INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.637/23

ADVANCED WORKSHOP ON ARITHMETIC ALGEBRAIC GEOMETRY

(31 August - 11 September 1992)

Algebraic Number Theory - Lecture II

M. Kenku
Department of Mathematics
University of Lagos
Akoka-Yaba
Lagos
Nigeria

These are preliminary lecture notes, intended only for distribution to participants

MAIN BUILDING STRADA COSTIERA, 11 TEL. 22401 TELEFAX 224163 TELEX 460392 ADRIATICO GUEST HOUSE VIA GRIGNANO, 9 TEL. 224241 TELEFAX 224531 TELEX 460449
MICROPROCESSOR LAB. VIA BEIRUT, 31 TEL. 224471 TELEFAX 224600 TELEX 460392 GALILEO GUEST HOUSE VIA BEIRUT, 7 TEL. 22401 TELEFAX 224559 TELEX 460392

Algebraic Number Theory (2)

M. A. Kenku

Geometry of numbers and some finiteness theorems

Preliminaries Let K be an algebraic number field of degree n.

There are n distinct isomorphisms of K in $\mathbb{C}$, the field of complex numbers. We denote them by σ_i, $1 \le i \le n$, and arrange them so that σ_i, $1 \le i \le r_1$ are the real ones and

$\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for $j = 1, \ldots, r_2$.

Let $\mathcal{O}_K$ be the ring of integers of K, which is the integral closure of $\mathbb{Z}$ in K. $\mathcal{O}_K$ is a Dedekind domain and as a $\mathbb{Z}$-submodule of K it is free of rank n. If $(\omega_1, \ldots, \omega_n)$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$ then the absolute discriminant of K is

$$d_K = \det\left(\operatorname{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)\right)_{1 \le i,j \le n} = \det\left(\sigma_j(\omega_i)\right)_{1\le i,j\le n} \neq 0$$

For $\mathfrak{a}$ an integral ideal, $\mathfrak{a} \neq (0)$, $\mathcal{O}_K/\mathfrak{a}$ is finite and we define the absolute norm of $\mathfrak{a}$

$$\mathbb{N}(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$$

It is easy to show that

(i) If $\mathfrak{a} = (a)$ a principal ideal $N(a) = |N_{K/\mathbb{Q}}\, a|$

(ii) $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$ for non-zero integral ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}_K$.

An immediate consequence of the finiteness of $A/\mathfrak{a}$ is that $\mathfrak{a}$ is also a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank n. This follows from the fact a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module of rank n is free of rank $\leq n$. Since $\mathfrak{a}$ is of finite index in $\mathcal{O}_K$ its rank is also n.

The starting point of this talk is the following exact sequence which featured in the talk of Nart.

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1.$$

where $\mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$, J_K is the group of fractional ideals and Cl_K is the ideal class group of $\mathcal{O}_K$.

The main aim of this lecture is give a proof of the finiteness of Cl_K and to show that $\mathcal{O}_K^\times \cong W_K \times \mathbb{Z}^{r_1+r_2-1}$

where W_K is the group of roots of unity of K

Geometry of Numbers H

Def A subgroup of the Euclidean space $\mathbb{R}^n$ is discrete if for any compact subset B of $\mathbb{R}^n$ the intersection $H \cap B$ is finite

Example $H = \mathbb{Z}^n$ is a discrete subgroup of $\mathbb{R}^n$.

The following theorem shows that this is almost the prototype of discrete subgroups of $\mathbb{R}^n$

Theorem An additive subgroup H of $\mathbb{R}^n$ is discrete if and only if it is generated by r vectors which are linearly independent over $\mathbb{R}$ so $(r \leq n)$.

For a proof of this see Weiss [4].

