INTRODUCTION TO THE LOCAL-GLOBAL PRINCIPLE

LIANG XIAO

Abstract. This is the notes of a series lectures on local-global principle and quaternion algebras, given at Connecticut Summer School in Number Theory.

1. Day I: Quaternion Algebras and $\mathbb{Q}_p$

1.1. What are Quaternion Algebras?

1.1.1. *Hamiltonian* $\mathbb{H}$. Recall that we setup mathematics in such a way starting with positive integers $\mathbb{N}$ and integers $\mathbb{Z}$ to build $\mathbb{Q}$ as its quotient field, and then defining $\mathbb{R}$ using several equivalent axioms, e.g. Dedekind cut, or as certain completions. After that, we introduced the field of complex numbers as $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}\mathbf{i}$, satisfying $\mathbf{i}^2 = -1$.

One of the most important theorem for complex numbers is the *Fundamental Theorem of Algebra*: all complex coefficients non-constant polynomials $f(x) \in \mathbb{C}[x]$ has a zero. In other words, $\mathbb{C}$ is an algebraically closed field; so there is no bigger field than $\mathbb{C}$ that is finite dimensional as an $\mathbb{R}$-vector space.

(With the development of physics), Hamilton discovered that there is an "associative-but-non-commutative field" (called a *skew field* or a *division algebra*) $\mathbb{H}$ which is 4-dimensional over $\mathbb{R}$:

$$\begin{aligned}\mathbb{H} &= \mathbb{R} \oplus \mathbb{R}\mathbf{i} \oplus \mathbb{R}\mathbf{j} \oplus \mathbb{R}\mathbf{k} \\ &= \big\{ a\mathbf{i} + b\mathbf{j} + c\mathbf{j} + d\mathbf{k} \;\big|\; a, b, c, d \in \mathbb{R} \big\},\end{aligned}$$

where the multiplication is $\mathbb{R}$-linear and subject to the following rules:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \text{and} \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

This particular $\mathbb{H}$ is called the *Hamiltonian quaternion*.

One simple presentation of $\mathbb{H}$ is:

$$\mathbb{H} := \mathbb{C}\langle \mathbf{i}, \mathbf{j} \rangle \big/ \big(\mathbf{i}^2 + 1,\, \mathbf{j}^2 + 1,\, \mathbf{ij} + \mathbf{ji} \big).$$

Question 1.1.2. Are there other quaternions that look like the Hamiltonian quaternion? Can we classify them?

1.1.3. *Quaternion algebra.* Over $\mathbb{R}$, such quaternion algebra is unique, but over other fields, there are plenty. For example, we can consider

$$D = \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle \big/ \big(\mathbf{i}^2 + 1,\, \mathbf{j}^2 + 1,\, \mathbf{ij} + \mathbf{ji} \big), \tag{1.1.1}$$

or more generally, for any field k (of characteristic zero or just $\mathbb{Q}$, at least today), and any two elements $a, b \in k^\times$ we put

$$D_{k,a,b} := k\langle \mathbf{i}, \mathbf{j} \rangle \big/ \big(\mathbf{i}^2 - a,\, \mathbf{j}^2 - b,\, \mathbf{ij} + \mathbf{ji} \big). \tag{1.1.2}$$

For example, the quaternion in (1.1.1) is $D_{\mathbb{Q},-1,-1}$. These $D_{k,a,b}$ are called *quaternion algebras* over k. In other literature, the quaternion algebras are often denoted by $\left(\frac{a,b}{k}\right)$. It is conventional to put $\mathbf{k} = \mathbf{ij}$ so that

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \text{and} \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Like in the case of complex numbers, every element $\alpha = x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$ has a *conjugate*: $\bar{\alpha} := x - y\mathbf{i} - z\mathbf{j} - w\mathbf{k}$. We note:

$$\mathrm{Tr}(\alpha) := \alpha + \bar{\alpha} = 2x \in k;$$
$$\mathrm{Nm}(\alpha) := \alpha\bar{\alpha} = x^2 - ay^2 - bz^2 + abw^2 \in k.$$

(It looks like we are solving quadratic equations in a non-commutative ring.)

In particular, if $\mathrm{Nm}(\alpha) \neq 0$, then α has an inverse:

$$\alpha^{-1} = \frac{1}{\mathrm{Nm}(\alpha)}\alpha.$$

Quaternion algebras are called *division algebras* if every nonzero element of $D_{k,a,b}$ has a multiplicative inverse (both left and right), this is equivalent to the condition that $x^2 - ay^2 - bz^2 + abw^2$ is always nonzero unless all x, y, z, w are zero.

Example 1.1.4. For $a, b \in \mathbb{Q}_{<0}$, $D_{\mathbb{Q},a,b}$ is a division algebra, because for rational numbers x, y, z, w, $x^2 - ay^2 - bz^2 + abw^2 = 0$ would force $x = y = z = w = 0$ by positivity.

The matrix algebra $\mathrm{M}_2(\mathbb{Q})$ is also a quaternion algebra (but not a division algebra), isomorphic to $D_{\mathbb{Q},-1,1}$, in the sense that taking $\mathbf{i} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\mathbf{j} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ defines an isomorphism $D_{\mathbb{Q},1,-1} \cong \mathrm{M}_2(\mathbb{Q})$.

Question 1.1.5. Are these $D_{k,a,b}$ genuinely different? In Exercise 1.4.6, you will verify some obvious equalities, like $D_{k,a,b} = D_{k,a,-ab} = D_{k,ac^2,b}$ for $a, b, c \in k^\times$.

When are these $D_{k,a,b}$ division algebras?

Example 1.1.6. When $k = \mathbb{R}$, there are (up to isomorphism) two quaternion algebras:

- $\mathbb{H} \cong D_{\mathbb{R},a,b}$ whenever a, b are both negative;
- $\mathrm{M}_2(\mathbb{R}) \cong D_{\mathbb{R},a,b}$ whenever at least one of a and b is positive.

1.1.7. *Local-global approach.* To answer to Question 1.1.5 (for general field k) directly is very difficult; but the question is easier for some particular fields, like $\mathbb{R}$.

In this lecture series, we address Question 1.1.5 in the case when $k = \mathbb{Q}$, and our approach takes the following form: for a quaternion algebra $D_{\mathbb{Q},a,b}$ with $a, b \in \mathbb{Q}$, we consider

$$D_{\mathbb{Q},a,b} \otimes_{\mathbb{Q}} \mathbb{R} \cong D_{\mathbb{R},a,b}.$$

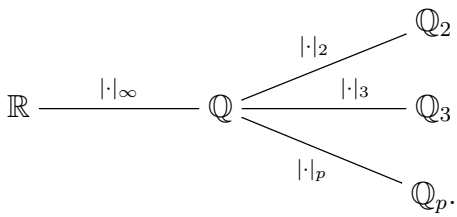
So if for two pairs (a, b) and (a', b'), if $D_{\mathbb{R},a,b} \ncong D_{\mathbb{R},a',b'}$ (which can be tested easily using 1.1.6), then $D_{\mathbb{Q},a,b} \ncong D_{\mathbb{Q},a',b'}$. In other words, what we are doing is:

- testing whether $D_{\mathbb{Q},a,b}$ is isomorphic to $D_{\mathbb{Q},a',b'}$ by tensoring over a bigger field $k/\mathbb{Q}$ (which in our case will be "local fields"), where the corresponding question is easier (namely, a local question); and
- there is a local-global principal we will prove at the end, which shows that, if $D_{\mathbb{Q},a,b}$ and $D_{\mathbb{Q},a',b'}$ are isomorphic after tensoring with "all" local fields, then they are isomorphic.

Such type of argument is called a "local-global argument."

1.2. **Introduction to $\mathbb{Q}_p$.**

1.2.1. *Local fields.* The way we define the real numbers $\mathbb{R}$ (from $\mathbb{Q}$) can be viewed as taking the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|_\infty$, namely to adjoin limits of Cauchy sequences in $\mathbb{Q}$.



In fact, besides the usual absolute value, there are other "absolute values" or norms on $\mathbb{Q}$, essentially one for each prime number p. Completion with respect to the norm associated to the prime p gives the main player today: $\mathbb{Q}_p$.

Definition 1.2.2. Fix a prime p from now on. We define the *p-adic valuation* of a non-zero integer a, denoted by $v_p(a)$, to be the maximal (non-negative integer) exponent n such that $p^n|a$ (or sometimes we write $p^{v_p(a)}||a$). We put $v_p(0) = +\infty$. Clearly we have the following properties:

$$v_p(ab) = v_p(a) + v_p(b) \quad \text{and} \quad v_p(a+b) \geq \min\{v_p(a), v_p(b)\}. \tag{1.2.1}$$

This p-adic valuation extends to a p-adic valuation on $\mathbb{Q}$, given by

$$\begin{aligned} v_p : \mathbb{Q} &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ x = \tfrac{a}{b} &\longmapsto v_p\big(\tfrac{a}{b}\big) := v_p(a) - v_p(b). \end{aligned}$$

We can check that the expression above does not depend on the choice of the writing of x as a rational number $\frac{a}{b}$. The above properties (1.2.1) are still preserved.

Let us put it another way, define:

$$|a|_p := p^{-v_p(a)} \quad \text{for} \quad a \in \mathbb{Q}.$$

For example, $p = 5$, $v_5(\frac{14}{75}) = -2$, and $\big|\frac{14}{75}\big|_5 = 25$. For another, $v_5(100) = 2$ and $\big|100\big|_5 = \frac{1}{25}$.

Let us formalize everything.

Definition 1.2.3. A *valuation* on a field k is a map

$$v : k \longrightarrow \mathbb{Z} \cup \{+\infty\},$$

such that

(a) $v(x) = +\infty$ if and only if $x = 0$,
(b) $v(xy) = v(x) + v(y)$ for all $x, y \in k$, and
(c) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in k$.

We point out that if $v(x) \neq v(y)$, the inequality in (c) is an equality, namely $v(x+y) = \min\{v(x), v(y)\}$ (see Exercise 1.4.8).

A *norm* on a field k is a map

$$|\cdot| : k \to \mathbb{R}_{\geq 0}$$

such that

(1) $|x| = 0$ if and only if $x = 0$,

(2) $|xy| = |x| \cdot |y|$ for all $x, y \in k$, and
(3) (Triangle inequality) $|x + y| \leq |x| + |y|$ for all $x, y \in k$.

It is called *non-archimedean*, if the norm satisfies

(3') (Strong triangle inequality) $|x + y| \leq \max\{|x|, |y|\}$.

In this sense, we have just defined a valuation $v_p(-)$ on $\mathbb{Q}$ for each prime number p, and a norm $|\cdot|_p$ on $\mathbb{Q}$ for each prime number p.

