ZAHLENTHEORIE NOTE 14

THE UNIT THEOREM

Today we are going to speak about the units in $\mathcal{O}_k$

k = number field, $\mathcal{O}_k$ = ring of integers

$U_k = \mathcal{O}_k^*$ = group of units in $\mathcal{O}_k$

U_k is an abelian group. Its torsion part is

$$\mu_k = \{\text{roots of unity in } k\}$$

Prop: μ_k is finite and cyclic.

Thm [DIRICHLET'S UNIT THEOREM]

Let $r = |\{\text{real embeddings } k \hookrightarrow \mathbb{C}\}|$

$2s = |\{\text{nonreal embeddings } k \hookrightarrow \mathbb{C}\}|$

Then U_k is a finitely generated abelian group of rank $r+s-1$.

Hence, abstractly we have that

$$U_k \cong \mu_k \times \mathbb{Z}^{r+s-1}$$

Example: QUADRATIC FIELDS

Let d be a sqfr integer. Recall that

$$\{\mathbb{Q}[\sqrt{d}]\} \quad d \equiv 2,3 \ (4)$$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \ (4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \ (4) \end{cases}$$

So an element in $\mathcal{O}_K$ is of the form
$m + n\sqrt{d}$ or $m + n\left(\frac{1+\sqrt{d}}{2}\right)$, $m, n \in \mathbb{Z}$
and these are units if and only if their norm is ± 1 (recall: $\alpha \in \mathcal{O}_K$ is invertible $\Leftrightarrow N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ is invertible i.e. ± 1)
Computing the norm we get

$$N_{K/\mathbb{Q}}(m + n\sqrt{d}) = m^2 - n^2 d = \pm 1 \qquad (d \equiv 2,3 \ (4))$$
$$N_{K/\mathbb{Q}}\left(m + n\frac{1+\sqrt{d}}{2}\right) = \left(m + \frac{n}{2}\right)^2 - \frac{n^2}{4} d = \pm 1 \ (d \equiv 1 \ (4))$$

Let's see what does the theorem tells us:

- We first look at μ_K. To compute the roots of unity in K, observe that if $\zeta_n \in K$ is a root of unity of order $n \geq 3$ (otherwise $\zeta_n = \pm 1$), then $\mathbb{Q}(\zeta_n) \subseteq K$ so that $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \mid [K : \mathbb{Q}] = 2$ hence $\varphi(n) = 1, 2$. Since $n \geq 3$, it must be that $\varphi(n) = 2$ and then $K = \mathbb{Q}(\zeta_n)$.
Moreover $\varphi(n) = 2$ if and only if $n = 3, 4, 6$ and in those cases we get the fields

$$\mathbb{Q}(\zeta_4) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}) \qquad \mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$$

$$\mathbb{Q}(\zeta_3) = \mathbb{Q}\left(\frac{1+i\sqrt{3}}{2}\right) = \mathbb{Q}(\sqrt{-3})$$

Hence we get

$$\mu_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \langle i \rangle & \text{if } d = -1 \\ \langle \zeta_6 \rangle & \text{if } d = -3 \\ \pm 1 & \text{if otherwise} \end{cases}$$

- Now we look at the torsion-free part:

$(d<0)$ in this case we have $r=0$, $s=1$ hence

$$U_k \cong \mathbb{Z}^{r+s-1} \times \mu_k = \mu_k$$

so the group is cyclic and we have already classified it before. Notice that in particular the group U_k is finite, which was clear from the equations with the norm of before

$(d>0)$ in this case we have $r=2$, $s=0$.

Hence

$$U_k = \langle \pm 1 \rangle \times \mathbb{Z}$$

hence there is a unit $u \in \mathcal{O}_k^*$ s.t.

$$U_k = \{ \pm u^n \mid n \in \mathbb{Z} \}$$

This is called a FUNDAMENTAL UNIT.

In particular, this tells us that the equations with the norm of before have infinitely many

solutions, which is a priori not clear.

