Algebraic Number Theory – Lecture 4

Sandro Bettin

"What the world needs is more geniuses with humility, there are so few of us left."

– Oscar Levant

1. Discriminants

Definition 1. Let K be a number field and $\underline{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$ be a basis for K. The discriminant of $\underline{\alpha}$ is

$$\Delta[\underline{\alpha}] = (\det(\sigma_i(\alpha_j)))^2$$

where σ_i are the embeddings $K \hookrightarrow \mathbb{C}$.

Remark. $\Delta[\underline{\alpha}] \in \mathbb{Q}$ since

$$\begin{aligned}\sigma_\rho(\Delta[\underline{\alpha}]) &= (\det(\sigma_\rho\sigma_i(\alpha_j)))^2 \\ &= (\pm\det(\sigma_i(\alpha_j)))^2 \\ &= \Delta[\underline{\alpha}].\end{aligned}$$

If $\underline{\alpha} \subset \mathcal{O}_K$ then $\Delta[\underline{\alpha}] \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Theorem S1. *There exists an integral basis $\underline{\alpha} = \{\alpha_1 \ldots, \alpha_n\}$ with $n = [K : \mathbb{Q}]$.*

Sketch proof. Take a $\mathbb{Q}$-basis $\underline{\alpha} \subset \mathcal{O}_K$ of K with $\Delta[\underline{\alpha}]$ minimal. Then suppose that $\underline{\alpha}$ is not an integral basis, so there exists $\omega \in \mathcal{O}_K$ with, say,

$$\omega = \theta_1\alpha_1 + \ldots + \theta_n\alpha_n$$

where $\theta_1 \notin \mathbb{Z}$, i.e. $\theta_1 = \theta + r$ for some $0 < r < 1$. Then $\underline{\alpha}' = \{\omega - \theta\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is given by

$$\underline{\alpha}' = \begin{pmatrix} \theta_1 - \theta & \theta_2 & \theta_3 & \cdots & \theta_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \underline{\alpha}.$$

So

$$\Delta[\underline{\alpha}'] = r^2\Delta[\underline{\alpha}] < \Delta[\underline{\alpha}]$$

contradicting the minimality of $\Delta[\underline{\alpha}]$. $\square$

Corollary. *All integral bases of a given number field have the same discriminant up to sign, say $|\Delta|$.*

Corollary. *If $\underline{\alpha}$ is a $\mathbb{Q}$-basis of K and $\underline{\alpha} \subset \mathcal{O}_K$, and if $\Delta[\underline{\alpha}]$ is square free then $\underline{\alpha}$ is an integral basis.*

Proof. If $\underline{\alpha}'$ is an integral basis then $\underline{\alpha} = (c_{i,j})\underline{\alpha}'$ for some matrix $(c_{i,j}) \in \mathbb{Z}^{n,n}$. So $\Delta[\underline{\alpha}] = (\det(c_{i,j}))^2\Delta$, whence $\det(c_{i,j}) = \pm 1$ as $\Delta[\underline{\alpha}]$ is square free. So $(c_{i,j}) \in \mathrm{Gl}_n(\mathbb{Z})$ and so $\underline{\alpha}' = (c_{i,j})^{-1}\underline{\alpha}$, thus $\underline{\alpha}$ is an integral basis as well. □

Theorem S2. *If $K = \mathbb{Q}(\theta)$ is a number field of degree n, then*

$$\Delta[1, \theta, \dots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(Dp(\theta))$$

where p is the minimal polynomial of θ and D is the formal derivative.

2. Quadratic fields

K is a quadratic field if $[K : \mathbb{Q}] = 2$. If $K = \mathbb{Q}(\theta)$ is a quadratic field then

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

i.e. θ is a root of $t^2 + at + b$. Writing $\sqrt{a^2 - 4b} = r\sqrt{d}$ with $d \in \mathbb{Z}$ square free, then clearly $K = \mathbb{Q}(\sqrt{d})$.

Theorem S3. *Let $d \in \mathbb{Z}$ be square free and $K = \mathbb{Q}(\sqrt{d})$. Then*

- *if $d \not\equiv 1 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $\Delta = 4d$;*
- *if $d \equiv 1 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{d})/2]$ and $\Delta = d$.*

Proof. Let $\alpha \in K$, so $\alpha = \dfrac{a + b\sqrt{d}}{c}$ with $\mathrm{hcf}(a, b, c) = 1$. Claim that $\alpha \in \mathcal{O}_K$ if and only if

$$\left(t - \frac{a + b\sqrt{d}}{c}\right)\left(t - \frac{a - b\sqrt{d}}{c}\right) \in \mathbb{Z}[t].$$

So if and only if

$$\frac{2a}{c} \in \mathbb{Z}, \text{ and} \tag{1}$$

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}. \tag{2}$$

Let $q = \mathrm{hcf}(a, c)$. From (2), $q^2 \mid a^2 - b^2 d$. But $q^2 \mid a^2$ and d is square free, so $q \mid b$. But $hcf(a, b, c) = 1$ so $q = 1$. From (1), then, $c = 1$ or 2. If $c = 1$ then $\alpha \in \mathcal{O}_K$ anyway.

