Noriʒs Lectures on Algebraic Number Theory

Lecture 2: 06/22/2007

Interesting book:
Weil, "History of Number Theory".

§2.1 Let D be a finite dimensional division algebra over $\mathbb{Q}$. Write $n = \dim_{\mathbb{Q}} D$.
Last time we proved the following:

If $M \subset D$ is an additive finitely generated subgroup containing a $\mathbb{Q}$-basis of D (i.e., is such that $\mathbb{Q} \otimes_{\mathbb{Z}} M \xrightarrow{\simeq} D$), then $\exists\, c \in \mathbb{N}$ so that $(cM)\cdot(cM) \subset cM$. Consequently, $A = \mathbb{Z} + mcM$ is an order in D $\forall m \in \mathbb{N}$.

~~Def:~~ ~~A (left) fractional ideal~~

§2.2. **Definition.** A (left) fractional ideal $I \subset D$ is a finitely generated left A-submodule of D. (Observe that if $I \subset D$ is a fractional ideal, then $\exists\, c \in \mathbb{N}$ such that $c \cdot I \subset A$, and hence $c \cdot I$ is a (left ideal of A.)

§2.3. Dirichlet's theorem. The set of nonzero left A-fractional ideals modulo right principal equivalence is finite.

This is what we proved last time.

§2.4. Motivation for the next result.

$$\mathbb{Q}^\times = \{\pm 1\} \times \bigoplus_{p=\text{prime}} \mathbb{Z}$$

($\{\pm 1\}$: units in $\mathbb{Z}$)

via $\bigoplus_p \mathbb{Z} \xrightarrow{\simeq} \mathbb{Q}^\times_{>0}$

$$(n_p)_{p=\text{prime}} \longmapsto \prod p^{n_p}$$

So even if we are only interested in fields K, in order to understand the structure of the unit group $K^\times$, we should try to find a suitable subring $A \subset K$ which has unique factorization and has K as its field of fractions, and then also analyze the structure of the group of units $A^\times$.

§2.5. Base change, $\otimes$ products, etc.

B = an algebra over a field F

Given a field extension $E \supset F$, we will write $B_E := E \underset{F}{\otimes} B$.

This is an E-algebra.

Example. Suppose $\mathbb{B} = L$ is a finite separable extension of F. What does L_E look like?

Since L is separable and finite over F, we can find an element $\Theta \in L$ with $L = F[\Theta]$. Let $f(X)$ be the minimal (monic) polynomial of Θ over F. Then we can identify $L \cong F[X]/(f(X))$, and therefore

$$L_E = E \otimes_F L \cong E[X]/(f(X)).$$

Of course, $f(X)$ need not remain irreducible over E. Let us factor

$$f(X) = f_1(X) f_2(X) \dots f_r(X)$$

where $f_j(X) \in E[X]$ are monic irreducible polynomials. Since $f(X)$ is separable, we see that the $f_j(X)$ are pairwise distinct and are separable over E.

By the Chinese Remainder Theorem,

$$E[X]/(f(X)) \xrightarrow{\cong} \prod_{j=1}^{n} E[X]/(f_j(X)),$$

and $L_j := E[X]/(f_j(X))$ is a finite separable extension of E.

§2.6. Let us apply these remarks to the following situation: $F = \mathbb{Q}$

L = finite (automatically separable) extension of $\mathbb{Q}$; write $n := [L : \mathbb{Q}]$

$E = \mathbb{R}$

Then we must have $L_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, with $r_1, r_2 \in \mathbb{Z}$, $r_1, r_2 \geq 0$, $n = r_1 + 2r_2$.

Now we can state

Dirichlet's unit theorem. Suppose A is an order in L. Then

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

this is necessarily the torsion of $A^\times$, i.e., the subgroup of $A^\times$ formed by the roots of unity in A

§2.7. Remark. Suppose instead we take a finite extension L of $\mathbb{F}_q(t)$. Write $R = \mathbb{F}_q[t]$. What should replace $\mathbb{R}$ in the story explained in §2.6?

(Note: we are replacing $\mathbb{Z}$ with the PID R, and $\mathbb{Q}$ with $K = \mathbb{F}_q(t)$, and looking at R-orders in L, with the notation of the first lecture.)

Now consider

$$\mathbb{F}_q(t) = \mathbb{F}_q(t^{-1}) \hookrightarrow \mathbb{F}_q((t^{-1}))$$

(formal Laurent series)

This is what replaces $\mathbb{R}$.

Analogue of Dirichlet's unit theorem.