Now we give the proofs of the results.
The first one is actually easy:

<u>Lemma</u>: μ_K is finite.

<u>proof</u>: suppose $\zeta_n \in \mu_K$ is a primitive root of unity. Then $\mathbb{Q}(\zeta_n) \subseteq K$, so that
$$\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \mid K$$
Hence K can contain only those primitive n-th root of unity s.t. $\varphi(n) \mid K$, and these are a finite number. $\square$

<u>Lemma</u>: Let K be a field and $G \subseteq K^*$ a finite multiplicative subgroup. Then G is cyclic.

<u>proof</u>: see at the end of the notes for a proof.

<u>proof of Prop</u>: since μ_K is a finite subgroup of K^*, it is cyclic. $\square$

Dirichlet's theorem is a more involved.

<u>Lemma</u>: Fix m, M integers

$$\left\{ \alpha \in \mathbb{C} \text{ algebraic integer} \;\middle|\; \begin{array}{l} [\mathbb{Q}(\alpha):\mathbb{Q}] \leq m \\ |\alpha'| \leq M \text{ for all conjugates } \alpha' \text{ of } \alpha \end{array} \right\}$$

is finite

<u>proof</u>: such integers are all roots of degree $\leq m$ integer monic polynomials by the first conditions. Moreover, the coefficients of these polynomials are bounded by the second conditions. Hence, there are a finite number of such polynomials. $\square$

<u>Cor</u>. Let α be an algebraic integer such that all its conjugates α' have absolute value $|\alpha'| = 1$. Then α is a root of unity.

<u>proof</u>: consider the set $\{1, \alpha, \alpha^2, \alpha^3, \dots\}$ then all those elements have degree bounded by $[\mathbb{Q}(\alpha):\mathbb{Q}]$, and moreover the absolute value of each conjugate is 1. Hence, this set is finite by the lemma, so that $\alpha^n = \alpha^m$ for a certain $n > m$, i.e. $\alpha^{n-m} = 1$. $\square$

Now, let

$\rho_1, \rho_2, \dots, \rho_r$ = real embeddings

$$\begin{matrix} \tau_1, \tau_2, \dots, \tau_s \\ \overline{\tau}_1, \overline{\tau}_2, \dots, \overline{\tau}_s \end{matrix} = \begin{matrix} \text{non-real embeddings} \\ K \hookrightarrow \mathbb{C} \end{matrix}$$

Recall from last time the map

$$\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$$
$$\alpha \longmapsto (\rho_1(\alpha), \dots, \rho_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha))$$

We consider now the map

$$L : K^* \hookrightarrow \mathbb{R}^r \times \mathbb{R}^s$$
$$\alpha \longmapsto (\log|\rho_1(\alpha)|, \dots, \log|\rho_r(\alpha)|, \log|\tau_1(\alpha)|, \dots)$$

We make some observations:

- L is <u>well defined</u>: since $\alpha \neq 0$, $\rho_i(\alpha) \neq 0$, $\tau_j(\alpha) \neq 0$.
- L is <u>a homomorphism of groups</u>:
$$\log|\rho_i(\alpha\beta)| = \log|\rho_i(\alpha)\rho_i(\beta)| = \log|\rho_i(\alpha)| + \log|\rho_i(\beta)|$$
and the same for σ_j.
- <u>$\operatorname{Ker} L = \mu_K$</u>: $\alpha \in \operatorname{Ker} L$ if and only if for each conjugate α' it holds that $\log|\alpha'| = 1$, i.e. $|\alpha'| = 1$. By the previous corollary, this means that $\alpha \in \mu_K$.
Conversely, this also proves that $\mu_K \subseteq \operatorname{Ker} L$.
- Let $H = \left\{ \begin{matrix} x_1, \dots, x_r \\ y_1, \dots, y_s \end{matrix} \in \mathbb{R}^r \times \mathbb{R}^s \;\middle|\; \sum x_i + 2\sum y_j = 0 \right\}$

