8$.

Proof. This was proved in chapter 2. □

Lemma 2.2 (Chinese Remainder Theorem)**.** Fix $n \in \mathbb{N}$. Let A, M be sets of n integers each, with the integers in M relatively prime. Then, there exists $x \in \mathbb{Z}$ such that for all $a \in A, m \in M$ we have

$$x \equiv a \mod m.$$

Proof. Given a_1, a_2, m_1, m_2 with $m_1 \perp m_2$ we have that m_1 is invertable modulo m_2. Hence, the equation

$$m_2 z + a_1 \equiv a_2 \mod m_1$$

has an integer solution. The Chinese Remainder Theorem follows by induction. □

Lemma 2.3 (Dirichlet's Theorem)**.** Given coprime integers a, m there are infinitely many primes in $p + a\mathbb{Z}$.

Proof. We will give an analytic number theory proof in a later Chapter. □

Lemma 2.4 (Approximation Theorem)**.** Let S be a finite subset of V. The image of $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$ is dense in this product.

Proof. It can only make our task harder to enlarge S. Thus, to eliminate casework we assume that S contains ∞. Let $n = |S| - 1$. Let $p_1, \ldots, p_n$ denote the non-infinite elements of S. Our goal is to show, for any $(x_\infty, x_1, \ldots, x_n) \in \prod_{v \in S} \mathbb{Q}_v$ and any $\varepsilon > 0$ that there is some $x \in \mathbb{Q}$ such that $|x - x_i|_{p_i} < \varepsilon$ and $|x - x_\infty|_\infty < \varepsilon$.

For each $i \in [n]$, let $N_i = 1$ if $\nu_{p_i}(x_i) \geq 0$, and $p^{-\nu_{p_i}(x_i)}$ otherwise. Let $N = \prod_i N_i$. Clearly if we can find $x \in \mathbb{Q}$ whose image is arbitrarily close to $(Nx_\infty, Nx_1, \ldots, Nx_n)$ then we can also find $x' \in \mathbb{Q}$ whose image is arbitrarily close to $(x_\infty, x_1, \ldots, x_n)$. Thus, we may restrict to considering

$$(Nx_\infty, Nx_1, \ldots, Nx_n) \in \mathbb{R} \times \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}.$$

Let $(x'_\infty, x'_1, \ldots, x'_n) = (Nx_\infty, Nx_1, \ldots, Nx_n)$.

Fix $\varepsilon > 0$. Take M such that $2^{-M} < \varepsilon$. By the Chinese Remainder Theorem we can find $x_0 \in \mathbb{Z}$ such that for all $i \in [n]$

$$x_0 \equiv x'_i \mod p_i^M.$$

Let $q \in \mathbb{Z}$ be relatively prime to $\prod_{i \in [n]} p_i$. For any $a \in \mathbb{Z}, M' \in \mathbb{N}$ and for each $i \in [n]$ we have

$$\left| \frac{a}{q^{M'}} \prod_{i \in [n]} p_i^M + x_0 - x'_i \right|_{p_i} \leq p^{-M} \leq \varepsilon.$$

By choosing a, M' appropriately (i.e., because $\mathbb{Q}$ is dense in $\mathbb{R}$) we can make

$$\left| \frac{a}{q^{M'}} \prod_{i \in [n]} p_i^M + x_0 - x'_\infty \right| < \varepsilon.$$

Thus, for appropriate a, M' the rational $\frac{a}{q^{M'}} \prod_{i \in [n]} p_i^M + x_0$ fulfills our needs. $\square$

3 Main Theorem

The remainder of this lecture will be devoted to proving the following theorem.

Theorem 3.1 (Theorem 4 in Serre)**.** Let $A \subset \mathbb{Q}^*$ be a finite set of rationals. Let $\sigma : A \times V \to \{-1, 1\}$. We say that $x \in \mathbb{Q}^*$ ***fulfills*** A, σ if $\sigma(a, v) = (a, x)_v$ for all $a \in A, v \in V$.

There exists x fulfilling A, σ if and only if the following conditions are met:

1. $\{(a, v) \mid \sigma(a, v) = -1\}$ is finite.
2. For all $a \in A$ we have $\prod_{v \in V} \sigma(a, v) = 1$.
3. For all $v \in V$ there exists $x_v \in \mathbb{Q}_v^*$ such that for all $a \in A$ we have $(a, x_v)_v = \sigma(a, v)$.