L = finite separable extension of $\mathbb{F}_q(t)$

A = an $\mathbb{F}_q[t]$ - order in L

$E := \mathbb{F}_q((t^{-1}))$

Write $L_E \cong L_1 \times L_2 \times \dots \times L_r$,

where L_i is a field extension of E.

Then: $A^\times \cong$ (finite cyclic group) $\times \mathbb{Z}^{r-1}$.

§2.8. Let us go back to number fields $L \supset \mathbb{Q}$.

Already for $r_1 = 2$, $r_2 = 0$, it is rather nontrivial to show the existence of a unit $\neq \pm 1$. This was first proved by Lagrange, and has to do with Pell's equation:

$$a^2 - b^2 d = \pm 1 \qquad (*)$$

for a fixed $d \in \mathbb{N}$ with is not a square. Note that (a, b) is a solution of $(*)$ if and only if $a + b\sqrt{d}$ is a unit in $A = \mathbb{Z}[\sqrt{d}]$ (which is an order in $\mathbb{Q}(\sqrt{d})$)

(of course, we are assuming $a, b \in \mathbb{Z}$.)

Lagrange's theorem. Let $d \in \mathbb{N}$, d not a full square. Then there exists $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $(a, b) \neq (\pm 1, 0)$ so that $a^2 - b^2 d = 1$.

Now we will begin the proof of Dirichlet's unit theorem.

§2.9. Norms. Let B be an F-algebra such that $\dim_F(B) < \infty$. Given $b \in B$, let $r_b : B \longrightarrow B$ consider the F-linear map given by $x \longmapsto xb$.

Def: The norm of B (relative to F) is defined by $N_{B/F}(b) := \det(r_b)$

Properties. (i) $N_{B/F}(b_1 b_2) = N_{B/F}(b_1)\, N_{B/F}(b_2)$

(ii) As a function, $N_{B/F} : B \longrightarrow F$ is homogeneous of degree $n = \dim_F(B)$.

Remark: In general, if $l_b : B \longrightarrow B$ is given by $l_b(x) = bx$, it might happen that $\det(l_b) \neq \det(r_b)$ for some $b \in B$.

However, for division algebras, this unpleasantness does not occur.

Exercises. (1) see what happens for $B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in F \right\} \subset Mat_2(F)$.

(2) Let B be a finite dimensional division algebra over F. Given $\beta \in B$, let $f(X)$ be the minimal monic polynomial of β over F.

Let $r = \deg(f)$, and write

$$f(X) = X^r + a_1 X^{r-1} + \dots + a_r.$$

Show that $r \mid n$ and

$$\det(l_\beta) = \det(r_\beta) = \left((-1)^r \cdot a_r\right)^{\frac{n}{r}}.$$

§2.10. Lemma. Let D be a finite dimensional division algebra over $\mathbb{Q}$, and let $A \subset D$ be an order. Fix $a \in A$.

Then (i) $N_{D/\mathbb{Q}}(a) \in \mathbb{Z}$.

(ii) $a \in A^\times \iff N_{D/\mathbb{Q}}(a) = \pm 1$.

The proof is an easy exercise in linear algebra.

We are aiming towards:

Volumes, lattices ... Minkowski's lemma.

§2.11. Definition. A lattice in $\mathbb{R}^n$ is an additive subgroup $\Gamma \subset \mathbb{R}^n$ which is discrete (hence closed) and cocompact, i.e., $\mathbb{R}^n/\Gamma$ is compact with respect to the quotient topology.

Exercise. If $\Gamma \subset \mathbb{R}^n$ is a lattice, then there exists an $\mathbb{R}$-basis $w_1, \ldots, w_n$ of $\mathbb{R}^n$ such that

$$\Gamma = \mathbb{Z}w_1 \oplus \ldots \oplus \mathbb{Z}w_n.$$

§2.12. Let us fix a volume form, or the Lebesgue measure, etc., on $\mathbb{R}^n$. For a measurable subset $S \subset \mathbb{R}^n$, we will denote its volume (or measure) by $\mathrm{vol}(S)$.

Def: A subset $F \subset \mathbb{R}^n$ is called a **fundamental set** for Γ if F is measurable and the natural map $\coprod_{\gamma \in \Gamma} (F + \gamma) \longrightarrow \mathbb{R}^n$ is a bijection.

Lemma: If $F_1, F_2 \subset \mathbb{R}^n$ are fundamental sets for the same lattice $\Gamma \subset \mathbb{R}^n$, then $\mathrm{vol}(F_1) = \mathrm{vol}(F_2)$.