Then $\underline{L(U_k) \subseteq H}$: if $\alpha \in U_k$, then $|N_{k/\mathbb{Q}}(\alpha)| = 1$, so we get

$$1 = |N_{k/\mathbb{Q}}(\alpha)| = \left| \prod \rho_i(\alpha) \prod \sigma_j(\alpha)\overline{\sigma_j(\alpha)} \right|$$
$$= \prod |\rho_i(\alpha)| \cdot \prod_j |\sigma_j(\alpha)|^2$$

hence

$$0 = \log 1 = \sum \log|\rho_i(\alpha)| + 2\sum_j \log|\sigma_j(\alpha)|$$

So, this shows that $L(U_k) \subseteq H$ is a subgroup of $H \cong \mathbb{R}^{r+s-1}$. Now we show that this is actually a lattice

<u>Lemma</u>: $\Lambda \subseteq \mathbb{R}^n$ subgroup. Let $\|\cdot\|$ be any norm on $\mathbb{R}^n$. Then Λ is a lattice if and only if the set

$$\{\lambda \in \Lambda \mid \|\lambda\| \leq c\}$$

is finite for any $c > 0$.

<u>proof</u>: Λ is a lattice if and only if it is discrete. Suppose that Λ satisfies the above condition but it is not discrete. Then there is a point $\lambda_0 \in \Lambda$ that is not open: hence, λ_0 is an accumulation point for Λ

so that in each neighborhood of λ_0 there are infinitely many elements of $\Lambda \setminus \{\lambda_0\}$.
By translation by $-\lambda_0$, we see that this is true also of 0. But this is a contradiction.
The other direction is an easy exercise. $\square$

<u>Prop</u>: The image $L(U_K) \subseteq H$ is a lattice

<u>proof</u>: it is enough to show that $L(U_K) \subseteq \mathbb{R}^r \times \mathbb{R}^s$ is a lattice. Consider the $\|\cdot\|_\infty$ norm on $\mathbb{R}^{r+s}$ and let $C > 0$: we want to prove that the set

$$\{\alpha \in U_K \mid \|L(\alpha)\|_\infty \leq C\}$$

is finite. Observe that if $\|L(\alpha)\|_\infty \leq C$ then for each conjugate α' of α we have

$$\log|\alpha| \leq C$$

hence

$$|\alpha| \leq e^C$$

so that this set is finite by our proposition of before (observe that the degree is bounded by $[K:\mathbb{Q}]$) $\square$

<u>Cor</u>: U_K is finitely generated, and

$$U_K \cong \mu_K \times L(U_K)$$

<u>proof</u>: since $L(U_K)$ is a lattice, it is finitely generated. Moreover, we have a surjective homomorphism $U_K \overset{L}{\twoheadrightarrow} L(U_K)$ with kernel μ_K. Then let $e_1, \dots, e_r$ be a basis of $L(U_K)$ and $u_1, \dots, u_r \in U_K$ units s.t. $L(u_i) = e_i$

Show as an exercise that $L(U_k)$ is generated by μ_k and $u_1, \dots, u_n$, and this gives an isomorphism

$$U_k = \mu_k \times L(U_k). \qquad \square$$

The last step to prove the theorem is that $L(U_k) \subseteq H$ is a lattice of rank $r+s-1$, i.e. a full lattice.

To prove this we need a way to build units in $\mathcal{O}_k$.

We look again at the space $V = \mathbb{R}^r \times \mathbb{C}^s$

$$\sigma : \mathcal{O}_k \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s = V$$
$$\alpha \longmapsto (\rho_1(\alpha), \dots, \rho_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha))$$

On V we define the norm map

$$N(x_1, \dots, x_r, z_1, \dots, z_s) := \prod x_i \cdot \prod z_j \overline{z_j}$$

This is clearly continuous, and

$$|N(\sigma(\gamma))| = |N_{K/\mathbb{Q}}(\gamma)| \quad \forall \gamma \in \mathcal{O}_k$$

Furthermore, for two $v, w \in V$ we denote by $v \cdot w$ the coordinate-wise multiplication.

