Algebraic Number Theory – Lecture 6

Andrew Potter

"It was mentioned on CNN that the new prime number discovered recently is four times bigger then the previous record."

– John Blasik

1. Setting

Throughout, let k be a number field of degree n. Recall that $\mathcal{O}_k$ is a Dedekind domain, in particular it has unique factorisation of ideals. That is, each ideal $\mathfrak{a} \subset \mathcal{O}_k$ factorises uniquely as a product of prime ideals. So, in some sense, "ideals take the place of rational integers".

Definition. Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_k$ be ideals. Their greatest common divisor, $\gcd(\mathfrak{a}, \mathfrak{b})$, is the ideal $\mathfrak{g}$ with the properties

(1) $\mathfrak{g} \mid \mathfrak{a}$ and $\mathfrak{g} \mid \mathfrak{b}$;
(2) if $\mathfrak{g}'$ satisfies (1) then $\mathfrak{g}' \mid \mathfrak{g}$.

Similarly, their least common multiple, $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b})$, is the ideal $\mathfrak{l}$ satisfying

(1) $\mathfrak{a} \mid \mathfrak{l}$ and $\mathfrak{b} \mid \mathfrak{l}$;
(2) if $\mathfrak{l}'$ satisfies (1) then $\mathfrak{l} \mid \mathfrak{l}'$.

We have the useful properties

- $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$
- $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$.

Let $\mathfrak{a} \subset \mathcal{O}_k$ be an ideal and $b \in \mathcal{O}_k$. We write $\mathfrak{a} \mid b$ to mean $\mathfrak{a} \mid (b)$, the principal ideal generated by b. Then

$$\mathfrak{a} \mid b \quad \Leftrightarrow \quad b \in \mathfrak{a}.$$

This notation is useful because if $\mathfrak{p}$ is a prime ideal then

$$\mathfrak{p} \mid ab \quad \Rightarrow \quad \mathfrak{p} \mid a \text{ or } \mathfrak{p} \mid b.$$

What about non-principal ideals?

Theorem 1. *Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}_k$ and let β be an element of $\mathfrak{a}$. Then there exists $\alpha \in \mathcal{O}_k$ such that $\mathfrak{a} = (\alpha, \beta)$.*

2. Norms

Recall that if $\alpha \in k$ and σ_i are the n embeddings $k \hookrightarrow \mathbb{C}$ then we define

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Definition. The norm of an ideal $\mathfrak{a} \subset \mathcal{O}_k$ is

$$N(\mathfrak{a}) = \left| \mathcal{O}_k / \mathfrak{a} \right|.$$

This is always a finite number, as seen in Dan's lecture.

What's the connexion between the norm of an ideal and that of an element?

Theorem 2. (1) *Every ideal $\mathfrak{a} \subset \mathcal{O}_k$, $\mathfrak{a} \neq 0$, has a $\mathbb{Z}$-basis $\{\alpha_1, \dots, \alpha_n\}$.*

(2) $N(\mathfrak{a}) = \left| \dfrac{\Delta[\alpha_1, \dots, \alpha_n]}{\Delta} \right|^{1/2}$ *where Δ is the discriminant of k.*

Corollary. *If $\mathfrak{a} = (a)$ then $N(\mathfrak{a}) = |N(a)|$.*

The main, useful property of norms is their multiplicativity:

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

But other interesting properties include:

(1) if $N(\mathfrak{a})$ is prime then $\mathfrak{a}$ is a prime ideal;
(2) $N(\mathfrak{a}) \in \mathfrak{a}$, i.e. $\mathfrak{a} \mid N(\mathfrak{a})$;
(3) if $\mathfrak{a}$ is a prime ideal then $N(\mathfrak{a}) = p^m$ for some $m \leqslant n$. Moreover, $\mathfrak{a}$ divides exactly one p, so exactly one prime $p \in \mathbb{Z}$ is in $\mathfrak{a}$.

Thus norms are very handy for finding ideal factorisations. They also have several useful finiteness properties:

(1) Every nonzero ideal of $\mathcal{O}_k$ has finitely many divisors.
(2) A nonzero rational integer belongs to only a finite number of ideals of $\mathcal{O}_k$.
(3) Only finitely many ideals of $\mathcal{O}_k$ have a given norm.

3. Unique factorisation

Let R be a ring. A principal ideal domain is always a unique factorisation domain: PID $\Rightarrow$ UFD. But, in general, UFD $\not\Rightarrow$ PID. However:

Theorem 3. *$\mathcal{O}_k$ is a UFD if and only if it is a PID.*

Proof. ($\Leftarrow$) This implication is always true for rings.

($\Rightarrow$) Because of unique factorisation of ideals we only need to show that every prime ideal is principal. Let $\mathfrak{p}$ be a prime ideal. There exists $N = N(\mathfrak{p})$ such that $\mathfrak{p} \mid N$. $\mathcal{O}_k$ is a UFD by assumption so $N = \pi_1 \cdots \pi_s$ for π_i irreducible in $\mathcal{O}_k$. But

$\mathfrak{p} \mid N$ so $\mathfrak{p} \mid \pi_1 \cdots \pi_s$, hence $\mathfrak{p} \mid \pi_i$ for some i, after relabeling we may assume $i = 1$. Now, π_1 is irreducible and $\mathcal{O}_k$ is a UFD so π_1 is a prime element of $\mathcal{O}_k$. Thus (π_1) is a prime ideal, so $\mathfrak{p} = (\pi_1)$, so every prime ideal is principal. $\square$

4. The class group: a preview

Recall that the fractional ideals form an abelian group $\mathcal{F}$. The principal fractional ideals form a subgroup $\mathcal{P}$ that is normal since $\mathcal{F}$ is abelian. Let $\mathcal{H} = \mathcal{F}/\mathcal{P}$, and call $\mathcal{H}$ the class group. Let $h = |\mathcal{H}|$, then h is called the class number. If $h = 1$ then every ideal is principal and hence $\mathcal{O}_k$ is a UFD, and by the previous theorem, if $\mathcal{O}_k$ is a UFD then every ideal is principal and $h = 1$. So the class number somehow measures by how much unique factorisation fails.