Theorem 1.2.4. *(Ostrowski) The following lits all the norms of $\mathbb{Q}$:*

(1) *the trivial norm $|\cdot|_{\text{triv}}$, namely $|x|_{\text{triv}} = 1$ if $x \neq 0$, and 0 if $x = 0$;*
(2) *(Essentially the real norm) $|\cdot|_\infty^s$ for $s \in (0, 1]$; and*
(3) *(Essentially the p-adic norm) $|\cdot|_p^s = p^{-sv_p(\cdot)}$ for $s \in \mathbb{R}_{>0}$.*

Notation 1.2.5. In view of Ostrowski's theorem, we say *a place* of $\mathbb{Q}$ to mean either a prime number, or the real norm (often denoted by ∞). We may complete $\mathbb{Q}$ with respect to the norm at each place, and get either $\mathbb{Q}_\infty := \mathbb{R}$ or $\mathbb{Q}_p$ for some prime p.

Construction 1.2.6. We define the ring of p-adic integers $\mathbb{Z}_p$ to be the completion of $\mathbb{Z}$ with respect to the p-adic valuation. We can understand this using one of the following equivalent ways.

Understanding I: A p-adic integer is a sequence of integers:

$$a_1, a_2, \dots$$

such that $a_n \equiv a_{n+1} \pmod{p^n}$. (Note that $a_n \equiv a_{n+1} \pmod{p^n}$ implies that $|a_{n+1} - a_n|_p \leq p^{-n}$ which converges to zero.)

We can extend the p-adic valuation v_p to $\mathbb{Z}_p$ by setting

$$v_p((a_n)_{n\in\mathbb{N}}) := \lim_{n\to\infty} v_p(a_n);$$

this limit stabilizes as $n \gg 0$ (or the limit is $0 \in \mathbb{Z}_p$).

Understanding II: A p-adic integer is a sequence of congruences

$$a_1 \bmod p,\ a_2 \bmod p^2,\ a_3 \bmod p^3,\ \dots,$$

such that $a_n \equiv a_{n+1} \pmod{p^n}$.

Understanding III: A p-adic integer can be uniquely written as a infinite series

$$a_0 + a_1 p + a_2 p^2 + \cdots, \tag{1.2.2}$$

with $a_i \in \{0, \dots, p-1\}$. This is called the *$p$-adic expansion* of the p-adic number. In this format, we have

$$v_p(a_0 + a_1 p + \cdots) = \min\{n;\ a_n \neq 0\}.$$

Understanding IV: A p-adic integer is an infinite series

$$a_0 + a_1 p + a_2 p^2 + \cdots \qquad \text{with } a_i \in \mathbb{Z}_p.$$

Here we bring up a key point in p-adic analysis: due to the strong triangle inequality, an infinite sequence converges if the limit of the norm of each term converges to zero (which would imply that the limit of the partial sum $a_m + \cdots + a_n$ converges to zero as both $m, n \to \infty$, as $|a_m + \cdots + a_n| \leq \max\{|a_m|, |a_{m+1}|, \dots, |a_n|\} \to 0$.

Example 1.2.7. We perform a multiplication in the form of Understanding III. Say $p = 5$.

$$\begin{aligned}
&(1 + 5 + 2 \times 5^2 + \cdots) \cdot (3 + 3 \times 5 + 4 \times 5^2 + \cdots) \\
=&1 \cdot 3 + 5 \cdot 3 + 1 \cdot 3 \times 5 + 1 \cdot 4 \times 5^2 + 5 \cdot 2 \times 5 + 2 \times 5^2 \cdot 3 + \cdots \\
=&3 + 6 \times 5 + 12 \times 5^2 + \cdots \\
=&3 + 1 \times 5 + 13 \times 5^2 + \cdots \\
=&3 + 1 \times 5 + 3 \times 5^2 + 2 \times 5^3 + \cdots
\end{aligned}$$

Example 1.2.8. 2 is invertible in the ring $\mathbb{Z}_7$. Modulo 7, we can solve $2x \equiv 1 \pmod 7$, for example $x \equiv 4 \pmod 7$. Then we consider modulo 7^2, we solve $2x \equiv 1 \pmod{7^2}$, we get $x \equiv 25 \pmod{7^2}$. We continue this process to get a sequence of numbers

$$4 \bmod 7,\ 25 \bmod 7^2,\ 172 \bmod 7^3,\ \ldots$$

This gives the multiplicative inverse of 2 in $\mathbb{Z}_7$.

In general, as long as $a \in \mathbb{Z}$ with $p \nmid a$, then a is invertible in $\mathbb{Z}_p$. Or even more generally, if $a \in \mathbb{Z}_p$ with $v_p(a) = 0$, then a is invertible in $\mathbb{Z}_p$. These numbers are call *p-adic units*.

Definition 1.2.9. We define $\mathbb{Q}_p$ to be the fraction field of $\mathbb{Z}_p$, but in fact as illustrated in the example above, $\mathbb{Q}_p \cong \mathbb{Z}_p[\frac{1}{p}]$, because those p-adic integers that are not divisible by p are already invertible in $\mathbb{Z}_p$.

1.3. **Hensel's Lemma.**

Example 1.3.1. We start with an example: finding $\sqrt{2}$ in $\mathbb{Z}_7$. This is equivalent to solving the equation

$$x^2 = 2 \quad \text{in } \mathbb{Z}_7.$$

Method I: We can try to formally do the following:

$$\begin{aligned}
x = 2^{1/2} = (9-7)^{1/2} &= 3 \cdot (1 - \tfrac{7}{9})^{1/2} \\
&= \pm 3 \cdot \sum_{n=0}^{\infty} \binom{1/2}{n} (-\frac{7}{9})^n,
\end{aligned}$$

where $\binom{1/2}{n} := \frac{\frac{1}{2}(-\frac{1}{2})\cdots(\frac{3}{2}-n)}{n!}$ is the formal binomial coefficients. The series converges because $\binom{1/2}{n} \in \mathbb{Z}_7$ and $v_7((-\frac{7}{9})^n) = n \to \infty$.

Method II: We first solve the equation modulo 7. At this stage, we have a choice of square root, either $x \equiv 3 \pmod 7$ or $x \equiv 4 \pmod 7$. We first consider the former case, and the latter case can be obtained similarly (or by just taking the inverse). Now, we solve this modulo $7^2 = 49$. To solve it, we should take $x = 3 + 7y$ for some y. So we are looking at the equation:

$$\begin{aligned}
(3 + 7y)^2 &\equiv 2 \pmod{49}, \\
9 + 42y + 49y^2 &\equiv 2 \pmod{49}, \\
7 + 42y &\equiv 0 \pmod{49}, \\
1 + 6y &\equiv 0 \pmod 7.
\end{aligned}$$

So $y \equiv 1 \pmod 7$. In other words, $x \equiv 3 + 7 \cdot 1 = 10 \pmod{49}$.

We can continue this by considering modulo $7^3 = 343$. We set $x = 10 + 49z$ and consider

$$(10 + 49z)^2 \equiv 2 \pmod{343},$$
$$100 + 20 \cdot 49z + 49^2 z^2 \equiv 2 \pmod{343},$$
$$98 + 20 \cdot 49z \equiv 0 \pmod{343},$$
$$2 + 20z \equiv 0 \pmod{7} \cdots$$

Theorem 1.3.2 (Hensel's Lemma)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$ be a polynomial and let $\bar{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0 \in \mathbb{F}_p[x]$ be its reduction modulo p (where $\bar{a}_i = a_i \bmod p$). Suppose that $\bar{f}(x)$ is a nonzero polynomial (namely $f(x)$ is not entirely divisible by p), and let $\bar{\alpha} \in \mathbb{F}_p$ be a* simple *zero of $\bar{f}(x)$. Then there exists a unique zero $\alpha \in \mathbb{Z}_p$ of $f(x)$ such that $\alpha = \bar{\alpha} \bmod p$.*

Proof. We will construct a sequence of elements $\alpha_1 = \bar{\alpha}, \alpha_2, \alpha_3, \ldots$ such that $\alpha_i \in \mathbb{Z}/p^i\mathbb{Z}$ is a zero of $f(x) \bmod p^n$ and $\alpha_i = \alpha_{i+1} \bmod p^i$.

α_1 is already given to be $\bar{\alpha}$. Now suppose that we have already constructed α_i. In particular $f(\alpha_i) \equiv 0 \pmod{p^i}$. We pick an arbitrary lift α'_{i+1} of α_i in $\mathbb{Z}/p^{i+1}\mathbb{Z}$. It is then clear that $f(\alpha'_{i+1}) \equiv 0 \pmod{p^i}$ but α'_{i+1} might not be a zero of $f(x) \pmod{p^{i+1}}$.

We want to show that we can modify α'_{i+1} to some $\alpha'_{i+1} + cp^i$ with $c \in \{0, \ldots, p-1\}$ such that

$$f(\alpha'_{i+1} + cp^i) \equiv 0 \pmod{p^{i+1}}.$$

There is a formal Taylor expansion law:

$$f(a + b) = f(a) + bf'(a) + b^2 \cdot \tfrac{f''(a)}{2!} + \cdots$$

(Note that the seemingly denominators can be canceled by the coefficients coming out from the derivatives; and this is a finite sum.) So we try to find c such that

$$f(\alpha'_{i+1}) + cp^i f'(\alpha'_{i+1}) + (cp^i)^2 \tfrac{f''(\alpha'_{i+1})}{2!} + \cdots \equiv 0 \pmod{p^{i+1}}.$$

We may ignore the higher degree terms involving $(cp^i)^r$ for $r \geq 2$. So we want

$$\tfrac{f(\alpha'_{i+1})}{p^i} + cf'(\alpha'_{i+1}) \equiv 0 \pmod{p}.$$

By our assumption, $\bar{\alpha}$ is a simple zero for $\bar{f}(x)$; so $f'(\alpha'_{i+1})$ is in fact a p-adic unit. So we can simply take

$$c = \frac{f(\alpha'_{i+1})}{p^i f'(\alpha'_{i+1})} \bmod p.$$

□

Corollary 1.3.3. *Assume $p \geq 3$. For $v \in \mathbb{Z}_p^\times$ to be a square in $\mathbb{Z}_p$, it is necessary and sufficient to ask $\bar{v} = v \bmod p$ is a square in $\mathbb{F}_p$.*

1.4. **Exercises.**

Exercise 1.4.1. Are $\mathbf{i}^2 - \mathbf{j}^2$ and $(\mathbf{i}+\mathbf{j})(\mathbf{i}-\mathbf{j})$ equal in $\mathbb{H}$?

Exercise 1.4.2. Verify the following properties about conjugation for $q = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \in \mathbb{H}$. We have $\bar{q}_1 + \bar{q}_2 = \overline{q_1+q_2}$, $\bar{q}_1 \cdot \bar{q}_2 = \overline{q_2 q_1}$, $\bar{\bar{q}} = q$, and $\bar{q} = q$ if and only if $q \in \mathbb{R}$.