Proof. The fact that conditions 1,2,3 are necessary for existence of x fulfilling A, σ is easy to see. Condition 1 and Condition 2 are necessary by Theorem 1.3. Condition 3 is necessary, because if x exists fulfilling A, σ then we can simply take $x_v = x$ and thereby fulfill Condition 3. Now we show that these three conditions are actually sufficient to guarantee the existence of such an x.

Let $\mathcal{A}$ denote the set of prime factors of $2 \prod_{a \in A} a$, union $\{\infty\}$. Let M denote the set of "moduli" v such that $\sigma(a, v) = -1$ for some $a \in A$. Note that by Condition 1 $\mathcal{A}, M$ are finite.

Case I: $\mathcal{A} \cap M = \varnothing$. Our strategy here is to explicitly construct x. Define

$$\alpha = 4 \prod_{a \in \mathcal{A} \setminus \{\infty\}} a \quad \text{and} \quad m = \prod_{p \in M \setminus \{\infty\}} p.$$

Because $\mathcal{A} \cap M = \varnothing$, we have $\alpha \perp m$. By Dirichlet's theorem this implies the existence of a positive integer k such that $m + \alpha k$ is a prime q not contained in $\mathcal{A} \cup M$. Set $x = m(m + \alpha k)$. We claim that x fulfills

A, σ. The reasons for this choice of x will soon be clear. As a preliminary sanity check, the discriminant of $z^2 - ay^2 - mqw^2$ is amq. So, if we have prime p with $p \nmid amq$ then $(a, mq)_p = 1$. Thus, it is crucial that each $v \in M$ has $v \mid x$ or else $(a, x)_v = -1$ would be impossible regardless of a. This analysis also shows that for all primes $p \notin \mathcal{A} \cup M \cup \{q\}$ we instantly have $(a, x)_p = 1 = \sigma(a, p)$ as desired. The additional properties of our chosen x will serve to make $(a, x)_v$ have the correct value in the remaininng cases. Now we verify for each a, v that $\sigma(a, v) = (x, a)_v$. We break the verification into several cases based on the value of v.

- **Case I.1:** $v \in \mathcal{A}$. The assumption defining Case I is that $\mathcal{A} \cap M = \varnothing$. Hence, $v \notin M$, and our goal in Case I.1 is to show that $(a, x)_v = 1$ for all $a \in A$.
- **Case I.1.1:** $v = \infty$. We have $x > 0$, so $(a, x)_\infty = 1$ for all $a \in A$.
- **Case I.1.2:** $v = 2$. We have
$$x \mod 8 \equiv m^2 + m\alpha k \equiv m^2 \equiv 1$$
due to $m \perp 2$ and $8 \mid \alpha$. Thus, by our classification of squares in $\mathbb{Q}_2$ (see Lemma 2.1) x is a square in $\mathbb{Q}_2^*$. Thus, $(a, x)_2 = 1$ for all $a \in A$.
- **Case I.1.3:** $v \in \mathcal{A} \setminus \{2, \infty\}$. We have
$$x \mod v \equiv m^2 + m\alpha k \equiv m^2 \not\equiv 0$$
by $m \perp v$ and $v \mid \alpha$ so by our classification of squares in $\mathbb{Q}_v$ we have that x is a square in $\mathbb{Q}_v^*$, and hence $(a, x)_v = 1$ for all $a \in A$.
- **Case I.2: v is a prime $p \notin \mathcal{A}$.** In particular this implies that $\nu_p(a) = 0$. Thus, by the formula for the Hilbert Symbol (see Theorem 1.1) we have that for all b,
$$(a, b)_p = \left(\frac{a}{p}\right)^{\nu_p(b)}. \tag{1}$$
- **Case I.2.1:** $p \notin M \cup \{q\}$. Here we have $\nu_p(mq) = 0$. Then by (1) we have $(a, x)_p = 1$ for all $a \in A$. And, because $p \notin M$ we have $\sigma(a, p) = 1$ for all $a \in A$. Thus, we have $\sigma(a, p) = (a, x)_p$ for all $a \in A$.[1]
- **Case I.2.2:** $p \in M$. Here we have $\nu_p(mq) = 1$. So by (1) we have
$$(a, mq)_p = \left(\frac{a}{mq}\right).$$
Thus, our goal here is to show that $\left(\frac{a}{mq}\right) = \sigma(a, p)$. Recall Condition 3: there exists $x_p \in \mathbb{Q}_p^*$ such that $(a, x_p)_p = \sigma(a, p)$ for all $a \in A$. By (1) we have
$$(a, x_p)_p = \left(\frac{a}{p}\right)^{\nu_p(x_p)}.$$
Because $p \in M$ there is some a with $\sigma(a, p) = -1$. Thus, $(a, x_p)_p$ cannot always be $+1$, which necessitates $\nu_p(x_p) = 1$ and
$$(a, x_p)_p = \left(\frac{a}{p}\right).$$
In summary we have shown:
$$\sigma(a, p) = (a, x_p)_p = \left(\frac{a}{p}\right) = (a, x)_p,$$
as desired.
- **Case I.2.3:** $p = q$. Fix $a \in A$. We show $(a, x)_p = \sigma(a, p)$. By the Hilbert Product formula Theorem 1.3 we have
$$(a, x)_p = \prod_{v \neq p} (a, x)_v.$$
We have already shown
$$\prod_{v \neq p} (a, x)_v = \prod_{v \neq p} \sigma(a, v).$$

