\[ R^n > \Gamma = \text{lattice} \]

Last time we have defined \( \text{vol}(R^n/\Gamma) \)

Lemma 1. Let \( \Gamma_1, \Gamma_2 \subset R^n \) be lattices such that \( \Gamma_2 \subset \Gamma_1 \). Then

\[ \text{vol}(R^n/\Gamma_2) = \text{vol}(R^n/\Gamma_1) \cdot [\Gamma_1 : \Gamma_2] \]

a fortiori, the index \([\Gamma_1 : \Gamma_2]\) is finite.

Proof: Let \( F_1 \) be a fundamental set for \( \Gamma_1 \). Let \( S \) be a set of representatives for the cosets of \( \Gamma_2 \) in \( \Gamma_1 \), i.e.,

\[ \Gamma_1 = \bigsqcup_{s \in S} (s + \Gamma_2). \]

It is straightforward to check that

\[ F_2 := \bigsqcup_{s \in S} (s + F_1) \]

is a fundamental set for \( \Gamma_2 \), from which the lemma follows, straight off.

\[ \square \]
Lemma 2. Consider a lattice $\Gamma \subseteq \mathbb{R}^n$ and an element $T \in GL_n (\mathbb{R})$ such that $T(\Gamma) \subseteq \Gamma$. Then $|\det T| = [\Gamma : T\Gamma]$. (Easy exercise)

§3.2. Let us recall the first form of Dirichlet's unit theorem:

**Thm:** $L = $ finite field extension of $\mathbb{Q}$ of degree $\nu \in \mathbb{N}$

$L \otimes \mathbb{Q} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ \hspace{1cm} ($r_1 + 2r_2 = \nu$)

If $A \subset L$ is an order, then

$A^* \cong$ (finite cyclic group) $\times \mathbb{Z}^{r_1 + r_2 - 1}$

§3.3. Last time we proved a different form of this theorem:

**Thm:** With the notation of §3.2, the quotient group $L^+/A^*$ is compact.

§3.4. Second form $\Rightarrow$ First form.

$L \otimes \mathbb{Q} R = L_{\mathbb{Q}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

We have Norm: $L \otimes \mathbb{Q} R \rightarrow \mathbb{R}$. 
Explicitly:

\[ c = (x_1, \ldots, x_n, z_1, \ldots, z_{r_2}) \in \mathbb{R}^n \times \mathbb{C}^{r_2} \]

\[ \Rightarrow \det(c) = \text{norm}(c) = |x_1 \cdots x_n| |z_1|^2 \cdots |z_{r_2}|^2. \]

Now \[ L^1_{\mathbb{R}} = \left\{ c \in (L^0 \mathbb{R})^* \mid |\text{norm}(c)| = 1 \right\} \]

This is a topological group. Let us describe it more explicitly.

\[ \mathbb{R}^\times \cong \{ \pm 1 \} \times \mathbb{R} \quad \text{via} \quad x \mapsto \left( \frac{x}{|x|}, \log |x| \right) \]

and

\[ \mathbb{C}^\times \cong S^1 \times \mathbb{R} \quad \text{via} \quad z \mapsto \left( \frac{z}{|z|}, 2 \log |z| \right) \]

Consider the homomorphism

\[ L^\times_{\mathbb{R}} \cong \{ \pm 1 \}^n \times (S^1)^{r_2} \times \mathbb{R}^{n_1 + r_2} \rightarrow \mathbb{R}^{n_1 + r_2} \]

\[ \text{projection} \]

\[ h \]

\[ \text{sum of all coordinates} \]

\[ \mathbb{R} \]

It is easy to see that

\[ L^1_{\mathbb{R}} = \ker(h) \]

\[ \left\{ c \in L^\times_{\mathbb{R}} \mid |\text{norm}(c)| = 1 \right\}. \]
If we write \( V = \left\{ (a_1, \ldots, a_r) \in \mathbb{R}^{r_1+r_2} \mid a_1 + \cdots + a_r = 0 \right\} \),

then we see that

\[ L^1_{\mathbb{R}} \cong K \times V, \quad \text{where} \quad K = \left\{ \pm 1 \right\}^{r_1} \times (S^1)^{r_2} \]

\[ \mathsection{3.6.} \text{Lemma.} \quad \text{Let} \ G \ \text{be a locally compact Hausdorff topological group, let} \ K \ \text{be a compact Hausdorff topological group, and let} \ \Gamma \subset K \times G \ \text{be a discrete subgroup such that} \ \frac{K \times G}{\Gamma} \ \text{is compact.} \]

\[ \text{If} \ \pi_2 : K \times G \to G \ \text{is the natural projection, then} \ \pi_2(\Gamma) \ \text{is discrete in} \ G, \ \text{and} \ \frac{G}{\pi_2(\Gamma)} \ \text{is compact.} \quad \text{(Proof: exercise.)} \]

\[ \mathsection{3.7.} \quad \text{Now we are done. Indeed,} \ A^* \subset L^1_{\mathbb{R}} \]

is a discrete subgroup, and \( L^1_{\mathbb{R}} / A^* \) is compact. By Lemma 3.6, the image of \( A^* \) in \( V \) is discrete and co-compact.