Exercise 1.4.3. Show that the center of $\mathbb{H}$ is $\mathbb{R}$, namely,

$$\left\{q \in \mathbb{H} \;\middle|\; qq' = q'q \text{ for all } q' \in \mathbb{H}\right\}.$$

Exercise 1.4.4. Verify that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} := \mathbb{C}\langle \mathbf{i}, \mathbf{j}\rangle \cong \mathrm{M}_2(\mathbb{C})$. What is $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$ isomorphic to?

Exercise 1.4.5. Write down explicitly an $\mathbb{R}$-algebra embedding of $\mathbb{H}$ into $\mathrm{M}_2(\mathbb{C})$.

Exercise 1.4.6. For the quaternion algebra $D_{k,a,b}$ defined in (1.1.2), show that

$$D_{k,a,b} \cong D_{k,b,a} \cong D_{k,a,-ab}.$$

Also, for elements $r, s \in k^\times$, we have

$$D_{k,a,b} \cong D_{k,ar^2,bs^2}.$$

Using these special isomorphisms, deduce that there are only two quaternion algebras over $\mathbb{R}$: namely, $\mathbb{H} = D_{\mathbb{R},-1,-1}$ and $\mathrm{M}_2(\mathbb{R}) \cong D_{\mathbb{R},1,1} \cong D_{\mathbb{R},-1,1} \cong D_{\mathbb{R},1,-1}$.

Exercise 1.4.7. For the quaternion algebra $D_{k,a,b}$, if a is a square in k, then $D_{k,a,b}$ is isomorphic to the matrix algebra $\mathrm{M}_2(k)$.

Exercise 1.4.8. Let v be a valuation on a field k. For any two elements $x, y \in k$, if $v(x) \neq v(y)$, then $v(x+y) = \min\{v(x), v(y)\}$. In particular, this means that all the triangles in $\mathbb{Q}_p$ are isosceles.

Exercise 1.4.9. Let R be an integral domain and let $k := \mathrm{Frac}(R)$ be its fraction field. Suppose that we are given a valuation v on R, namely a map $v : R \to \mathbb{Z} \cup \{0\}$ satisfying conditions Definition 1.2.3(a)(b)(c) for $x, y \in R$. Prove that v admits a unique extension to a valuation on k.

Exercise 1.4.10. For $r \in \mathbb{R}_{>0}$, consider the following norm on $\mathbb{Q}_p[x]$: for $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Q}_p[x]$,

$$\|f(x)\|_r := \max_i \left\{|a_i|_p r^i\right\},$$

namely we set $\|x\|_r = r$ and for general polynomial, we just take the maximum.

Prove that this defines a valuation on $\mathbb{Q}_p[x]$ and hence defines a valuation on $\mathbb{Q}_p(x)$ by Exercise 1.4.9.

Exercise 1.4.11. Prove the following stronger version of the Hensel's lemma. Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial and suppose that $\bar{f}(x) := f(x) \bmod p$ factors as $\bar{g}(x)\bar{h}(x)$ with $\bar{g}(x), \bar{h}(x) \in \mathbb{F}_p[x]$ coprime and $\bar{g}(x)$ monic. Then there exists a unique factorization $f(x) = g(x)h(x)$ such that

$$\bar{g}(x) = g(x) \bmod p, \qquad \bar{h}(x) = h(x) \bmod p,$$

and that $g(x)$ is monic and $\deg g(x) = \deg \bar{g}(x)$.

2. Day II: Hilbert Symbols

2.1. Structure of $\mathbb{Q}_p^\times$.

Lemma 2.1.1. *For each $\bar{a} \in \mathbb{F}_p^\times$, there is a unique $(p-1)$st root of unity a whose reduction modulo p is $\bar{a}$. This a is called the* Teichmüller lift *of $\bar{a}$.*

Moreover, for $\bar{a}, \bar{b} \in \mathbb{F}_p^\times$, we have $[\bar{a}] \cdot [\bar{b}] = [\bar{a}\bar{b}] \in \mathbb{Z}_p^\times$.

Proof. Recall that the multiplicative group $\mathbb{F}_p^\times$ is cyclic of order $p-1$. So each element gives a solution to the equation $x^{p-1} - 1 = 0$ in $\mathbb{F}_p$, and by counting, they are all the solutions (and they are distinct). By Hensel's lemma (Theorem 1.3.2) the solution $\bar{a}$ lifts uniquely to a solution, denoted by $[\bar{a}]$, of the equation $x^{p-1} - 1 = 0$ in $\mathbb{Z}_p$, such that $[\bar{a}] \bmod p = \bar{a}$. This $[\bar{a}]$ is what we sought for.

To see $[\bar{a}] \cdot [\bar{b}] = [\bar{a}\bar{b}]$, we observe that $[\bar{a}]$ and $[\bar{b}]$ being $(p-1)$st roots of unity implies that $[\bar{a}] \cdot [\bar{b}]$ is also a $(p-1)$st root of unity, whose reduction modulo p is $\bar{a}\bar{b}$. By the uniqueness, we see that $[\bar{a}] \cdot [\bar{b}] = [\bar{a}\bar{b}]$. □

The goal in this subsection is to prove the following:

Proposition 2.1.2. *For a prime $p \geq 3$, we have isomorphisms of topological groups:*

$$\begin{array}{ccccc} \mathbb{Q}_p^\times & \xrightarrow{\cong} & \mathbb{Z} \times \mathbb{Z}_p^\times & \xrightarrow{\cong} & \mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p \\ p^n a & \longmapsto & (n, a) & & \\ & & (n, [\bar{a}] \cdot \exp(px)) & \longmapsto & (n, \bar{a}, x), \end{array}$$

where $\exp(px) := 1 + px + \frac{(px)^2}{2!} + \cdots \in 1 + p\mathbb{Z}_p$ which converges for $x \in \mathbb{Z}_p$, and $[a]$ is the Teichmüller lift of $\bar{a}$.

When $p = 2$, we need a small modification:

$$\begin{array}{ccccc} \mathbb{Q}_2^\times & \xrightarrow{\cong} & \mathbb{Z} \times \mathbb{Z}_2^\times & \xrightarrow{\cong} & \mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^\times \times \mathbb{Z}_2 \\ 2^n a & \longmapsto & (n, a) & & \\ & & (n, [\bar{a}] \cdot \exp(4x)) & \longmapsto & (n, \bar{a}, x), \end{array}$$

where $\exp(4x) := 1 + 4x + \frac{(4x)^2}{2!} + \cdots \in 1 + 4\mathbb{Z}_2$ which converges for $x \in \mathbb{Z}_2$, and

$$[1 \bmod 4] = 1 \in \mathbb{Z}_2 \quad \textit{and} \quad [-1 \bmod 4] = -1 \in \mathbb{Z}_2.$$

Proof. First, any non-zero element of $\mathbb{Q}_p$ can be written as a product $p^n a$ with $n \in \mathbb{Z}$ and $a \in \mathbb{Z}_p$ such that a is not divisible by p. As explained in Example 1.2.8, a is invertible in $\mathbb{Z}_p$. So we have a natural isomorphism

$$\begin{array}{ccc} \mathbb{Q}_p^\times & \xrightarrow{\cong} & \mathbb{Z} \times \mathbb{Z}_p^\times \\ p^n a & \longmapsto & (n, a) \\ a & \longmapsto & (v_p(a), a p^{-v_p(a)}). \end{array}$$

Now we study the group structure of $\mathbb{Z}_p^\times$. We write $q = p$ if $p \geq 3$ and $q = 4$ if $p = 2$, we have maps in both directions

$$\begin{array}{ccc} \mathbb{Z}_p^\times & \overset{\text{mod } q}{\underset{[-]}{\rightleftarrows}} & (\mathbb{Z}/q\mathbb{Z})^\times \\ a & \longmapsto & a \bmod q \\ [\bar{a}] & \longmapsfrom & \bar{a}. \end{array}$$

When $p \geq 3$, the reverse map is the Teichmüller map $[-]$. When $p = 2$, the reverse map $(\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{Z}_2^\times$ sends 1 mod 4 to $1 \in \mathbb{Z}_2^\times$ and sends -1 mod 4 to $-1 \in \mathbb{Z}_2^\times$.

The mod q map is surjective; the composition $[\bar{a}] \bmod q = \bar{a}$ is the identity. So we can split off this factor as

$$\begin{array}{ccc} \mathbb{Z}_p^\times & \xrightarrow{\cong} & (\mathbb{Z}/q\mathbb{Z})^\times \times (1 + q\mathbb{Z}_p)^\times \\ [\bar{a}]b & \longmapsfrom & (\bar{a}, b) \\ a & \longmapsto & (a \bmod q,\ a \cdot [a \bmod q]^{-1}). \end{array}$$

We finally come to give the structure of $(1 + q\mathbb{Z}_p)^\times$. For this, we introduce two functions, inverse of each other.

$$\begin{array}{ccc} (1 + q\mathbb{Z}_p)^\times & \overset{\frac{1}{q}\log(\bullet)}{\underset{\exp(q\bullet)}{\rightleftarrows}} & \mathbb{Z}_p \\ 1 + qa & \longmapsto & \frac{1}{q}\log(1 + qa) \\ \exp(qb) & \longmapsfrom & b. \end{array}$$

These two maps are given by

$$\tfrac{1}{q}\log(1 + qa) = \tfrac{1}{q}\big(qa - \tfrac{(qa)^2}{2} + \tfrac{(qa)^3}{3} - \cdots\big) = a - \tfrac{qa^2}{2} + \tfrac{q^2a^3}{3} - \cdots,$$

$$\exp(qb) = 1 + qb + \tfrac{(qb)^2}{2!} + \tfrac{(qb)^3}{3!} + \cdots.$$

They clearly converge and have to be inverse of each other. □

2.2. **Classification of quaternion algebras over $\mathbb{R}$ or $\mathbb{Q}_p$.** We have done the classification of quaternion algebras over $\mathbb{R}$ in Example 1.1.6. In this subsection, we study this over $\mathbb{Q}_p$. We start with some general facts about quaternion algebras.