Def A discrete subgroup H of $\mathbb{R}^n$ of rank n is called a lattice

Given such a lattice H let $\underline{e} = (e_1, \quad , e_n)$

be a $\mathbb{Z}$-basis. Denote by P_e the half open parallelotope

$$P_e = \{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} \alpha_i e_i \text{ with } 0 \le \alpha_i < 1 \}$$

P_e is a fundamental domain for H . . . so that every point of $\mathbb{R}^n$ is congruent to one and only one point of P_e modulo H.

Let μ denote the Lebesgue measure in $\mathbb{R}^n$ and for a measurable subset S of $\mathbb{R}^n$, let $\mu(S)$ denote the measure of S.

If $\underline{f} = (f_1, \ldots, f_n)$ is another $\mathbb{Z}$-basis of H. Since $\underline{f} = \underline{e}\,(a_{ij})$ $\quad a_{ij} \in \mathbb{Z}$ $\quad 1 \le i, j \le n$.

$$\mu(P_f) = |\det(a_{ij})|\, \mu(P_e) = \mu(P_e)$$

so that this is independent of the particular basis and it is called the volume of the lattice and denoted by $v(H)$.

<u>Theorem</u> (Minkowski). Let H be a lattice in $\mathbb{R}^n$ and let S be a measurable subset of $\mathbb{R}^n$. If $\mu(S) > v(H)$ then there exists distinct elements x, y in S such that $x - y \in H$.

Proof ~~Since~~ Let $\underline{e} = (e_1, \quad e_n)$ be a $\mathbb{Z}$-basis of H. Since P_e is a fundamental domain for H in $\mathbb{R}^n$

$$S = \bigcup_{h \in H} \left(S \cap (P_e + h)\right)$$

so that

$$\mu(S) = \sum \mu\left(S \cap (P_e + h)\right)$$

Since μ is translation invariant

$$\mu\left(S \cap (P_e + h)\right) = \mu\left((-h + S) \cap P_e\right).$$

If the $(-h + S) \cap P_e$ are pair-wise disjoint as h varies over H, then

$$\sum \mu\left((-h+S) \cap P_e\right) \leq \mu(P_e) = v(H)$$

and this will contradict the hypothesis that

$$v(S) > v(H)$$

Hence there exists distinct points h, h' such

$$(-h + S) \cap (-h' + S) \neq \emptyset.$$

Let $x, y \in S$ be such that

$$-h + x = -h' + y. \quad \text{Then}$$

$$x - y = h - h' \in H \quad \text{and } x - y \neq 0.$$

Corollary If H is a lattice in $\mathbb{R}^n$ and S is a measurable, convex subset of $\mathbb{R}^n$ which is symmetric with respect to 0, then if S satisfies either

(i) $\mu(S) > 2^n v(H)$

(ii) $\mu(S) \geq 2^n v(H)$ and S is compact then there exists a non-zero element of S which lies in H

Proof: (i) Put $S' = \frac{1}{2} S$. Then $\mu(S') = 2^{-n} \mu(S) > v(H)$

so by Minkowski's theorem $\exists\ x, y \in S'$ $x \neq y$ such that $x - y \in H$.

$x - y = \frac{1}{2}(2x - 2y)$,

Clearly $2x$ and $2y$ lie in S. Since S is symmetric with respect to 0, $-2y$ also lies in S. As S is convex $\frac{1}{2}(2x - 2y) \in S$.

Hence $x - y \in S$, but $x - y$ also lies in H.

(ii) For $\varepsilon > 0$ Put $S_\varepsilon = (1+\varepsilon) S$

Then $\mu(S_\varepsilon) = (1+\varepsilon)^n \mu(S) > 2^n v(H)$

and so from (i) $S_\varepsilon \cap H - \{0\} \neq \emptyset$ for each $\varepsilon > 0$. In fact it is finite as S_ε is compact.