Note that, in view of the exercise in §2.11, the existence of a fundamental set for any lattice $\Gamma \subset \mathbb{R}^n$ is obvious. Assuming the lemma above, we define

$$\mathrm{vol}(\mathbb{R}^n/\Gamma) := \mathrm{vol}(F),$$

where $F \subset \mathbb{R}^n$ is any fundamental set for Γ.

Proof of the lemma. Let $G \subset \mathbb{R}^n$ be any measurable subset. By definition,

$$G = \bigsqcup_{\gamma \in \Gamma} \left((F_1 + \gamma) \cap G \right)$$

$$\Rightarrow \operatorname{vol}(G) = \sum_{\gamma \in \Gamma} \operatorname{vol}\left((F_1 + \gamma) \cap G \right)$$

$$= \sum_{\gamma \in \Gamma} \operatorname{vol}\left(F_1 \cap (G - \gamma) \right).$$

Now take $G = F_2$. We get

$$\operatorname{vol}(F_2) = \sum_{\gamma \in \Gamma} \operatorname{vol}\left(F_1 \cap (F_2 - \gamma) \right)$$

$$= \sum_{\gamma \in \Gamma} \operatorname{vol}\left((F_2 + \gamma) \cap F_1 \right)$$

$$= \operatorname{vol}(F_1)$$

using the change of variables $\gamma \longleftrightarrow -\gamma$

using the computation above with F_1 replaced by F_2.

§2.13. Minkowski's convex body lemma.

Let $\Gamma \subset \mathbb{R}^n$ be a lattice. Let $C \subset \mathbb{R}^n$ be a convex symmetric measurable subset with

$$\operatorname{vol}(C) > 2^n \cdot \operatorname{vol}(\mathbb{R}^n / \Gamma).$$

Then $C \cap \Gamma \neq \{0\}$.

Remark: "symmetric" means $C = -C$.

Question: Is every convex subset of $\mathbb{R}^n$ automatically Lebesgue measurable?

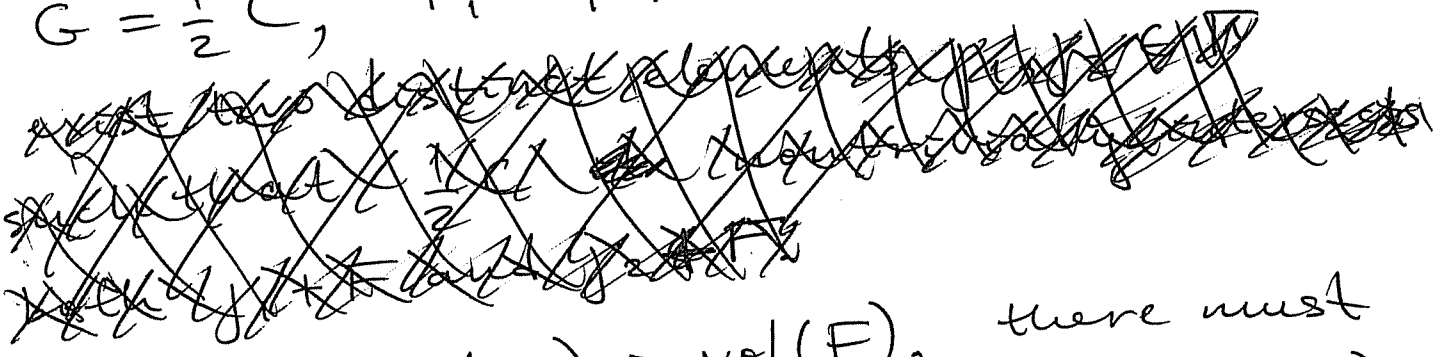
Remark: If we assume that C is compact, symmetric and convex, then it is enough to assume that $\mathrm{vol}(C) \geq 2^n \mathrm{vol}(\mathbb{R}^n/\Gamma)$.

§2.14. Proof of Minkowski's lemma.

We have $\mathrm{vol}\left(\frac{1}{2}C\right) = \frac{1}{2^n}\mathrm{vol}(C) > \mathrm{vol}(\mathbb{R}^n/\Gamma)$.

Let $F \subset \mathbb{R}^n$ be any fundamental subset for Γ and use the computation in §2.12 with

$G = \frac{1}{2}C$, $F_1 = F$.