Lemma 2.2.1 (bis. Exercise 1.4.7)**.** *If $a \in k^\times$ is a square, namely, $a = (\sqrt{a})^2$ for some $\sqrt{a} \in k^\times$, then for any $b \in k^\times$, $D_{k,a,b}$ is isomorphic to $\mathrm{M}_2(k)$.*

Proof. It is easy to check that the following map $\varphi : D_{k,a,b} \to \mathrm{M}_2(k)$ gives a (k-algebra) isomorphism

$$\varphi(\mathbf{i}) = \left(\begin{smallmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{smallmatrix}\right) \quad \text{and} \quad \varphi(\mathbf{j}) = \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right).$$

The key here is that, for this carefully chosen map, $\varphi(\mathbf{i})\varphi(\mathbf{j}) = -\varphi(\mathbf{j})\varphi(\mathbf{i})$. □

Proposition 2.2.2. *Suppose that $a \in k^\times$ is not a square in k. Then the quaternion algebra $D_{k,a,b}$ for $b \in k^\times$ is isomorphic to $\mathrm{M}_2(k)$ if and only if b is a norm from $k(\sqrt{a})$, namely,*

$$b = \mathrm{Nm}(x + \sqrt{a}y) := (x + \sqrt{a}y)(x - \sqrt{a}y) = x^2 - ay^2 \quad \text{for some } x, y \in k.$$

Remark 2.2.3. In view of Lemma 2.2.1, the assumption that $a \in k^\times$ is not a square in k is not necessary, as in that case, Lemma 2.2.1 implies that $D_{k,a,b}$ is isomorphic to $\mathrm{M}_2(k)$ and b is clear a norm from $k(\sqrt{a}) = k$.

Proof of Proposition 2.2.2. If $b = x^2 - ay^2$ for some $x, y \in k$, we can define a map $\varphi : D_{k,a,b} \to \mathrm{M}_2(k)$ that gives a (k-algebra) isomorphism

$$\varphi(\mathbf{i}) = \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right) \quad \text{and} \quad \varphi(\mathbf{j}) = \left(\begin{smallmatrix} x & ay \\ -y & -x \end{smallmatrix}\right).$$

Note here that the key is that we can check

$$\varphi(\mathbf{j})^2 = \left(\begin{smallmatrix} x & y \\ -ay & -x \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ -ay & -x \end{smallmatrix}\right) = \left(\begin{smallmatrix} x^2-ay^2 & xy-yx \\ -ayx-x(-ay) & -ay^2+(-x)^2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} b & 0 \\ 0 & b \end{smallmatrix}\right), \quad \text{and}$$

$$\varphi(\mathbf{i})\varphi(\mathbf{j})\varphi(\mathbf{i}^{-1}) = \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & ay \\ -y & -x \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1/a & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -ay & -ax \\ x & ay \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1/a & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -x & -ay \\ y & x \end{smallmatrix}\right) = -\varphi(\mathbf{j}).$$

Conversely, we assume that there is an isomorphism $\varphi : D_{k,a,b} \to \mathrm{M}_2(k)$. Then $\varphi(\mathbf{i})$ is a matrix that satisfies $\varphi(\mathbf{i})^2 = a \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (namely it is a zero of the equation $x^2 - a = 0$). We can always conjugate it into its "normal form,", namely, there exists $g \in \mathrm{GL}_2(k)$ such that

$$g\varphi(\mathbf{i})g^{-1} = \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right)$$

So we can consider a new k-algebra isomorphism $\varphi' : D_{k,a,b} \to \mathrm{M}_2(k)$ given by $\varphi'(q) := g\varphi(q)g^{-1}$. Thus $\varphi'(\mathbf{i}) = \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right)$.

Now, we put

$$\varphi'(\mathbf{j}) = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right), \quad \text{where } (x, y, z, w) \neq (0, 0, 0, 0).$$

Then it must satisfy the conditions

$$\varphi'(\mathbf{i})\varphi'(\mathbf{j}) = -\varphi'(\mathbf{j})\varphi'(\mathbf{i}), \text{ namely, } \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) = -\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right).$$

From this we deduce that $y = -az$ and $x = -w$. Plugging this information to the equality $\varphi'(\mathbf{j})^2 = \left(\begin{smallmatrix} b & 0 \\ 0 & b \end{smallmatrix}\right)$, we deduce that

$$\left(\begin{smallmatrix} -w & -az \\ z & w \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} b & 0 \\ 0 & b \end{smallmatrix}\right), \quad \text{and hence} \quad w^2 - az^2 = b.$$

This implies that b is the norm of $w + z\sqrt{a} \in k(\sqrt{a})$. □

The following corollary is a variant of the Proposition above.

Corollary 2.2.4. *Suppose that $a \in k^\times$ is not a square in k. Let b' be a norm from $k(\sqrt{a})$. Then the quaternion algebra $D_{k,a,b}$ is isomorphic to $D_{k,a,bb'}$.*

Proof. We leave this as an exercise. □

Remark 2.2.5. At least for $k = \mathbb{R}$ or $\mathbb{Q}_p$, the converse of Corollary 2.2.4 is true, namely if the quaternion algebra $D_{k,a,b}$ and $D_{k,a,b'}$ are isomorphic if and only if $b'/b \in k$ is a norm from $k(\sqrt{a})$.

Definition 2.2.6. Let K denote either $\mathbb{R}$ or a p-adic field $\mathbb{Q}_p$. For two elements $a, b \in K$, we define the *Hilbert symbol* of a and b relative to K to be

- $(a, b) = 1$ if $D_{K,a,b}$ is isomorphic to $\mathrm{M}_2(K)$, and
- $(a, b) = -1$ otherwise.

(Note: our definition is slightly different from but is equivalent to the usual definition.) By Exercise 1.4.6, It is clear that if we multiply a or b by a square in K, the value of the Hilbert symbol is unchanged. So the Hilbert symbol defines a map

$$(-,-):\ K^\times/(K^\times)^2\ \times\ K^\times/(K^\times)^2\ \longrightarrow \{\pm 1\}.$$

Moreover, if either a or b is a square itself, $(a,b)=1$.

Example 2.2.7. For $K=\mathbb{R}$, $(a,b)=1$ if either a or b is positive (namely a square); and $(a,b)=-1$ if $a<0$ and $b<0$.

Lemma 2.2.8. *The Hilbert symbols satisfy the following relations, for $a,b,c,r,s\in k^\times$.*

(1) $(a,b)=(b,a)=(a,-ab)$, $(a,c^2)=1$, *and* $(a,b)=(ar^2,bs^2)$.
(2) $(a,1-a)=1$ *if* $a\neq 1$.
(3) *if* $(a,b)=1$ *then* $(a,b')=(a,bb')$.

Proof. (1) These equalities follow from the isomorphisms among the corresponding quaternion algebras, listed in Question 1.1.5 (and Lemma 2.2.1).

(2) follows from Lemma 2.2.2 because (when a is not a square) $1-a$ is the norm of $1+\sqrt{a}\in k(\sqrt{a})$.

(3) By Proposition 2.2.2, $(a,b)=1$ implies that b is a norm from $k(\sqrt{a})$, which further implies $D_{K,a,b'}\cong D_{K,a,bb'}$ by Corollary 2.2.4. □

Theorem 2.2.9. *Fix the field K to be either $\mathbb{R}$ or a p-adic field $\mathbb{Q}_p$.*

(1) *All quaternion algebras $D_{K,a,b}$ with $(a,b)=-1$ are division rings and are isomorphic to each other. So the isomorphism classes of quaternion algebras over K is uniquely determined by the Hilbert symbol $(-,-)$.*
(2) *The pairing $(-,-)$ on $K^\times/(K^\times)^2$ is symmetric and* bilinear. *Explicitly, when $K=\mathbb{R}$, we have*

$$(a,b)_\infty=\begin{cases}1 & \text{if } a \text{ or } b \text{ is positive}\\ -1 & \text{if both } a \text{ and } b \text{ are negative.}\end{cases}$$

When $K=\mathbb{Q}_p$, if $a=p^\alpha u$ and $b=p^\beta v$ for $u,v\in\mathbb{Z}_p^\times$, then

$$(a,b)_p=\begin{cases}(-1)^{\alpha\beta\cdot(p-1)/2}\left(\frac{u}{p}\right)^\beta\left(\frac{v}{p}\right)^\alpha, & \text{if } p>2\\ (-1)^{\frac{(u-1)(v-1)}{4}}\cdot(-1)^{\alpha\frac{v^2-1}{8}+\beta\frac{u^2-1}{8}}, & \text{if } p=2,\end{cases}\tag{2.2.1}$$

where $\left(\frac{u}{p}\right)$ (and similarly $\left(\frac{v}{p}\right)$) is the quadratic residue, namely it is 1 if u is a square modulo p, and -1 otherwise.

When p is odd, we also list its values on coset representatives of the quotient $K^\times/(K^\times)^2$. Let $\bar\alpha$ denote a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$, and $\alpha:=[\bar\alpha]$ denote its Teichmüller lift as in Proposition 2.1.2. Then $\{1,\alpha,p,p\alpha\}$ form a coset representative of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. The pairing $(a,b)_p$ is presented in the following two tables.

$(a,b)_p$ *for* $p\equiv 1 \pmod 4$	$a=1$	$a=\alpha$	$a=p$	$a=p\alpha$
$b=1$	1	1	1	1
$b=\alpha$	1	1	-1	-1
$b=p$	1	-1	1	-1
$b=p\alpha$	1	-1	-1	1

$(a,b)_p$ *for* $p \equiv 1 \pmod 4$	$a=1$	$a=\alpha$	$a=p$	$a=p\alpha$
$b=1$	1	1	1	1
$b=\alpha$	1	1	-1	-1
$b=p$	1	-1	-1	1
$b=p\alpha$	1	-1	1	-1

Proof. We separate the cases depending on K. The bilinearity of the Hilbert symbol is a corollary of the explicit formula we give.

When $K=\mathbb{R}$, this is clear.

When $K=\mathbb{Q}_p$ with p an odd prime, Proposition 2.1.2 says that $\mathbb{Q}_p^\times$ is isomorphic to $\mathbb{Z}\times(\mathbb{Z}/p\mathbb{Z})^\times\times\mathbb{Z}_p$ as a topological group. It follows that

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \frac{\mathbb{Z}}{2\mathbb{Z}}\times\frac{(\mathbb{Z}/p\mathbb{Z})^\times}{((\mathbb{Z}/p\mathbb{Z})^\times)^2}\times\frac{\mathbb{Z}_p}{2\mathbb{Z}_p}. \tag{2.2.2}$$

Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$, the quotient $(\mathbb{Z}/p\mathbb{Z})^\times/((\mathbb{Z}/p\mathbb{Z})^\times)^2$ has order 2 and is generated by a generator, say $\bar\alpha$, of $(\mathbb{Z}/p\mathbb{Z})^\times$. We write $\alpha=[\bar\alpha]$ for its Teichmüller lift. Since p is odd, $\mathbb{Z}_p=2\mathbb{Z}_p$. The last term of (2.2.2) is trivial. So the total quotient (2.2.2) is isomorphic to the Klein group with generators p and α (after realizing the elements in $\mathbb{Q}_p^\times$). This implies that the set $\{1,\alpha,p,p\alpha\}$ form a coset representatives of the quotient $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

We first verify (2.2.1); for which it suffices to discuss the case when $\alpha,\beta\in\{0,1\}$.