Since $S_{\varepsilon'} \supset S_\varepsilon$ if $\varepsilon' > \varepsilon$

$$S \cap H - \{0\} = \bigcap_{\varepsilon > 0} \left(S_\varepsilon \cap H - \{0\} \right) \quad \text{is not empty.}$$

<u>Applications</u>

We define an imbedding of K into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as follows

$$\sigma : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

so that $\sigma(x) = (\sigma_1(x), \quad , \sigma_{r_1+r_2}(x))$

We may view $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as $\mathbb{R}^n$ by splitting a complex entry into its real and imaginary components.

For the theorems we have in view, our lattices will be the images of integral ideals under this canonical embedding. So, first, we prove the following

<u>Theorem</u> If M is a free $\mathbb{Z}$-module of rank n and if $x = (x_1, \ldots x_n)$ is a $\mathbb{Z}$-basis of M then $\sigma(M)$ is a lattice of $\mathbb{R}^n$ with volume

$$V(\sigma(M)) = 2^{-r_2} \left| \det(\sigma_j(x_i)) \right|.$$

<u>Proof</u>. With respect to the canonical basis of $\mathbb{R}^n$ the coordinates of

$\sigma(x_i)$ is $(\sigma_1(x_i), \quad \sigma_{r_1}(x_i), R\sigma_{r_1+1}(x_i), I\sigma_{r_1+1}(x_i), \ldots R\sigma_{r_1+r_2}(x_i), I\sigma_{r_1+r_2}(x_i))$

where $R(z)$ and $iI(z)$ stand for the real and imaginary parts of z, a complex number.

The determinant D of the matrix whose ith column is $\sigma(x_i)$ is

$$D = (2i)^{-r_2} \det(\sigma_j(x_i))$$

Since $M \otimes_{\mathbb{Z}} \mathbb{Q} = K$ and K is a separable extension of $\mathbb{Q}$, $D \neq 0$. Hence $(\sigma(x_1), \ldots \sigma(x_n))$ is linearly independent in $\mathbb{R}^n$ over $\mathbb{R}$ and $\sigma(M)$ is a lattice in $\mathbb{R}^n$. Since the lattice $\mathbb{Z}^n$ has volume 1

$$v(\sigma(M)) = 2^{-r_2} \left|\det(\sigma_j(x_i))\right|.$$

<u>Cor</u> In particular if $M = \mathcal{O}_K$, (resp. $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$) then

$$v(\sigma(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|d_K|}$$

$$\left(\text{resp } v(\sigma(\mathfrak{a})) = 2^{-r_2}\sqrt{|d_K|} \cdot N(\mathfrak{a})\right).$$

For our next theorem, we need to know the measure of the following set. Let $t \in \mathbb{R}$ be such that $t > 0$

Put

$$S_t = \left\{ x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \;\middle|\; x = (y_1, \ldots y_{r_1}, z_1, \ldots z_{r_2}) \text{ with } \sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|z_j| \leq t \right.$$

<u>Lemma</u> $$\mu(S_t) = \frac{2^{r_1 - r_2}\pi^{r_2} t^n}{n!}$$

Proof This is by induction on n.

If $n=1$, $r_1=1$, $r_2=0$

$$\mu(S_t) = 2t$$

If $n=2$, $\begin{cases} r_1=2, & r_2=0 \quad : \quad \mu(S_t) = 2t^2 \\ r_1=0, & r_2=1 \quad \quad \mu(S_t) = \frac{\pi t^2}{4}. \end{cases}$

Suppose by induction hypothesis it is true for $r<n$.

Then if $r=n$

for $r_1>0$
$$\mu(S_t) = 2\int_0^t \frac{2^{r_1-r_2-1}\pi^{r_2}(t-s)^{n-1}}{(n-1)!}\,ds$$
$$= \frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!}$$

if $r_2>0$
$$\mu(S_t) = \int_0^{t/2} \frac{2^{r_1-r_2+1}\pi^{r_2-1}(t-2s)^{n-2}(2\pi s)}{(n-2)!}\,ds$$
$$= \frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!}$$

Proposition For K, n, r_1, r_2 as defined earlier. Given a non-zero integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$, there exists a non-zero element $x\in\mathfrak{a}$ such that
$$|N_{K/\mathbb{Q}}(x)| \le B\cdot \mathbb{N}(\mathfrak{a})$$
where $B = \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|}$ is called Minkowski's bound.