Since $\mathrm{vol}\left(\frac{1}{2}C\right) > \mathrm{vol}(F)$, there must exist distinct $\gamma_1, \gamma_2 \in \Gamma$ such that $F \cap \left(\frac{1}{2}C - \gamma_1\right)$ and $F \cap \left(\frac{1}{2}C - \gamma_2\right)$ are not disjoint. In particular, $\exists\, c_1, c_2 \in C$ with $\frac{c_1}{2} - \gamma_1 = \frac{c_2}{2} - \gamma_2$.

Hence $\frac{1}{2}\left(c_1 + (-c_2)\right) = \gamma_1 - \gamma_2 \in \Gamma$

$\gamma_1 - \gamma_2 \neq 0$.

$\uparrow$ C by symmetry and convexity

This completes the proof of Minkowski's lemma.

§2.15. We will now restate Dirichlet's unit theorem.

Let D be a division algebra of finite dim. / $\mathbb{Q}$.
Let $A \subset D$ be an order. Define

$$D_{\mathbb{R}}^1 = \{x \in D_{\mathbb{R}} \mid |\mathrm{Norm}(x)| = 1\}$$ and equip it with the topology induced by the standard topology on $D_{\mathbb{R}}$. Then

$$A^\times = A \cap D_{\mathbb{R}}^1.$$ ← follows from §2.10

Note that $D_{\mathbb{R}}^1$ is a topological group and $A^\times$ is a subgroup of $D_{\mathbb{R}}^1$.

Theorem: $D_{\mathbb{R}}^1 / A^\times$ is a compact topological space with respect to the induced topology.

Exercise. Deduce the classical form of Dirichlet's unit theorem from this.

§2.16. Proof of Theorem 2.15.

Fix a volume form on $D_{\mathbb{R}}$. Note that A is a lattice in $D_{\mathbb{R}}$. Choose any compact convex symmetric subset $C \subset D_{\mathbb{R}}$ so that $\mathrm{vol}(C) > 2^n \mathrm{vol}(D_{\mathbb{R}}/A)$

(where $n = [D : \mathbb{Q}] = \dim_{\mathbb{Q}}(D)$).

Let $x \in D^1_{\mathbb{R}}$. This means that

$$\mathrm{vol}(Z) = \mathrm{vol}(Z \cdot x) \quad \forall \text{ measurable subset } Z \subset D_{\mathbb{R}}.$$

It follows that $\mathrm{vol}(D_{\mathbb{R}}/A \cdot x) = \mathrm{vol}(D_{\mathbb{R}}/A)$.

By Minkowski's lemma, $\exists\, 0 \neq a \in A$ so that $ax = c \in C$.

Let $s = \sup\{ |\mathrm{Norm}(c)| \mid c \in C \} < \infty$.

Now if a, x, c are as above, then $\mathrm{Norm}(a) \in \mathbb{Z}$ and $|\mathrm{Norm}(x)| = 1$, whence $\mathrm{Norm}(c) \in \mathbb{Z}$. Let $1, 2, \ldots, m$ be all the natural numbers $\leq s$. Then $|\mathrm{Norm}(c)| = r$ for some $1 \leq r \leq m$. Define

$$A_r = \{ a \in A \mid |\mathrm{Norm}(a)| = r \}$$

and $C_r = \{ c \in C \mid |\mathrm{Norm}(c)| = r \}$.

Each C_r is a compact set.

upshot: So far, we have shown that

$$D^1_{\mathbb{R}} = \bigcup_{r=1}^{m} A_r^{-1} C_r.$$

Now $a \in A_r \iff [A : Aa] = r$. But there are only finitely many left ideals $I \subset A$ that are principal and contain $r \cdot A$. Choose a finite set $S_r \subset A$ so that $\{ Ay \mid y \in S_r \}$ is the list of all such ideals. Now $a \in A_r$

$\Rightarrow Aa = Ay$ for some $y \in S_r \iff$

$uy = a$ for some $u \in A^\times$.

Therefore $a^{-1} = y^{-1}u^{-1}$.

So we have shown that

$$D^1_{\mathbb{R}} = \bigcup_{r=1}^{m} S_r^{-1} A^\times C_r .$$

Exercise: Fix the argument above, replacing ideals with left ideals, right to obtain $D^1_{\mathbb{R}} = \bigcup_{r=1}^{m} A^\times S_r'^{-1} C_r$ instead.

Now each S_r' is finite and C_r is compact $\Rightarrow$ $S_r'^{-1} C_r$ is a compact subset of $D^1_{\mathbb{R}}$.

This means that $A^\times \backslash D^1_{\mathbb{R}}$ is compact, which completes the proof of Theorem 2.15.

Remark: Here, the fact that D is a division algebra over $\mathbb{Q}$ is essential.