If $c = 2$ then $a^2 - b^2 d \equiv 0 \pmod 4$ by (2). But a is odd as $q = 1$ and so b must be odd too, whence $a^2 \equiv b^2 \equiv 1 \pmod 4$. Hence $1 - d \equiv 0 \pmod 4$. □

3. Cyclotomic fields

Cyclotomic fields are those of the form $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/m}$ is a primitive, complex mth root of unity. We'll consider those of the form $m = p > 2$ with p prime.

Theorem S4. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. *Equivalently, the polynomial*

$$f(t) = t^{p-1} + t^{p-2} + \ldots + t + 1$$

is irreducible (and hence the minimal polynomial of ζ).

Proof. By the formula for a geometric sum,

$$f(t+1) = \frac{(t+1)^p - 1}{t} = \sum_{r=1}^{p} \binom{p}{r} t^r,$$

which is irreducible by Eisenstein's criterion. □

Theorem S5. *If $K = \mathbb{Q}(\zeta)$ then $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Proof. See Stewart and Tall page 72 or Neukirch page 60. □

Corollary. *The discriminant Δ of $\mathbb{Q}(\zeta)$ is $(-1)^{(p-1)/2}p^{p-2}$.*

Proof. By theorems S2 and S5 we have

$$\Delta = \Delta[1, \zeta, \ldots, \zeta^{p-2}] = (-1)^{(p-1)(p-2)/2} N(Df(\zeta)).$$

We have

$$Df(t) = \frac{(t-1)pt^{p-1} - (t^p - 1)}{(t-1)^2}$$

whence

$$Df(\zeta) = \frac{-p\zeta^{p-1}}{1-\zeta}$$

and so

$$\begin{aligned} N(Df(\zeta)) &= \frac{N(-p)N(\zeta)^{p-1}}{N(1-\zeta)} \\ &= \frac{(-p)^{p-1}}{p} \\ &= p^{p-2}. \end{aligned}$$

□

4. Factorisation into irreducibles

Definition 2. Given a ring R,

(1) we say $x \in R$ is irreducible if and only if $x = mn$ implies m or n is a unit;
(2) we say $p \in R$ is prime if and only if p is not a unit or zero, and $p \mid mn$ implies $p \mid m$ or $p \mid n$.

Every prime is irreducible, but not necessarily vice versa. We often denote the units of a ring R by $U(R)$ or, if the ring is clear from the context, then just U.

Definition 3. An integral domain D is called noetherian if one of the following holds:

(1) every ideal in D is finitely generated;
(2) (the ascending chain condition) if $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ are all ideals then there exists $N \in \mathbb{N}$ such that $I_n = I_N$ for every $n \geqslant N$;
(3) (maximality condition) every nonempty set of ideals of D has a maximal element by inclusion.

Theorem S6. *If D is noetherian then every nonzero element can be written as a product of irreducible elements.*

Proof. Exercise. Hints: proceed by contradiction and let

$$X = \{x \in D \backslash U \mid x \text{ cannot be expressed as a product of irreducible elements}\} \subset D.$$

Consider the ideals (x) with $x \in X$, and choose the maximal one – which we can do since D is noetherian. Note that x is not irreducible since it is in X so write $x = yz$ for non-units y and z and consider the ideals (y) and (z). Show these aren't in X and hence derive a contradiction to $x \in X$. $\square$

Theorem S7. *For any number field K the ring $\mathcal{O}_K$ is noetherian.*

Proof. Let $I \subseteq \mathcal{O}_K$ be an ideal. As an additive group $\mathcal{O}_K$ is free abelian of rank $n = [K : \mathbb{Q}]$, so the subgroup $(I, +)$ is free abelian of rank $s \leqslant n$. If $\{x_1, \dots, x_s\}$ is a $\mathbb{Z}$-basis for $(I, +)$ then $I = (x_1, \dots, x_s)$, so I is finitely generated and hence $\mathcal{O}_K$ is noetherian. $\square$

Corollary. *Factorisation into irreducibles is possible in $\mathcal{O}_K$ for any number field K.*