<u>Key</u>

<u>Lemma</u>: There is a compact subset $T^1 \subseteq V$ such that for every $v \in V$, $|N(v)| = 1$, there is an unit $\varepsilon \in U_k$ s.t.

$$\sigma(\varepsilon) \in T^1$$

Now we prove that $L(U_k)$ is a full lattice, assuming the key lemma:

<u>Proof of Dirichlet's Theorem</u>: we need to show that $L(U_k)$ has rank $r+s-1$. First observe that since T' is compact, there is an $M>0$ s.t. for every $w \in T'$ all the coordinates of w have absolute value $\leq M$. Now we prove that $L(U_k)$ is a full lattice. If $r+s-1=0$, then ok. Otherwise for every j from 1 to $r+s-1$ let $v_j \in V$ be an element whose i-th coordinate $(i \neq j)$ is very large compared to M and the j-th coordinate is such that $|N(v)=1|$. Then there is an unit ε_j s.t.

$$v_j \cdot \sigma(\varepsilon_j) \subseteq T'$$

Recall that

$$\sigma(\varepsilon_j) = (\rho_1(\varepsilon_j), \dots, \rho_r(\varepsilon_j), \tau_1(\varepsilon_j), \dots, \tau_s(\varepsilon_j))$$

$$L(\varepsilon_j) = (\log|\rho_1(\varepsilon_j)|, \dots, \log|\tau_s(\varepsilon_j)|)$$

Now we observe that by our choice of v_j, the i-th coordinate of $\sigma(\varepsilon_j)$ must be very small for $j \neq i$, hence the i-th coordinate of $L(\varepsilon_j)$ is negative for $j \neq i$.

We claim that the vectors

$$L(\varepsilon_1), L(\varepsilon_2), \dots, L(\varepsilon_{r+s-1}) \subseteq H$$

are linearly independent. Let's write these vectors in column form as

$$\begin{array}{cccc} L(\varepsilon_1) & L(\varepsilon_2) & & L(\varepsilon_{r+s-1}) \\ \left(\begin{array}{c} a_{11} \\ a_{21} \\ \vdots \\ a_{r+s-1,1} \\ a_{r+s,1} \end{array}\right. & \left|\begin{array}{c} a_{12} \\ a_{22} \\ \vdots \\ a_{r+s-1,2} \\ a_{r+s,2} \end{array}\right. & \left|\begin{array}{c} \cdots \\ \cdots \\ \\ \cdots \\ \cdots \end{array}\right. & \left.\begin{array}{c} a_{1,r+s-1} \\ a_{2,r+s-1} \\ \vdots \\ a_{r+s-1,r+s-1} \\ a_{r+s,r+s-1} \end{array}\right) \end{array}$$

We need to prove that this matrix has rank $r+s-1$. We know that:

- $a_{ij} < 0$ for $i \neq j$
- $\sum_{i=1}^{r} a_{ij} + \sum_{i=1}^{s-1} 2a_{r+i,j} + 2a_{r+s,j} = 0$ (because $L(\varepsilon_j) \in H$)

hence $\sum_{i=1}^{r} a_{ij} + \sum_{i=1}^{s-1} 2a_{r+i,j} = -2a_{r+s,j} > 0$

Then it follows that the matrix has maximal rank (Exercise). $\square$

Now we need to prove the Key Lemma:

<u>proof of Key Lemma</u>: we consider for each $v \in V$ s.t. $|N(v)| = 1$ the set

$$\{ \sigma(v) \mid \sigma \in \Phi \}$$

$$\{v \cdot \sigma(\mathcal{O}_K) = \{v \cdot \sigma(\gamma) \mid \gamma \in \mathcal{O}_K\}$$

One can show that this is also a lattice and that the volume of a fundamental parallelepipod is

$$\frac{1}{2^s}\sqrt{|\Delta_K|}$$

Now, let $T \subseteq V$ be one compact, convex subset symmetric w.r.t. the origin and with volume larger than $\frac{1}{2^s}\sqrt{|\Delta_K|}$.