[1] In fact, we actually already handled this case earlier via analysis of the discriminant.

By Condition 2 we have

$$\prod_{v \neq p} \sigma(a, v) = \sigma(a, p).$$

Combining our three observations yields $(a, x)_p = \sigma(a, p)$.

Case II: $\mathcal{A} \cap M \neq \varnothing$. Our strategy here is to reduce to Case I some topological facts.

Fact 3.2. The squares of $\mathbb{Q}_v^*$ form an open subgroup of $\mathbb{Q}_v^*$. This follows from our classification of the squares in $\mathbb{Q}_v$. For instance, if v is an odd prime p then a neighborhood of the square $x^2 \in \mathbb{Q}_p^*$ contained in the squares of $\mathbb{Q}_p^*$ is $(1 + p\mathbb{Z}_p) \cdot x^2$.

Recall also Lemma 2.4: the image of $\mathbb{Q}$ is dense in $\prod_{v \in \mathcal{A}} \mathbb{Q}_v$. Finally, recall that for each $v \in V$ there are $x_v \in \mathbb{Q}_v^*$ such that $(a, x_v)_v = \sigma(a, v)$ for all $a \in A$. Combining these three observations, we can find $x' \in \mathbb{Q}^*$ such that[2] $x' \in x_v \cdot (\mathbb{Q}_v^*)^2$ for all $v \in \mathcal{A}$. In particular this means that $(a, x')_v = (a, x_v)_v = \sigma(a, v)$ for all $v \in \mathcal{A}$ (the Hilbert symbol is the same if we multiply be a square).

Define $\sigma'(a, v) = \sigma(a, v) \cdot (a, x')_v$. We claim that σ' satisfies the three conditions, and that σ', A falls under Case I. It is clear by the Hilbert Product Formula that σ' is 1 on all but finitely many (a, v), so σ' satisfies Condition 1. Again using the Hilbert Product Formula we have that for any $a \in A$,

$$\prod_{v \in V} \sigma'(a, v) = \prod_{v \in V} \sigma(a, v)(a, x')_v = \prod_{v \in V} \sigma(a, v) \prod_{v \in V} (a, x')_v = 1,$$

so σ' satisfies Condition 2. Finally, to see that Condition 3 is satisfied observe that

$$(a, x_v/x')_v = (a, x_v)_v \cdot (a, x')_v = \sigma(a, v)(a, x')_v = \sigma'(a, v).$$

To see why σ', A falls under Case I observe that for any $v \in \mathcal{A}$ we have

$$\sigma'(a, v) = \sigma(a, v) \cdot (a, x')_v = \sigma(a, v) \cdot (a, x_v)_v = \sigma(a, v)^2 = 1.$$

Applying Case I to σ', A we receive $y \in \mathbb{Q}^*$ such that

$$(a, y)_v = \sigma'(a, v)$$

for all $a \in A, v \in V$. Taking $x = yx'$ we have

$$(a, yx')_v = \sigma'(a, v)(a, x')_v = \sigma(a, v)(a, x')_v^2 = \sigma(a, v),$$

as desired.

□

[2] $(\mathbb{Q}_v^*)^2$ denotes the non-zero squares in $\mathbb{Q}_v$, not a Cartesian product.