Proof Let $\sigma: K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the canonical embedding of K and let S_t be as defined in the preceding lemma. Choose t such that

$$\mu(S_t) \geq 2^n\, v(\sigma(\mathfrak{a}))$$

i.e.

$$\frac{2^{r_1 - r_2}\pi^{r_2} t^n}{n!} \geq 2^{n-r_2}\sqrt{|d_K|}\; N(\mathfrak{a}) \qquad (1)$$

S_t is compact, convex and measurable with respect to O in $\mathbb{R}^n$ hence by Minkowski's theorem $\exists\, 0 \neq x \in \mathfrak{a} \ni \sigma(x) \in S$.

From (1) we have that

$$t^n \geq 2^{n-r_1}\pi^{-r_2} n! \sqrt{|d_K|}\; \mathbb{N}(\mathfrak{a}).$$

hence

$$|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r_1}|\sigma_i(x)| \prod_{j=r_1+1}^{r_2}|\sigma_j(x)|^2 \leq \left|\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(x)| + \frac{2}{n}\sum_{j=r_1+1}^{r_2}|\sigma_j(x)|\right|^n \leq \frac{t^n}{n^n}$$

The first inequality arising because geometric mean does not exceed arithmetic mean

Hence $|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|}\;\mathbb{N}(\mathfrak{a})$

Corollary Every ideal class C contains an integral ideal $\mathfrak{b}$ such that

$$\mathbb{N}(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|}$$

Proof. Let $\mathfrak{a}'$ be an ideal of class C. By multiplying by a principal ideal (d) say $d \neq 0$, $d \in K$ we can take $\mathfrak{a}'$ such that its inverse $\mathfrak{a} = \mathfrak{a}'^{-1}$ is an integral ideal of $\mathcal{O}_K$

(not just a fractional ideal). By the preceding theorem, $\exists\ 0 \neq x \in \mathfrak{a}$ $\ni$

$$\left| N_{K/\mathbb{Q}}(x) \right| \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|d_K|}\ N(\mathfrak{a}).$$

Take $\mathfrak{b} = (x)\,\mathfrak{a}^{-1}$ ($\subset \mathcal{O}_K$ since $\mathfrak{a}$ divides (x)).

Hence $|N(\mathfrak{b})| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|}$.

<u>Corollary</u> Let K be a number field of degree n and let d_K be its absolute discriminant. Then for $n \geq 2$

$$|d_K| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}$$

In particular $|d_K| > 1$. (Hermite – Minkowski)

Furthermore $n/\log|d_K|$ is bounded above.

<u>Proof</u>. As shown above for any given class C of Cl_K, there is an integral ideal $\mathfrak{b}$ such that

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|}$$

since $\mathfrak{b}$ is integral $N(\mathfrak{b}) \geq 1$

hence $\sqrt{|d_K|}\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \geq 1$

$$\Rightarrow |d_K| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2}$$

As $\frac{\pi}{4} < 1$ and $2r_2 \leq n$.

We see that

$$|d_K| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2} = a_n \quad \text{(say)}.$$

$$a_2 = \frac{\pi^2}{4}; \qquad \frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} = \frac{\pi}{4}\left(1+2+\text{(positive terms)}\right)$$

hence $$|d_K| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2} \qquad \ldots \quad (2)$$

clearly $|d_K| > 1$ for $K \neq \mathbb{Q}$

taking logarithm in (2) we have that

$\dfrac{n}{\log|d_K|}$ is bounded above.