Minkowski's convex body theorem tells us that there is a $\gamma \in \mathcal{O}_K$, $\gamma \neq 0$ s.t. $v \cdot \sigma(\gamma) \in T$.

Now, observe that since T is compact and N is continuous, there is a $M > 0$ s.t. $|N(w)| \leq M$ $\forall w \in T$. In particular, if $\gamma \in \mathcal{O}_K$ and $v \cdot \sigma(\gamma) \in T$ then

$$|N_{K/\mathbb{Q}}(\gamma)| = |N(\sigma(\gamma))| = |N(v \cdot \sigma(\gamma))| \leq M$$

Hence, all the ideals in the set

$$\{\gamma \cdot \mathcal{O}_K \mid v \cdot \sigma(\gamma) \in T \text{ for a certain } v, |N(v)| = 1\}$$

have numerical norm $\|I\| = |N_{K/\mathbb{Q}}(\gamma)| \leq M$ so that the set is finite. Let

$\gamma_1 \mathcal{O}_K, \gamma_2 \mathcal{O}_K, \ldots, \gamma_t \mathcal{O}_K$ be its elements.

and let

$$T' = \sigma(\gamma_1^{-1})T \cup \ldots \cup \sigma(\gamma_t^{-1})T$$

this will be the compact set that we want. Indeed for any $v \in V$ s.t. $|N(v)| = 1$ we know that there is a $\gamma \in \mathcal{O}_K$ s.t. $v \cdot \sigma(\gamma) \in T$. Hence $\gamma \mathcal{O}_K = \gamma_i \mathcal{O}_K$ for a certain i, so that

$$\gamma = \varepsilon \gamma_i \quad \text{for } \varepsilon \in U_K.$$

Then

$$v\sigma(\gamma) \in T \Rightarrow v\sigma(\varepsilon)\sigma(\gamma_i) \in T \Rightarrow v \cdot \sigma(\varepsilon) \in \sigma(\gamma_i^{-1})T. \quad \square$$

This concludes the proof of Dirichlet's theorem.

An extra lemma not proved before:

<u>Lemma</u>: Let K be any field and $G \subseteq K^*$ a finite subgroup. Then G is cyclic.

<u>proof</u>: Let $n = |G|$. for any $d \mid n$ let $G_d = \{x \in G \mid x \text{ has order } d\}$

We claim that $|G_d| = 0$ or $|G_d| = \varphi(d)$.

Suppose that $G_d \neq \emptyset$ so there is $\alpha \in G_d$.

Now we see that

$$G_d \subseteq \{x \in G \mid x^d - 1 = 0\}$$
$$\langle \alpha \rangle \subseteq \{x \in G \mid x^d - 1 = 0\}$$

however $|\{x \in G \mid x^d - 1 = 0\}| \leq d$ because the polynomial $x^d - 1$ can have at most

d roots in a field. However $\langle \alpha \rangle$ has also d elements because α has order d, so that $\langle \alpha \rangle = \{ x \in G \mid x^d = 1 \}$. Hence, $G_d \subseteq \langle \alpha \rangle$ and this means that G_d consists precisely of the elements in $\langle \alpha \rangle$ of order d. Since $\langle \alpha \rangle \cong \mathbb{Z}/d\mathbb{Z}$ there are $\varphi(d)$ of these.

Now, observe that $G = \bigsqcup_{d \mid n} G_d$, hence

$$n = |G| = \sum_{d \mid n} |G_d| \leq \sum_{d \mid n} \varphi(d) = n$$

Hence it must be that $|G_d| = \varphi(d) \ \forall d \mid n$.

In particular $|G_n| = \varphi(n) \neq 0$, so there is an element of order n, meaning that G is cyclic. $\square$

Ultima modifica: 14:44