Case of $\alpha=\beta=0$: We need to show that $D_{\mathbb{Q}_p,u,v}$ is isomorphic to $\mathrm{M}_2(\mathbb{Q}_p)$ (if $u,v\in\mathbb{Z}_p^\times$). If either $u \bmod p$ or $v \bmod p$ (which is non-zero by our assumption) is a square in $\mathbb{F}_p$ then Hensel lemma would imply that either u or v is square in $\mathbb{Z}_p$, we are done by Lemma 2.2.1.

We now assume that this is not the case. So we need to show that v is a norm from $\mathbb{Q}_p(\sqrt{u})$, namely of the form x^2-uy^2.

We first consider this modulo p. Since $\sqrt{u}$ is not a square in $\mathbb{F}_p$, $\mathbb{F}_p[\sqrt{u}]$ is a quadratic extension of $\mathbb{F}_p$, which must be isomorphic to the unique finite field of order p^2. Its multiplicative group is a cyclic group of order p^2-1. The map $s+\sqrt{u}t\mapsto s-\sqrt{u}t$ for $s,t\in\mathbb{F}_p$ is the unique automorphism of $\mathbb{F}_p[\sqrt{u}]$ that fixes $\mathbb{F}_p$, which must be the same as raising to the pth power in $\mathbb{F}_{p^2}$. From this, we see that the norm map

$$\mathbb{F}_p[\sqrt{u}]^\times\cong\mathbb{F}_{p^2}^\times\to\mathbb{F}_p^\times$$

is given by raising to the $(p+1)$st power, and can be identified with the map of cyclic groups

$$\mathbb{Z}/(p^2-1)\mathbb{Z}\longrightarrow\mathbb{Z}/(p-1)\mathbb{Z},\qquad \lambda\mapsto(p+1)\lambda.$$

In particular such norm map is surjective. So any element $\bar v\in\mathbb{F}_p^\times$ is in the image of this norm map, namely, $\bar v=\bar x^2-\bar u\bar y^2$ for some $\bar x,\bar y\in\mathbb{F}_p$. Moreover, in our situation with $\bar v=v \bmod p$, $\bar y$ cannot be zero because $\bar v$ is not a square modulo p is either.

Now we want to lift the equality $\bar v=\bar x^2-\bar u\bar y^2$ to an equality in $\mathbb{Z}_p$. For this, we pick an arbitrary lift x of $\bar x$. Then $uy^2=x^2-v$ has non-zero solutions (and hence different) solutions modulo p. Hensel's lemma (Theorem 1.3.2) allows us to give an element $y\in\mathbb{Z}_p$ such that $uy^2=x^2-v$. This completes the proof in this case.

Case of $\alpha=0$ and $\beta=1$: We have $a=pu$ and $b=v$ for $u,v\in\mathbb{Z}_p^\times$.

In this case, we need to show that $(a,b)_p=\left(\frac{v}{p}\right)$. If $v \bmod p$ is a square modulo p, then it is a square in $\mathbb{Z}_p$ by Hensel's lemma. In this case $D_{\mathbb{Q}_p,a,v}$ is isomorphic to $\mathrm{M}_2(\mathbb{Q}_p)$.

If $v \bmod p$ is not a square in $\mathbb{Z}_p$ (so v is not a square in $\mathbb{Z}_p$), we need to show that $D_{\mathbb{Q}_p,a,v}$ is not isomorphic to $\mathrm{M}_2(\mathbb{Q}_p)$, or equivalently a is not a norm from $\mathbb{Q}_p(\sqrt{v})$, namely $pu = a = x^2 - vy^2$ does not have solutions in $\mathbb{Q}_p$. Suppose it does. Note that the p-adic valuations of x^2 and vy^2 are even integers, so by strong triangle inequality, we must have $v_p(x^2) = v_p(vy^2) \leq 0$. Say $v_p(x) = v_p(y) = -n$ for $n \in \mathbb{Z}_{\geq 0}$. Then we have $p^{2n+1}u = (p^n x)^2 - v(p^n y)^2$. Modulo p, we see that $0 = \bar{\lambda}^2 - \bar{v}\bar{\mu}^2$ for $\bar{\lambda} = p^n x \bmod p$, and $\bar{\mu} = p^n y \bmod p$. But this would then imply that $\bar{v} = (\bar{\mu}/\bar{\lambda})^2$ is a square in $\mathbb{F}_p$, which contradicts our assumption.

Case of $\alpha = \beta = 1$: For $a = pu$ and $b = pv$, we have

$$(pu, pv)_p = (pu, -p^2uv)_p = (pu, -uv)_p = \big(\frac{-uv}{p}\big) = \big(\frac{-1}{p}\big)\big(\frac{u}{p}\big)\big(\frac{v}{p}\big) = (-1)^{(p-1)/2}\big(\frac{u}{p}\big)\big(\frac{v}{p}\big).$$

Now, we have to verify that when $(a, b) = -1$, the corresponding division algebras are isomorphic. For this, we separate the congruences.

Case of $p \equiv 1 \pmod 4$: This is the case when -1 is a square modulo p and hence a square in $\mathbb{Z}_p$ by Hensel's lemma (Theorem 1.3.2). When $p \equiv 1 \pmod 4$, the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$ (which is divisible by 4). So -1 is a square modulo p. By Hensel's Lemma (Theorem 1.3.2), -1 has a square root in $\mathbb{Z}_p$. It follows that

$$D_{\mathbb{Q}_p,a,b} \cong D_{\mathbb{Q}_p,a,-ab} \cong D_{\mathbb{Q}_p,a,ab} \tag{2.2.3}$$

in this case. taking $a = \alpha$ and $b = p$, we see that

$$D_{\mathbb{Q}_p,a,ap} \cong D_{\mathbb{Q}_p,a,p} \cong D_{\mathbb{Q}_p,p,a} \cong D_{\mathbb{Q}_p,p,ap}.$$

Case of $p \equiv 3 \pmod 4$: We leave this as an exercise. □

Lemma 2.2.10. *Let p be an odd prime. Suppose that $\bar{u}$ is not a square in $\mathbb{F}_p$. for any $\bar{v} \in \mathbb{F}_p^\times$, there exist exist non-zero elements $\bar{x}, \bar{y} \in \mathbb{F}_p$ such that $\bar{x}^2 - \bar{u}\bar{y}^2 = \bar{v}$ in $\mathbb{F}_p$.*

Proof. Since -1 is not a square in $\mathbb{F}_p$, neither $\bar{x}$ nor $\bar{y}$ can be zero if $(\bar{x}, \bar{y})$ is a solution. Moreover, -1 being non-square implies that $\mathbb{F}_p[\sqrt{-1}]$ gives a quadratic extension over $\mathbb{F}_p$, and itself must be isomorphic to the finite field of p^2 elements, namely, $\mathbb{F}_{p^2}$. □

2.3. **Exercises.**

Exercise 2.3.1. Prove Corollary 2.2.4 by writing down an explicit isomorphism (hint: how do we realize $x + y\sqrt{a}$ in $D_{k,a,b}$?) Show that its inverse for $k = \mathbb{R}$ and $\mathbb{Q}_p$ (in the sense of Remark 2.2.5) follows from Theorem 2.2.9.

Exercise 2.3.2. There is a different definition of Hilbert symbols. For $a, b \in K^\times$,

- $(a, b)' = 1$ if the equation $z^2 - ax^2 - by^2 = 0$ has nontrivial solutions in K,
- $(a, b)' = -1$ if otherwise.

Prove that $(a, b) = (a, b)'$.

Exercise 2.3.3. Assume that $p > 2$ is a prime number. This appeared in the course of the proof of Theorem 2.2.9. Consider an equation $ax^2+by^2 = c$ with $a, b \in \mathbb{Z}_p^\times$ and $c \in \mathbb{Z}_p$. Write $\bar{a}$, $\bar{b}$, and $\bar{c}$ for the reduction of a, b, and c respectively. Suppose that we have a solution $\bar{x}_0, \bar{y}_0 \in \mathbb{F}_p^\times$ of the mod p equation $\bar{a}\bar{x}^2+\bar{b}\bar{y}^2 = \bar{c}$. Describe all solutions (x, y) to $ax^2+by^2 = c$ for which $(x, y) \pmod p = (\bar{x}, \bar{y})$.

Geometrically, if we think that the equation $ax^2 + by^2 = c$ defines a curve in $\mathbb{Z}_p^2$, and its reduction $\bar{a}\bar{x}^2 + \bar{b}\bar{y}^2 = \bar{c}$ defines a curve over $\mathbb{F}_p^2$, then our question is to describe the inverse image of the point $(\bar{x}_0, \bar{y}_0)$ on the special fiber of the curve, under the mod p reduction map.

Exercise 2.3.4. Complete the proof of Theorem 2.2.9 in the case of $p = 2$, and the case when $p \equiv 3 \pmod 4$.

Exercise 2.3.5. For any $a, b \in \mathbb{F}_p^\times$, the quaternion algebra $D_{\mathbb{F}_p,a,b}$ is isomorphic to $\mathrm{M}_2(\mathbb{F}_p)$. (Hint: use the criterion in Proposition 2.2.2 and the argument in case $\alpha = \beta = 0$ in the proof of Theorem 2.2.9.)

Exercise 2.3.6. We want to generalize the embedding of $\mathbb{H}$ into $\mathrm{M}_2(\mathbb{C})$ in Exercise 1.4.5, to an embedding of general quaternion $D_{k,a,b}$ into a 2×2-matrix ring. We assume that the characteristic of k is not 2.

(1) For $a \in k^\times$, show that if a is a square, then $k[t]/(t^2 - a)$ is isomorphic to $k \times k$; and if a is not a square, $k[t]/(t^2 - a)$ is a degree 2 extension of k.

(2) Verify that the following map $\varphi : D_{k,a,b} \to \mathrm{M}_2(k[t]/(t^2 - a))$ defines a k-algebra isomorphism.

$$\varphi(\mathbf{i}) = \left(\begin{smallmatrix} t & 0 \\ 0 & -t \end{smallmatrix}\right), \quad \varphi(\mathbf{j}) = \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right).$$

(3) When a is a square in k, Lemma 2.2.1 implies that $D_{k,a,b}$ is isomorphic to $\mathrm{M}_2(k)$ by giving an explicit isomorphism. How does that isomorphism compare to the map φ in (2)?

3. Day III: Local-global Principle

Definition 3.0.1. Recall that a place of $\mathbb{Q}$ is either a prime number p or ∞ (which corresponds to the usual absolute norm). At each place, we have a completion of $\mathbb{Q}$: either $\mathbb{Q}_p$ or $\mathbb{Q}_\infty := \mathbb{R}$.

Let $D = D_{\mathbb{Q},a,b}$ be a quaternion algebra (associated to some $a, b \in \mathbb{Q}^\times$).