<u>Theorem</u> (Dirichlet) The ideal class group Cl_K is finite

<u>Proof</u>: As shown above each ideal class C has an integral ideal $\mathfrak{b}_c$ such that $N(\mathfrak{b}_c) \leq B$

So it suffices to prove that there are at most finitely many integral ideals with a given absolute norm.

To do this it suffices first to show that if $\mathfrak{a}$ is an integral ideal of absolute norm a then $a \in \mathfrak{a}$ and also to show that only finitely many integral ideals contain a.

Suppose $N(\mathfrak{a}) = a$ then $\# \mathcal{O}_K/\mathfrak{a} = a$.

Let $\alpha_1, \ldots, \alpha_a$ be a complete set of representatives of $\mathcal{O}_K/\mathfrak{a}$ in $\mathcal{O}_K$. Then $\alpha_1+1, \ldots, \alpha_a+1$ is also a a complete set of reps.

Therefore

$$\sum_{i=1}^{a} x_i \equiv \sum_{i=1}^{a} \alpha_i + 1 \pmod{\mathfrak{a}}$$

$$\Rightarrow \quad a \equiv 0 \pmod{\mathfrak{a}}$$

and $a \in \mathfrak{a}$.

Now suppose $a \in \mathfrak{a}$. This implies $(a) \subset \mathfrak{a}$ i.e. $\mathfrak{a} | (a)$. Since O_K is a Dedekind domain and there is unique factorisation of ideals, $\mathfrak{a}$ has to be one of the finitely many factors of the principal ideal (a).

This completes the proof.

<u>Theorem</u> (Hermite) There are only finitely many algebraic number fields with a given absolute discriminant d.

<u>Proof</u>. If n is the degree of such a field as shown earlier $|d| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}$ so that n is bounded. We can thus fix n and also r_1 and r_2 since we are only concerned about finiteness of the number of such fields.

Applying Minkowski's theorem we will construct a non-zero integer x of such a field K, which will be primitive and such that all its conjugates have bounded absolute values. This implies that the minimal equation which is necessarily of degree n, has integral coefficient which are bounded. Hence there are only finitely many such fields.

So let K be such a field. In $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ we consider the following set S

(i) If $r_1 > 0$ $S = \{ (y_1, \dots y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid$
$|y_1| \le 2^n \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}$, $|y_i| \le \frac{1}{2}$ $2 \le i \le r_1$ $|z_j| \le \frac{1}{2}$ $1 \le j \le r_2 \}$.

(ii) if $r_1 = 0$
$S = \{ (z_1, \dots, z_{r_2}) \in \mathbb{C}^{r_2} \mid |z_1 - \bar{z}_1| < 2^n \left(\frac{2}{\pi}\right)^{r_2 - 1} \sqrt{|d_K|}$
$|z_1 + \bar{z}_1| \le \frac{1}{2}$, $|z_j| \le \frac{1}{2}$ $2 \le j \le r_2 \}$

S is compact, convex and symmetric with respect to 0 in $\mathbb{R}^n$.
Its volume $\mu(S) = 2^{n-r_2} \sqrt{|d_K|} \ge v(\sigma(\mathcal{O}_K))$.
so that by the corollary to Minkowski's theorem $\exists$ a ~~non-zero~~ element $x \in \mathcal{O}_K$ such $\sigma(x) \in S$.
So we now show that x is primitive. To do this it suffices to show that $\sigma_1(x) \ne \sigma_j$ for $j \ne 1$

In case (i) Since $x \in \mathcal{O}_K$ $|N_{K/\mathbb{Q}}(x)| \ge 1$, which implies that
$|\sigma_1(x)| > 1$, ~~for~~ $|\sigma_j(x)| \le \frac{1}{2}$ for $j \ne 1$.

Hence $\sigma_1(x) \ne \sigma_j(x)$, $2 \le j \le r_1 + r_2$.
So that x is primitive

In case (ii) Again $|N_{K/\mathbb{Q}} x| \ge 1$ and $\sigma_1(x) \ne \sigma_j(x)$ $j \ne 1$.
$|\sigma_1(x)| = |\overline{\sigma_1(x)}| > 1$.