Thus we get an exact sequence

\[ 0 \to K \cap A^* \to A^* \to \pi_2(A^*) \to 0, \]

where \( \pi_2(A^*) \) is a lattice in \( V \). Thus \( \pi_2(A^*) \) is a free abelian group of rank \( r_1+r_2-1 \). On the other hand, \( K \cap A^* \) is discrete and compact \( \implies \) finite \( \implies \) cyclic, because \( A^* \subset L^1_{\mathbb{R}}. \)
Example. \( p = \text{an odd prime} \)

\( \zeta = \text{a primitive } p\text{-th root of unity in } \mathbb{Q} \)

\( L = \mathbb{Q}(\zeta), \quad A = \mathbb{Z}[\zeta] \) (clearly an order).

It is clear that \( L \) has no real embeddings, so \( L \otimes \mathbb{R} \cong \mathbb{C}^{\frac{p-1}{2}} \). Hence, by the Dirichlet Unit Theorem, \( \frac{p-1}{2} - 1 \)

\[ \{\text{units in } A\} \cong M_p \cong \mathbb{Z}^{\frac{p-1}{2}} \times \mathbb{Z} \]

We will find a subgroup of finite index in \( A^\times \).

For \( 2 \leq a \leq p-1 \), consider

\[ \lambda_a = \frac{\zeta^{a-1}}{\zeta - 1} = 1 + \zeta + \ldots + \zeta^{a-1} \in A \]

Now let \( b \in \mathbb{N} \) and write

\[ \frac{\zeta^{ab} - 1}{\zeta^a - 1} = 1 + \zeta^a + \ldots + \zeta^{a(b-1)} \in A \]

If we choose \( b \) so that \( ab \equiv 1 \pmod{p} \), then we see that \( \frac{1}{\lambda_a} \in A^\times \), i.e., \( \lambda_a \in A^\times \).

So we have produced \( p-2 \) units in \( A \).

Of course, there non-trivial relations between them.
For instance, it is easy to check that \((x/a/x-a)^2 = 1\), because

\[
\frac{x^a - 1}{x - 1} = -x^a \frac{x^a - 1}{x - 1}.
\]

**Fact:** The subgroup of \(A^x\) generated by

\[
\frac{x^2 - 1}{x - 1}, \frac{x^3 - 1}{x - 1}, \ldots, \frac{x^{p/2} - 1}{x - 1}
\]

has rank \(\frac{p-1}{2} - 1\), and therefore has finite index in \(A^x\).

**Remark:** Apparently, the only known proof of this elementary statement that works for all odd primes \(p\) uses the theory of \(L\)-series.

\[\square\]

§3.9. **Noncommutative examples**

\[H = R \oplus Ri \oplus Rj \oplus Rk\]

associative division algebra over \(R\)

\[i^2 = j^2 = k^2 = -1\]

\[ij = k = -1\]

We are interested in generalizations of this, called quaternion algebras.
Definition. Let $F$ be any field of characteristic $\neq 2$, and fix $a, b \in F^*$. Consider the $4$-dimensional $F$-algebra

$$D = \langle a, b \rangle_F = F \oplus F \cdot i \oplus F \cdot j \oplus F \cdot k$$

in which the multiplication is determined by

$$i^2 = a, \quad j^2 = b, \quad ij = k = -ji$$

($\Rightarrow k^2 = -ab$).

Usually one writes: $D_{a,b} = \langle a, b \rangle_F$.