- We say that D *splits* (or is *unramified*) at a place v if $D \otimes_{\mathbb{Q}} \mathbb{Q}_v = D_{\mathbb{Q}_v,a,b}$ is isomorphic to $\mathrm{M}_2(\mathbb{Q}_v)$;
- otherwise $D \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is isomorphic to a unique division algebra over $\mathbb{Q}_v$ by Theorem 2.2.9, and we say D is *ramified* at v.

Conventionally, we say a quaternion algebra D over $\mathbb{Q}$ is *definite* if it is ramified at ∞, and is *indefinite* if it splits at ∞.

Today, we prove the following theorem that classifies the quaternion algebras over $\mathbb{Q}$.

Theorem 3.0.2. *There is a one-to-one correspondence between the isomorphism classes of quaternion algebras over $\mathbb{Q}$ and finite subsets of places of $\mathbb{Q}$ with even cardinality. For a quaternion algebra D over $\mathbb{Q}$, the corresponding finite set is*

$$\Sigma(D) := \{v \text{ a place of } \mathbb{Q} \mid D \otimes_{\mathbb{Q}} \mathbb{Q}_v \text{ is a division algebra}\}.$$

This theorem consists of the following statements:

(1) If D is a quaternion algebra, then the set of ramified places $\Sigma(D)$ as defined above is a finite set with even cardinality.
(2) Conversely, given a finite set Σ of places of $\mathbb{Q}$ with even cardinality, there exists a quaternion algebra D_Σ which exactly ramifies at the places in Σ.
(3) Finally, for any two quaternion algebras D and D', if they are ramified at the same set of places.

Remark 3.0.3. This theorem is a typical example of local-global principle we normally see in mathematics. We should view it as a map (which I would call "global-to-local map")

$$\{\text{math objects over } \mathbb{Q}\} \longrightarrow \{\text{collections of math objects over each of } \mathbb{Q}_v\} \tag{3.0.1}$$

given by changing the base from $\mathbb{Q}$ to $\mathbb{Q}_v$ for each v.

(1) and (2) of Theorem 3.0.2 together can be interpreted as describing the image of this map, or equivalently the "cokernel" of this map. (3) essentially says that this map is "injective".

In mathematics, many mathematical problems over $\mathbb{Q}$ is broken up into several steps using such a global-to-local map:

(i) Understand the base change of this math problem to $\mathbb{Q}_v$ for each of the places of v.
(ii) Understand the kernel of the corresponding map (3.0.1) (which is probably often the easier direction).
(iii) Understand the image/cokernel of the corresponding map (3.0.1), which is often difficult.

3.1. Product formula for Hilbert Symbols.

Theorem 3.1.1 (Product formula)**.** *For two rational numbers $a, b \in \mathbb{Q}^\times$, we write $(a, b)_v$ for the Hilbert symbol of the pair (a, b) viewed as elements in $\mathbb{Q}_v^\times$. Then $(a, b)_v = 1$ for all*

but finitely many places v of $\mathbb{Q}$. Moreover, we have a product formula:

$$\prod_{v \text{ place of } \mathbb{Q}} (a,b)_v = 1. \tag{3.1.1}$$

If $D = D_{\mathbb{Q},a,b}$, then by definition $(a,b)_v = -1$ if and only if $v \in \Sigma(D)$. So Theorem 3.1.1 implies (1) of Theorem 3.0.2.

Remark 3.1.2. This type of product formula is a very common form of describing

A first example of such product formula is the following: for any element $x \in \mathbb{Q}^\times$, we have

$$\prod_{v \text{ places of } \mathbb{Q}} |x|_v = 1. \tag{3.1.2}$$

Here we normalize the norm so that $|p|_p = p^{-1}$. The proof of this is simple: since both side of (3.1.2) is multiplicative in x, it suffices to check it for $x = -1$ and $x = p$ for a prime p, which is clear.

Proof of Theorem 3.1.1. By the formula (2.2.1) in Theorem 2.2.9, for an odd prime p, $(a,b)_p = 1$ when both a and b have p-adic valuation 0. But given two non-zero rational numbers a and b, there are only finitely many odd primes p for which the p-adic valuation of a or b is nonzero. Adding the two places 2 and ∞, there are still only finitely many places v where $(a,b)_v \neq 1$. This shows the finiteness.

To see the product formula (3.1.1), we recall that Theorem 2.2.9 says that the Hilbert symbol is symmetric and bilinear in both variables. So it is enough to check (3.1.1) for the following list of cases (excluding the cases when a or b is 1 because that's when $(a,b)_v = 1$ for all v)

- $a = b = -1$. In this case $(a,b)_\infty = -1$ and $(a,b)_2 = (-1)^{\frac{(-1-1)(-1-1)}{4}} = -1$. So (2.2.1) holds.
- $(a,b) = (-1,p)$ for p an odd prime. $(-1,p)_p = \left(\frac{-1}{p}\right)$ and $(-1,p)_2 = (-1)^{(-1-1)(p-1)/4} = (-1)^{(p-1)/2}$. They multiply to 1.
- $(a,b) = (p,p)$ for an odd prime p. $(p,p)_p = (-1)^{(p-1)/2}$ and $(p,p)_2 = (-1)^{(p-1)^2/4}$. They also multiply to 1.
- $(a,b) = (p,\ell)$ for two odd distinct primes p and ℓ. This is the interesting case.

  $$(p,\ell)_p = \left(\frac{\ell}{p}\right), \quad (p,\ell)_\ell = \left(\frac{p}{\ell}\right), \quad \text{and} \quad (p,\ell)_2 = (-1)^{(p-1)(\ell-1)/2}.$$

  The product formula (2.2.1) in this case is equivalent to the equality

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

  This is precisely the quadratic reciprocity! (So to some extent, the product formula for Hilbert symbols is equivalent to Gauss's quadratic reciprocity.)
- Cases involving the prime number 2 is left as exercises.

□

3.2. **Globalizing local quaternion.** We verify (2). This is a combinatorial problem of creating a pair of numbers a and b.

Lemma 3.2.1. *For any given even subset Σ of places of $\mathbb{Q}$, there exists a quaternion algebra D_Σ which is ramified exactly at Σ.*

Proof. We will handle the case when $\infty \notin \Sigma$, and we leave it as an exercise for the readers to deal with the case when $\infty \in \Sigma$ (which requires a little modification). Let $p_1, \dots, p_r$ be the odd primes that are contained in Σ. We shall define a quaternion algebra $D = D_{\mathbb{Q},N,Q}$ where

- Q is a (huge) prime number such that $Q \bmod p$ is not a square and $Q \equiv 3 \pmod 4$ (the existence of such Q is guaranteed by the Dirichlet's theorem on primes in arithmetic progression Theorem 3.2.2).
- $N = \epsilon p_1 \cdots p_r$, where $\epsilon \in \{\pm 1\}$ is a sign determined by the following table.

ϵ	$2 \in \Sigma$	$2 \notin \Sigma$
$p_1 \cdots p_r \equiv 1 \pmod 4$	-1	1
$p_1 \cdots p_r \equiv 3 \pmod 4$	1	-1

We now check that, this quaternion algebra D ramifies exactly at Σ.

- The place ∞: since Q is positive, D splits at ∞.
- For a prime $\ell \nmid 2p_1 \cdots p_r Q$, we have $N, Q \in \mathbb{Z}_\ell^\times$. By Theorem 2.2.9, D splits at ℓ.
- At $p = p_i$, $p_i || N$ and $Q \bmod p_i$ is not a square, so D is ramified at p_i.
- At the place 2, our complicated choice of ϵ is designed so that $D_{N,Q}$ is ramified at 2 if $2 \in \Sigma$ and splits at 2 if $2 \notin \Sigma$, by Theorem 2.2.9.

It is not so easy to directly determine the ramification of D at Q, so at this point, we can conclude that the set of ramified places of D is either Σ or $\Sigma \cup \{Q\}$. But we know that the set of ramified places of D always have even cardinality. So it must be equal to Σ. □

Theorem 3.2.2. *Let $a, b \in \mathbb{N}$ be two coprime integers. Then in the arithmetic progression $\{a + bn\}_{n \in \mathbb{N}}$ there are infinitely prime numbers.*

3.3. **Hasse–Minkowski theorem for quadratic forms.** We are now left with proving Theorem 3.0.2(3), namely, if D and D' are two quaternion algebras over $\mathbb{Q}$ such that $D \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong D \otimes_{\mathbb{Q}} \mathbb{Q}_v$ for all places v of $\mathbb{Q}$, then $D \cong D'$.

We will only prove this when $D' = \mathrm{M}_2(\mathbb{Q})$, namely, if a quaternion algebra D over $\mathbb{Q}$ is isomorphic to the matrix algebra over each $\mathbb{Q}_v$, then it is isomorphic to the matrix algebra over $\mathbb{Q}$. The general case uses a more involved argument.

Recall that the quaternion algebra $D_{k,a,b}$ is isomorphic to isomorphic to $\mathrm{M}_2(k)$ if and only if b is a norm from $k(\sqrt{a})$, which is further equivalent to existing $x, y \in k$ such that $b = x^2 - ay^2$. Thinking of x and y as "rational numbers" represented by x/z and y/z, The latter statement is equivalent to having nonzero solutions $(x, y, z) \in k^3 \backslash \{(0, 0, 0)\}$ such that $bz^2 = x^2 - ay^2$.

So we arrive at the following.

Lemma 3.3.1. *The quaternion algebra $D_{k,a,b}$ is isomorphic to $\mathrm{M}_2(k)$ if and only if $x^2 = ay^2 + bz^2$ has nonzero solutions $(x, y, z) \in k^3 - \{(0, 0, 0)\}$.*

So we are left to prove that, for $a, b \in \mathbb{Q}^\times$, the equation $x^2 = ay^2 + bz^2$ has nonzero solutions in $\mathbb{Q}$ if and only if it has nonzero solutions in $\mathbb{Q}_v$ for all places v of $\mathbb{Q}$. This is true in a much more general setup.

Theorem 3.3.2 (Hasse-Minkowski)**.** *Consider a $\mathbb{Q}$-coefficient quadratic form*

$$Q(x_1, \ldots, x_n) = \sum_{i \le j} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{Q}.$$

It has non-zero solution in $\mathbb{Q}$ if and only if it has non-zero solution in $\mathbb{Q}_v$ for any places v of $\mathbb{Q}$.

Proof. We will not prove this deep theorem here, but we will include a proof in the case when the quadratic form is $Q(x, y, z) = x^2 - ay^2 - bz^2$ (which was due to Legendre). The necessity is clear, so we will prove sufficiency, namely, assuming that $Q(x, y, z)$ has non-zero solutions in $\mathbb{Q}_v$ for every place v of $\mathbb{Q}$, we want to show that $Q(x, y, z)$ has non-zero solutions in $\mathbb{Q}$.