Also $|\mathbb{R}\,\sigma_1(x)| \leq 1/4$ so that $\sigma_1(x)$ is not real.

Hence x is primitive

Dirichlet Unit Theorem

First we note that an integral element x of K is a unit if and only if $N_{K/\mathbb{Q}}\,x = \pm 1$

If $x \in \mathcal{O}_K^\times$, then

$$1 = N_{K/\mathbb{Q}}(1) = N_{K/\mathbb{Q}}(x x^{-1}) = N_{K/\mathbb{Q}}(x) \cdot N_{K/\mathbb{Q}}(x)^{-1}$$

since $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$, $N_{K/\mathbb{Q}}(x) = \pm 1$

Conversely if for $x \in \mathcal{O}_K$ $N_{K/\mathbb{Q}}(x) = \pm 1$ then the characteristic equation of x is of the form

$$x^n + \qquad + a_1 x \pm 1 = 0 \quad \text{with } a_i \in \mathbb{Z}.$$

so that $x^{-1} = x^{n-1} + \cdots + a_1 \in \mathcal{O}_K$.

Let W_K be the group of roots of unity in $\mathcal{O}_K^\times$.

The logarithmic embedding $\lambda : K^* \longrightarrow \mathbb{R}^{r_1+r_2}$ sends $\mathcal{O}_K^\times$ to the hyperplane $H = \left\{ (x_i) \,\middle|\, \sum_{i=1}^{r_1} x_i + 2\sum_{i=r_1+1}^{r_1+r_2} x_i = 0 \right\}$.

Let $\Gamma \subseteq H$ be the image of $\mathcal{O}_K^\times$

<u>Theorem</u> $1 \longrightarrow W_K \longrightarrow \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \longrightarrow 0$ is an exact sequen

<u>Proof.</u> It suffices to show that $W_K = \operatorname{Ker}\lambda$.

Since $1 = |1| = |\sigma_i(x)^2| = |\sigma_i(x)|^2 \Rightarrow |\sigma_i(x)| = 1$

$W_K \subseteq \operatorname{Ker}\lambda$.

Conversely $x \in \ker \lambda \Rightarrow |\sigma_i(x)| = 1$ for $1 \le i \le r_1 + r_2$ so $\sigma(x)$ lies in a compact set of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. As $\sigma(\mathcal{O}_K)$ is discrete, $\ker \lambda$ is finite. But every finite multiplicative subgroup of a field consists of roots of unity so $\ker \lambda \subseteq W_K$ and $\ker \lambda = W_K$.

To prove that $\mathcal{O}_K^\times \cong W_K \times \mathbb{Z}^{r_1 + r_2 - 1}$ we now only need to determine the structure of Γ.

We need the following lemma

<u>Lemma</u> There are only finitely many elements $\alpha \in \mathcal{O}_K$ modulo associates with a given norm.

<u>Proof</u>. Follows from the earlier proof about finiteness of integral ideals with a given absolute norm.

<u>Theorem</u> Γ is a lattice in H.

<u>Proof</u> First we prove that it is discrete. Let $\mathcal{B}$ be a compact set in $\mathbb{R}^{r_1+r_2}$, then there is a real number $\alpha > 1$ such that if $\lambda(x) \in \Gamma \cap B$

$\alpha^{-1} < |\sigma_i(x)| < \alpha$ for all $1 \le i \le r_1 + r_2$.

consequently there are only finitely many $x \in \mathcal{O}_K$ such that $\lambda(x) \in \Gamma \cap B$. Hence Γ is discrete.

