Algebraic Number Theory – Lecture 16

Lee Butler

"It is impossible to travel faster than the speed of light, and certainly not desirable, as one's hat keeps blowing off."

– Woody Allen

1. Numbers, units, and ideals

Algebraic number theory is first and foremost the study of algebraic numbers using algebra, analysis, and other, funkier stuff.

Definition. An (*algebraic*) *number field* K is a field extension $K \supset \mathbb{Q}$ such that the degree $[K : \mathbb{Q}]$ is finite. Elements of a number field are called *algebraic numbers*.

A number $\alpha \in \mathbb{C}$ is algebraic if and only if there is an irreducible, monic polynomial $0 \neq f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. This f is unique and called the minimal polynomial of α. If $f \in \mathbb{Z}[x]$ then α is called an algebraic integer.

The algebraic integers form a ring $\mathcal{O}$. Given a number field K the algebraic integers in K also form a ring, the *ring of integers of* K, $\mathcal{O}_K$.

Definition. The units in $\mathcal{O}_K$, $\mathcal{O}_K^\times$, are elements $u \in \mathcal{O}_K$ such that $uv = 1$ for some $v \in \mathcal{O}_K$.

In $\mathbb{Z}$ we can factorise numbers uniquely into primes, in the ring of integers of number fields this is not the case in general. But it is the case for ideals.

Definition. An ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is an abelian subgroup under addition such that $\mathfrak{a}\mathcal{O}_K \subset \mathfrak{a}$. An ideal $\mathfrak{p}$ is called:

- *prime* if whenever $\mathfrak{ab} \subset \mathfrak{p}$, either $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$;
- *maximal* if $\mathfrak{p} \neq \mathcal{O}_K$ and $\mathfrak{p} \subset \mathfrak{p}' \subset \mathcal{O}_K$ implies $\mathfrak{p}' = \mathfrak{p}$ or $\mathfrak{p}' = \mathcal{O}_K$.

Maximal ideals are always prime, and in special integral domains called *Dedekind domains*, every prime ideal is maximal. $\mathcal{O}_K$ is always a Dedekind domain so we can factorise ideals in $\mathcal{O}_K$ into primes.

Definition. An $\mathcal{O}_K$-submodule $\mathfrak{a} \subset K$ is called a *fractional ideal* if there is $c \in \mathcal{O}_K$ with $c \neq 0$ and such that $c\mathfrak{a}$ is an ideal in $\mathcal{O}_K$.

Fractional ideals form an abelian multiplicative group, J_K say, while the principal ideals form a normal subgroup, P_K, of J_K. Their quotient $\mathrm{Cl}_K = J_K/P_K$ is called the class group. It is finite and its size $h = |\,\mathrm{Cl}_K\,|$ is called the class number. It measures the expansion in passing from numbers to ideals, while the group of units measures the contraction in this process. This is captured by the exact sequence

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

2. Conjugates, norms, and traces

A number field K can always be generated over $\mathbb{Q}$ by a single algebraic number θ. If θ has minimal polynomial f of degree d, then the d roots of f are called the *conjugates of* θ. Suppose the conjugates of θ are $\theta_1, \ldots, \theta_d$; these numbers lead to the d distinct embeddings of K into $\mathbb{C}$, $\sigma_i : K \hookrightarrow \mathbb{C}$, given by

$$\sigma_i(\theta) = \theta_i.$$

We can then define the norm and trace of an element $\alpha \in K$ by

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

and

$$Tr(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha).$$

They are both rational numbers.

We can also define the norm of an ideal $\mathfrak{a} \subset \mathcal{O}_K$ by

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| < \infty.$$

3. The big, bad concepts

Definition. Given a number field K, we define the *Dedekind zeta function of* K by

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

The function is defined for $\mathrm{Re}(s) > 1$ and can be analytically continued to all of $\mathbb{C}$ except for a pole at $s = 1$, and the residue of this pole encodes a vast amount of information about K.

A related notion is that of the Dirichlet L-series.

Definition. A Dirichlet character (mod m) is a homomorphism

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \{z \in \mathbb{C} : |z| = 1\}.$$

It extends to a multiplicative function by

$$\chi(n) = \begin{cases} \chi(n \pmod m) & \text{if } \mathrm{hcf}(m,n) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Out of a Dirichlet character we form a *Dirichlet L-series* by

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Both these complex functions are generalisations of the Riemann zeta function (take $K = \mathbb{Q}$ and the "trivial" character $\chi \equiv 1 \pmod 1$ respectively), and are both generalised by *Hecke L-series*.

The Dedekind zeta function encodes a lot of information about the ideals of $\mathcal{O}_K$, but we also want to know about the units. In general they form an infinite group, but we can still get a feel for their size by Dirichlet's unit theorem.

Theorem. *Let $\mu(K)$ denote the set of roots of unity in K, let r and $2s$ be the number of real and pairs of complex embeddings $K \hookrightarrow \mathbb{C}$ respectively. Then*

$$\mathcal{O}_K^\times \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}.$$

What this means is that there are $t = r+s-1$ special units $\varepsilon_1, \ldots, \varepsilon_t$, called fundamental units, such that any unit ε in $\mathcal{O}_K$ can be written

$$\varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$$

for integers ν_i.

Another way of understanding number fields is to study their extensions. A special kind of extension is a Kummer extension.

Definition. Let K be a number field containing the nth roots of unity and $\Delta \subseteq K^\times$. A *Kummer extension of K* is one of the form $K(\sqrt[n]{\Delta})$.

Kummer extensions are important because they correspond to groups intermediate to the nth roots in $K^\times$ and $K^\times$ itself. Specifically we have the following.

Theorem. *There is a bijective correspondence between groups $(K^\times)^n \subseteq \Delta \subseteq K^\times$ and Kummer extensions of K.*

Kummer extensions are always abelian, i.e. Galois with abelian Galois group. The study of abelian extensions is the thrust of class field theory which we'll hopefully learn a lot more about this year.

Another place Galois extensions come in useful is when studying Hilbert's ramification theory. This studies how a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ factorises when considered as an ideal in a larger field $L \supset K$. In general it will factor as

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

for some prime ideals $\mathfrak{P}_i \subset \mathcal{O}_L$ and natural numbers e_i called the ramification indices. If $[L:K] = n$ and we define the inertia degree $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ then we get the fundamental identity

$$\sum_{i=1}^{r} e_i f_i = n.$$

The ideal $\mathfrak{P}_i$ is called unramified if $e_i = 1$, and $\mathfrak{p}$ is called unramified if all the $\mathfrak{P}_i$ are unramified. Otherwise they're called ramified. It turns out only finitely many prime ideals in $\mathcal{O}_K$ ramify in $\mathcal{O}_L$, and they're the divisors of a special ideal in $\mathcal{O}_K$ called the discriminant of the extension. Also surprising is that if the extension is Galois then the ramification indices and inertia degrees are independent of i, that is $e_1 = \ldots = e_r$ and $f_1 = \ldots = f_r$.

4. And more besides

That's a very brief sketch of most of the stuff we looked at last year. In the following year we will delve deeper into class field theory and the theory of valuations, including p-adic numbers, idèles and adèles, and more evil looking complex functions.