We may assume $|a| \le |b|$ and both a and b are square-free integers. We run induction on the size of $|a| + |b|$. When $|a| + |b| = 2$, or equivalently, $|a| = |b| = 1$, this can be easily checked case by case (exercise).

We now assume that $|a| + |b| > 2$ so that $|b| \ge 2$. Write

$$b = \pm p_1 \cdots p_r.$$

For $p = p_i$, we claim that a is a square modulo p. Indeed, we look at the solution $x^2 - ay^2 - bz^2 = 0$ in $\mathbb{Q}_p$. This follows from the same argument of Theorem 2.2.9 Case $\alpha = 1$ and $\beta = 0$.

Since $\mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r\mathbb{Z}$, we see that a is a square modulo b, i.e. there exists $b' \in \mathbb{Z}$ such that

$$bb' = t^2 - a$$

We may choose t so that $|t| \le \frac{b}{2}$ and thus $|b'| < |b|$. The key here is that bb' is a norm from $\mathbb{Q}(\sqrt{a})$, namely the norm of $t + \sqrt{a} \in \mathbb{Q}(\sqrt{a})$. So in particular, b is a norm from $\mathbb{Q}(\sqrt{a})$ if and only if b' is a norm from $\mathbb{Q}(\sqrt{a})$. Using Proposition 2.2.2, we know that $z^2 - ax^2 - by^2 = 0$ has nonzero solutions if and only if b is a norm from $\mathbb{Q}(\sqrt{a})$, which is further equivalent to b' being a norm from $\mathbb{Q}(\sqrt{a})$, which in turn is equivalent to $z^2 - ax^2 - b'y^2 = 0$ having nonzero solutions.

So the statement for (a, b) is reduced to the statement for (a, b'), which is know due to our inductive proof (and that $|b'| < |b|$). This completes the proof. $\square$

3.4. **Exercises.**

Exercise 3.4.1. When $a \neq -b \in k^\times$, show that the following map $\varphi : D_{k,a,b} \to D_{k,a+b,-ab}$ is an isomorphism

$$\varphi(\mathbf{i}) = \mathbf{i}' + \mathbf{j}' \quad \text{and} \quad \varphi(\mathbf{j}) = \mathbf{k}'.$$

For example, we deduce $D_{\mathbb{Q},2,3} \cong D_{\mathbb{Q},5,-6}$ this way. Can you prove that these two quaternions are isomorphic using Theorem 3.0.2? What is the corresponding set of ramified places?

Exercise 3.4.2. Complete the proof of Lemma 3.2.1 in the case when $\infty \in D$.

Exercise 3.4.3. We explain that the quaternion algebra $D_{\mathbb{Q},a,b}$ contains lots of quadratic extensions over $\mathbb{Q}$. Check that

$$(x\mathbf{i} + y\mathbf{j} + z\mathbf{k})^2 = ax^2 + by^2 - abz^2.$$

So in particular $D_{\mathbb{Q},a,b}$ contains $\mathbb{Q}(\sqrt{ax^2 + by^2 - abz^2})$ for any $x, y, z \in \mathbb{Q}$. (These fields all embed in $D_{\mathbb{Q},a,b}$ but they do not commute with each other; so their non-trivial composites cannot be embedded in D; so there is no contradiction on dimensions.)

Of course, it seems to be possible that $ax^2 + by^2 - abz^2$ is a square for some particular choices of x, y, z. But show that, if this happens for $(x, y, z) \neq (0, 0, 0)$, D is isomorphic to $\mathrm{M}_2(\mathbb{Q})$.

Exercise 3.4.4. In this exercise, we study more systematically when the quaternion algebra $D_{\mathbb{Q},a,b}$ contains a quadratic extension $\mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$. For this, we may assume that D is a square-free integer.

In particular, a real quadratic field $\mathbb{Q}(\sqrt{D})$ (i.e. $D > 0$) *cannot* be embedded into a definite quaternion algebra.

Exercise 3.4.5. Recall that in algebraic number theory, for a finite extension K of $\mathbb{Q}$, we write $\mathcal{O}_K$ for the ring of integers, consisting of elements that are "integral" over $\mathbb{Z}$, namely,

$$\mathcal{O}_K := \big\{\alpha \in K \;\big|\; \alpha \text{ is a zero of some monic polynomial } x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]\big\}.$$

We can make an analogous definition for a quaternion algebra $D = D_{\mathbb{Q},a,b}$ over $\mathbb{Q}$. Note that an element $q \in D$ always satisfies a *quadratic* equation

$$q^2 - \mathrm{tr}(q) \cdot q + \mathrm{Nm}(q) = 0,$$

for the trace and norm (which belong to $\mathbb{Q}$) defined in 1.1.3. So explicitly, we can define the *ring of integers* in D to be

$$\mathcal{O}_D := \big\{q \in D \;\big|\; \mathrm{tr}(q), \mathrm{Nm}(q) \in \mathbb{Z}\big\}.$$

Show that the ring of integers of $D_{\mathbb{Q},-1,-1}$ is

$$\mathcal{O}_{D_{\mathbb{Q},-1,-1}} = \mathbb{Z} \oplus \mathbb{Z}\mathbf{i} \oplus \mathbb{Z}\mathbf{j} \oplus \mathbb{Z}\tfrac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}.$$

Exercise 3.4.6. If a quaternion algebra D over $\mathbb{Q}$ contains a quadratic field L, show that $\mathcal{O}_L \subseteq \mathcal{O}_D$. Conversely, show that all the elements of $\mathcal{O}_D$ is contained in $\mathcal{O}_L$ for some quadratic field L embedded in D. Moreover, all the units $\mathcal{O}_D^\times$ are units in some $\mathcal{O}_L^\times$. (This almost follows from the previous sentence; what is missing?)

Exercise 3.4.7. Let D be a quaternion algebra over $\mathbb{Q}$.

(1) Show that an element $q \in \mathcal{O}_D$ is a unit if and only if $\mathrm{Nm}(q) = \pm 1$.

(2) Find all the units in $\mathcal{O}_{D_{\mathbb{Q},-1,-1}}$. What is this group isomorphic to?
(3) Show that $\mathcal{O}_D$ has only finitely many units if D is a definite quaternion, namely, $D \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to the Hamiltonian quaternion.
(4) Show that if D is an indefinite quaternion algebra, $\mathcal{O}_D$ has infinitely many units. (Hint: use Exercise 3.4.4.)

4. Day IV: Central Simple algebras

4.1. **Central Simple Algebras and Brauer Groups.** Central simple algebras are higher dimensional generalizations of quaternion algebras.

Definition 4.1.1. Let K be a field. A *central simple algebra* over K is a matrix algebra $M_n(D)$ for some $n \in \mathbb{N}$ and some division ring D whose center is exactly K. (This is actually an equivalent working definition; the common definition is a K-algebra C whose center is exactly K, and such that all finitely generated C-modules are isomorphic to a (finite) direct sum of a unique simple C-module.) When $n = 1$, we call D a *division central algebra* over K.

Example 4.1.2. When $K = \mathbb{R}$, all central simple algebras over $\mathbb{R}$ are $\mathrm{M}_n(\mathbb{R})$ and $\mathrm{M}_n(\mathbb{H})$.

Example 4.1.3. All quaternion algebras over K are central simple algebras.

Let L/K be a Galois extension whose Galois group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator and choose $b \in K^\times$. We define a central simple algebra

$$(L/K, \sigma, b) := L \oplus Lx \oplus Lx^2 \oplus \cdots \oplus Lx^{n-1},$$

where the multiplication is K-linear but subject to the following rules:

$$x\alpha = \sigma(\alpha)x, \quad \text{for all } \alpha \in K.$$

These central simple algebras are called *cyclic algebras*, and they have dimension n^2. In this sense, $\mathbb{H} = (\mathbb{C}/\mathbb{R}, -1)$.

Fact 4.1.4. For a division central simple algebra D over F and any (not necessarily finite) field extension L/K, the tensor product $D \otimes_K L$ is a central simple algebra over L.

Moreover, there exists a finite (separable) field extension L/K, such that $D \otimes_K L \cong \mathrm{M}_n(L)$. In particular, $\dim_K D = n^2$ is a square.

Fact 4.1.5. For central simple algebras $C = \mathrm{M}_n(D)$ and $\mathrm{M}_{n'}(D')$ over K, their tensor product $C \otimes_K C' = \mathrm{M}_{nn'}(D \otimes_K D')$ is also a central simple algebra over K. In particular, $D \otimes_K D'$ is again a central simple algebra over K, namely a matrix algebra in some (other) division algebra over K.

Example 4.1.6. For a division algebra D, we can define an *opposite division algebra* $(D^{\mathrm{op}}, *)$ such that $d_1 * d_2 := d_2 \cdot d_1$. (For quaternion algebras $D_{k,a,b}$, it is isomorphic to its opposite $D^{\mathrm{op}}_{k,a,b}$.) We can consider the action of $D \otimes_K D^{\mathrm{op}}$ on D by

$$(d_1, d_2) \cdot d := d_1 d d_2.$$

This action is K-linear but not D-linear. So we get a ring homomorphism

$$D \otimes_K D^{\mathrm{op}} \longrightarrow \mathrm{End}_K(D) \cong \mathrm{M}_{\dim D}(K).$$

In fact, this is an isomorphism.

Definition 4.1.7. The *Brauer group* of the field K is defined to be

$$\mathrm{Br}(K) := \big\{C \text{ central simple algebras over } K\big\}/\sim,$$

where $C \sim C'$ if (and only if) there exists natural numbers $n, m \in \mathbb{N}$ such that $\mathrm{M}_n(C) \cong \mathrm{M}_m(C')$. (This is equivalent to $C \cong \mathrm{M}_m(D)$ and $C' \cong \mathrm{M}_n(D)$ for some division central algebra over K.) In some sense, we are picking out the "essential part" of the central simple

algebra, namely the "core" division central algebra, but ignoring the added matrix algebra structure. We use $[C]$ to denote the equivalent classes of central simple algebras.

The identity of the group $\mathrm{Br}(K)$ is $[K]$. The multiplication in $\mathrm{Br}(K)$ is defined to be the algebra tensor product:

$$[C] \cdot [C'] := [C \otimes_K C'].$$

The inverse of $[C]$ is $[C^{\mathrm{op}}]$. Note that, by Fact 4.1.6, for a division central algebra D, $D \otimes_K D^{\mathrm{op}} \cong \mathrm{M}_{\dim_K D}(K) \sim K$.

Remark 4.1.8. An equivalent definition of $\mathrm{Br}(K)$ is

$$\mathrm{Br}(K) := \big\{\text{division central algebras } D \text{ over } F\big\},$$

and the multiplication is given by the tensor product and then "deprive" the matrix algebra part of the tensor product.