To prove that Γ is a lattice it suffices to find a bounded set $M \subseteq H$ such that

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma)$$

To do this it suffices to cover the norm-one sphere S in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by the translates by $\log^{-1}\Gamma$ of a certain bounded set $T \subseteq S$. ie show that $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} T \cdot \sigma(\varepsilon)$. (3)

(Note T bounded subset of $S \Rightarrow \log(T) \subseteq H$ is bounded.

For $i = 1, \ldots, n$ choose $c_i \in \mathbb{R}$ $c_i > 0$ $c_{r_1+j} = c_{r_1+r_2+j}$ $j = 1, \ldots$ such that $C = \prod_{i=1}^{n} c_i > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}$.

Consider $X = \{ (x_i) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_i| < c_i \}$

<u>Claim</u> for any $y = (y_i) \in S$ $\exists$ $a \in \mathcal{O}_K$ $a \neq 0$ such that $\sigma(a) \in X \cdot y$.

<u>proof of claim</u> $X \cdot y = \{ (x_i) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_i| < c_i |y_i| \}$ is symmetric and convex with respect to 0. The volume

$$v(X \cdot y) = \prod_{i=1}^{r_1} 2c_i|y_i| \cdot \prod_{i=r_1+1}^{r_1+r_2} \pi c_i^2 |y_i|^2 = 2^{r_1} \pi^{r_2} C > v(\sigma(\mathcal{O}_K))$$

(note that $N_{K/\mathbb{Q}}(y) = 1$).

We apply Minkowski's theorem to show $\exists\, 0 \neq a \in \mathcal{O}_K$ such that $\sigma(a) \in X \cdot y$. Note that $N_{K/\mathbb{Q}}(a) \leq C$

This settles the claim

Let $\alpha_1, \ldots, \alpha_N$ be a complete set of representatives of integers a up to associates such that $N_{K/\mathbb{Q}}(a) \leq C$

hence $T = S \cap \left(\bigcup_{i=1}^{N} X \cdot \sigma(\alpha_i)^{-1} \right)$

Claim T satisfies (3) above

Let $y \in S$. As shown above $\exists\, a \in \mathcal{O}_K$ such that $\sigma(a) \in X \cdot y^{-1}$ and $N_{K/\mathbb{Q}}(a) \leq C$.

So let α_i, $1 \leq i \leq n$, be such that $a\varepsilon = \alpha_i$ for some $\varepsilon \in \mathcal{O}_K^\times$.

Then $\sigma(a) = x y^{-1}$ for some $x \in X$.

hence $y = x \cdot \sigma(\alpha_i)^{-1}\, \sigma(\varepsilon)$.

and $y \in T \cdot \sigma(\varepsilon)$

Hence Γ is a lattice in H.

We therefore have $\underline{\mathcal{O}_K^\times \cong W_K \times \mathbb{Z}^{r_1+r_2-1}}$.

Finally, suppose we chose $\xi_1, \ldots, \xi_r$ ($r = r_1+r_2-1$) in $\mathcal{O}_K^\times$ such that $\{\lambda(\xi_1), \ldots, \lambda(\xi_r)\}$ generate the lattice Γ, then the set $\{\xi_1, \ldots, \xi_r\}$ is called a <u>fundamental system of units</u> of K and the absolute value of the determinant

$$\det\begin{pmatrix} \log|\sigma_1(\xi_1)|, & & \log|\sigma_r(\xi_1)| \\ \vdots & & \\ \log|\sigma_1(\xi_r)|, & & \log|\sigma_r(\xi_r)| \end{pmatrix}$$

is denoted by R and is called the <u>regulator</u> of K. It is independent of the choice of the fundamental system of units and the choice of distinct r embeddings out the first $r+1$.

Bibliography

[1] S. Lang: Algebraic Numbers. Addison Wesley 196[illegible]

[2] J. Neukirch. Algebraische Zahlentheorie. Springer 1992

[3] P. Samuel. Algebraic Theory of Numbers. Hermann Paris 1970

[4] E. Weiss Algebraic Number Theory. New York. McGraw-Hill 1963.