83.10. Theorem. (1) Either $\langle a, b \rangle_F \cong M_2(F)$ as an $F$-algebra, or $\langle a, b \rangle_F$ is a division ring.
(2) $\langle a, b \rangle_F$ is a division ring if and only if the quadratic form $x^2 - ay^2 - bz^2 + abw^2$ in the four variables $x, y, z, w$ does not represent $0$ over $F$; i.e., $(x, y, z, w) \neq (0, 0, 0, 0)$

$$\Rightarrow Q(x, y, z, w) := x^2 - ay^2 - bz^2 + abw^2 \neq 0.$$

(3) $\langle a, b \rangle_F$ is not a division ring $\iff$

- either $ae \in (F^*)^2$
- or $a \notin (F^*)^2$ and $b = \text{Norm}_{F}^{F(\sqrt{a})}$ for some $c \in F(\sqrt{a})^*$. 
Example. Take $F = \mathbb{Q}$. Choose $a, b \in \mathbb{Z}$ so that $\langle a, b \rangle_\mathbb{Q}$ is a division algebra and $\langle a, b \rangle_\mathbb{R} \cong M_2(\mathbb{R})$. Note that $A = \mathbb{Z} \oplus \mathbb{Z} i \oplus \mathbb{Z} j \oplus \mathbb{Z} k$ is an order in $\langle a, b \rangle_\mathbb{Q}$.

We put $D = \langle a, b \rangle_\mathbb{Q}$, so that $D_\mathbb{R} \cong M_2(\mathbb{R})$. One can show that $D_\mathbb{R}^+ = \{ g \in M_2(\mathbb{R}) \mid \det(g) = 1 \} \cong \text{SL}_2(\mathbb{R})$. The quotient $A^x \backslash \text{SL}_2(\mathbb{R})$ is compact, by the second form of Dirichlet's unit theorem.

$\text{PSL}_2(\mathbb{R})$ acts on $\mathbb{H} = \{ x + iy \mid y > 0 \}$ (open upper half-plane).

If $\Gamma \subset A^x$ is a torsion-free subgroup of finite index, then $\Gamma \backslash \mathbb{H}$ is a compact Riemann surface.

Moral: Quaternion algebras over $\mathbb{Q}$ give us a way of constructing discrete co-compact subgroups of $\text{SL}_2(\mathbb{R})$. 
§3.12. Sketch of the proof

of Theorem 3.10. Given \( x + y \mathbf{i} + z \mathbf{j} + w \mathbf{k} \in \langle a, b \rangle \), let us write \( \mathbf{I} = a - y \mathbf{i} - z \mathbf{j} - w \mathbf{k} \). Check that
\[
\mathbf{I} \in Q(x, y, z, w) \in F.
\]

Now if \( \langle a, b \rangle \) is a division ring, then \( \mathbf{I} \neq 0 \Rightarrow \mathbf{I} \neq 0 \).

The rest of the theorem will be proved simultaneously. Assume that there exists \( \mathbf{I} \in \langle a, b \rangle \setminus \{0\} \) with \( \mathbf{I} \mathbf{I} = 0 \), we wish to check, first of all, that
\[
\langle a, b \rangle \cong M_2(F).
\]

Write \( \mathbf{I} = x + y \mathbf{i} + z \mathbf{j} + w \mathbf{k} \).

We need to check the following things:

1. \( \mathbf{a} \in (\mathbf{F}^2)^2 \Rightarrow \langle a, b \rangle \cong M_2(F) \)
2. \( \mathbf{a} \notin (\mathbf{F}^2)^2 \) and \( b \in \text{Norm} (\mathbf{F}(\mathbf{a}^2)) \Rightarrow \langle a, b \rangle \cong M_2(F) \).

3. If \( Q \) represents zero over \( \mathbf{F} \), then one of the two possibilities mentioned above must be realized.
My comments.

Probably, one can prove the theorem without doing any complicated computations. First of all, a simple change of variables shows that if \( a \in (\mathbb{F}^*)^2 \), then \( \langle a, b \rangle_F \cong \langle 1, b \rangle_F \). Now, it is not hard to find an isomorphism \( \langle 1, b \rangle_F \cong M_2(F) \).

Next, \( \langle a, b \rangle_F \cong \langle a, b \rangle_{F \otimes F} \), and, of course, \( a \in (\mathbb{F}^*)^2 \), whence

\[ \langle a, b \rangle_{F \otimes F} \cong M_2(F) \]. Therefore \( \langle a, b \rangle_F \) is a central simple algebra over \( F \), and the rest is fairly straightforward.

(This is not the proof which was given during the lecture.)

\( \textbf{3.13.} \) Example. \( F = \mathbb{Q} \Rightarrow \) it is easy to check that \( \mathcal{D}_R \cong M_2(\mathbb{R}) \) iff \( a > 0 \) or \( b > 0 \) (use the theorem above). We want \( \langle a, b \rangle_{\mathbb{Q}} \neq M_2(\mathbb{Q}) \). Fix an odd prime \( p \) and let \( c \in \mathbb{Z} \) be such that \( c \) is not a square mod \( p \). Then you can take \( a = p, \ b = c \).