Example 4.1.9. For $K = \mathbb{R}$, the only division central algebras over $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{H}$, and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{M}_4(\mathbb{R})$. So $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Note that $\mathbb{C}$ is not a central simple algebra over $\mathbb{R}$ because the center of $\mathbb{C}$ is not $\mathbb{R}$.

Example 4.1.10. Assume that the characteristic of K is not 2. For any quaternion algebra D over a field K, $D \cong D^{\mathrm{op}}$ (Exercise 4.4.1). So $[D] \cdot [D] = [\mathrm{M}_4(K)] = [K]$. This means that $[D]$ has order 2 in $\mathrm{Br}(K)$ (if it is not the matrix algebra).

Conversely, one can show that each element $[C] \in \mathrm{Br}(K)$ of order 2 can be represented by a quaternion algebra D.

4.1.11. *Interpretation of Theorem 3.0.2.* Using Example 4.1.10, we can make (3.0.1) precise:

$$\Phi_2 : \mathrm{Br}(\mathbb{Q})[2\text{-tor}] \longrightarrow \bigoplus_{v \text{ place of } \mathbb{Q}} \mathrm{Br}(\mathbb{Q}_v)[2\text{-tor}],$$

where [2-tor] means the subset of elements of order 1 or 2. The source of the map Φ_2 is the set of (isomorphism classes of) quaternion algebras over $\mathbb{Q}$, and the target of the map Φ_2 is the set of collections $(D_v)_v$ of quaternion algebras for each place v of $\mathbb{Q}$. Theorem 3.0.2 says that the map Φ_2 is injective, and its image is, if we identify each $\mathrm{Br}(\mathbb{Q}_v)[2\text{-tor}]$ with $\mathbb{Z}/2\mathbb{Z}$, the collection $(\alpha_v)_v$ of elements $\alpha_v \in \mathbb{Z}/2\mathbb{Z}$ such that $\alpha_v = 0$ for all but finitely many v, and $\sum_v \alpha_v \equiv 0 \bmod 2$.

Phrasing this in another way, we consider a map

$$\bigoplus_{v \text{ place of } \mathbb{Q}} \mathrm{Br}(\mathbb{Q}_v)[2\text{-tor}] \xrightarrow{\text{inv}} \mathbb{Z}/2\mathbb{Z}$$

sending $[D_v]$ for any v to 0 if $[D_v]$ is the identity element of $\mathrm{Br}(\mathbb{Q}_v)[2\text{-tor}]$, and to 1 if $[D_v]$ is the non-trivial element of $\mathrm{Br}(\mathbb{Q}_v)[2\text{-tor}]$. Then Theorem 3.0.2 says that Φ_2 defines an isomorphism from $\mathrm{Br}(\mathbb{Q})[2\text{-tor}]$ to the kernel of the map inv.

4.2. **Classification of Central Simple Algebras over $\mathbb{Q}$.** This classification is yet another instance of the local-global principal.

Over $\mathbb{R}$: We have seen that $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$. For what follows, it is easier to identify $\mathrm{Br}(\mathbb{R})$ with $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ (as opposed to $\mathbb{Z}/2\mathbb{Z}$). We write this in the form of a map $\mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \xrightarrow{\cong} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

Over $\mathbb{Q}_p$: for p a prime number, there is a canonical isomorphism

$$\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z} = \bigcup_n \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

In particular, every element of $\mathrm{Br}(\mathbb{Q}_p)$ is torsion (meaning that if C is a central simple algebra over $\mathbb{Q}_p$, then $\underbrace{C \otimes_{\mathbb{Q}_p} \cdots \otimes_{\mathbb{Q}_p} C}_{n \text{ times}}$ is a matrix algebra for some n.

Explicitly, each coset element of the coset $\mathbb{Q}/\mathbb{Z}$ is represented by $\frac{a}{n}$ for $(a,n) = 1$ and $a \in \{0, \ldots, n-1\}$. The division algebra $D_{a/n}$ with invariant $\frac{a}{n}$ can be constructed as follows. Pick a degree n monic irreducible polynomial $\bar{f}(x) \in \mathbb{F}_p[x]$ so that adjoining one zero $\bar{\alpha}$ of $\bar{f}(x)$ to $\mathbb{F}_p$ defines a degree n extension of $\mathbb{F}_p$. The Galois group $\mathrm{Gal}(\mathbb{F}_p(\bar{\alpha})/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ admits a canonical generator: the Frobenius σ, which sends $\bar{\alpha}$ to $\bar{\alpha}^p$.

Pick any lift $f(x)$ of $\bar{f}(x)$ into a monic polynomial in $\mathbb{Z}_p[x]$ (of degree n). Then adjoining one zero α of $f(x)$ to $\mathbb{Q}_p$ will define a degree n extension L of $\mathbb{Q}_p$. In fact one can prove that this extension $L/\mathbb{Q}_p$ is Galois whose Galois group $\mathbb{Z}/n\mathbb{Z}$, canonically isomorphic to the Galois group $\mathrm{Gal}(\mathbb{F}_p(\bar{\alpha})/\mathbb{F}_p)$ by looking at the action of the Galois group on α modulo p. In this sense, we may extend the Frobenius σ on $\mathrm{Gal}(\mathbb{F}_p(\bar{\alpha})/\mathbb{F}_p)$ to an element of the Galois group $\mathrm{Gal}(L/\mathbb{Q}_p)$.

Then we can write explicitly

$$D_{a/n} := L\langle t \rangle \big/ \big(t^n - p^a,\ tbt^{-1} - \sigma(b) \text{ for all } b \in L\big).$$

This is a central simple algebra over $\mathbb{Q}_p$ which has dimension n over L and hence dimension n^2 over $\mathbb{Q}_p$.

Over $\mathbb{Q}$: The description of the Brauer group over $\mathbb{Q}$ uses the same technique that we used to classify the quaternion algebras. For each central simple algebra C over $\mathbb{Q}$, we can base change to $\mathbb{Q}_p$ to get a central simple algebra $C \otimes_{\mathbb{Q}} \mathbb{Q}_p$ over $\mathbb{Q}_p$. This defines a homomorphism

$$\begin{aligned} \Phi : \mathrm{Br}(\mathbb{Q}) &\longrightarrow \textstyle\prod_{v \text{ places of } \mathbb{Q}} \mathrm{Br}(\mathbb{Q}_v). \\ C &\longmapsto \big(C \otimes_{\mathbb{Q}} \mathbb{Q}_v\big)_v \end{aligned}$$

In fact the image of this map lands in the direct sum $\bigoplus_{v \text{ places of } \mathbb{Q}} \mathrm{Br}(\mathbb{Q}_v)$. (How much do they differ?)

Theorem 4.2.1. *The map Φ is injective and its image is precise the kernel of the following map*

$$\sum_v \mathrm{inv}_v : \bigoplus_{v \textit{ places of } \mathbb{Q}} \mathrm{Br}(\mathbb{Q}_v) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Using the fancy language of exact sequences, we have

$$0 \to \mathrm{Br}(\mathbb{Q}) \longrightarrow \bigoplus_{v \text{ places of } \mathbb{Q}} \mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0$$

4.3. **Failure of Local-global Principle and Tate–Shafarevich Group.** In fact, the local-global principle we advocate often fail beyond the cases we discussed here. But whenever it holds, it will have great influence and many applications in number theory. Or rather, understanding the local-global principle is probably the most effective way we have so far to attack an arithmetic and number theory questions over $\mathbb{Q}$.

Here is a classical example where the local-global principal fails.

Theorem 4.3.1 (Selmer)**.** *The equation* $3x^3 + 4y^3 + 5z^3 = 0$ *has only the zero solution over* $\mathbb{Q}$*, but there is a nonzero solution over every completion* $\mathbb{Q}_v$*.*

4.4. **Exercises.**

Exercise 4.4.1. For quaternion algebras $D_{k,a,b}$, it is isomorphic to its opposite $D_{k,a,b}^{\mathrm{op}}$.

Exercise 4.4.2. Suppose that K has a primitive nth roots of unity ζ_n, we can define a central simple algebra $\left(\frac{a,b}{K}\right)_n$ for $a, b \in K^\times$ given by

$$\left(\frac{a,b}{K}\right)_n = K\langle \mathbf{i}, \mathbf{j}\rangle \big/ \left(\mathbf{i}^n - a, \mathbf{j}^n - b, \mathbf{ij} - \zeta_n \mathbf{ji}\right).$$

Suppose that $K(\sqrt[n]{a})$ is a degree n extension of K, then it is cyclic of degree n (why?). Show that this central simple algebra is the same as a cyclic algebra as defined in Example 4.1.3.

Exercise 4.4.3. The definition of the quaternion algebra $D_{a/n}$ in Subsection 4.2 makes sense. Check that $D_{a/n} \cong D_{a+n/n}$ and $D_{a/n}^{\mathrm{op}} \cong D_{-a/n}$.

Exercise 4.4.4. In this exercise, we outline a complete proof of Selmer's example (Theorem 4.3.1). The goal is to prove that

$$3x^3 + 4y^3 + 5z^3 = 0 \tag{4.4.1}$$

has only the zero solution over $\mathbb{Q}$, but there is a nonzero solution over every completion $\mathbb{Q}_v$. This requires the basic knowledge of algebraic number theory.

Existence of solutions over each $\mathbb{Q}_p$ is essentially a Hensel type argument, which we follow the method suggested by K. Buzzard.

(1) Show that there exist non-zero solutions to (4.4.1) over $\mathbb{R}$.
(2) For $p = 3, 5$, show that there exist non-zero solutions to (4.4.1) over $\mathbb{Q}_p$.
(3) For $p \neq 3, 5$, show that there exist non-zero solutions to (4.4.1) over $\mathbb{Q}_p$.
(4) Show that there exists only zero solution to (4.4.1) over $\mathbb{Q}$. Here is a list of steps:
   (a) First changing the variables to turn (4.4.1) into $X^3 + 6Y^3 = 10Z^3$.
   (b) Consider $\alpha = \sqrt[3]{6}$ and $K = \mathbb{Q}(\sqrt{6})$, so that the above equation becomes
   $$(X + \alpha Y)(X^2 - \alpha XY + \alpha^2 Y) = 10Z^3$$
   (c) Prove that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
   (d) Prove that $\mathbb{Z}[\alpha]$ is a PID.
   (e) The quotient $\mathbb{Z}[\alpha]^\times/(\mathbb{Z}[\alpha]^\times)^3$ is represented by $(1 - 6\alpha + 3\alpha^2)^k$ for $k = 0, 1, 2$. (Remark: it is true that $\mathbb{Z}[\alpha]^\times = \pm(1 - 6\alpha + 3\alpha^2)^{\mathbb{Z}}$, but this takes more time to prove.)
   (f) Conclude that (4.4.1) has no non-zero solution over $\mathbb{Q}$.