Number Fields Revision

Abigail Tan
April 22, 2023

Lecture 1

In this lecture, we motivate the study of number fields. The main theorem here is that if S is finitely generated over R, then S is integral over R. It follows quickly that $\mathcal{O}_L$ is a ring in L.

The integers $\mathbb{Z}$ have a particular structure inside of $\mathbb{Q}$. In this course, for more general fields L, we study the properties of subrings $\mathcal{O}_L \in L$ that behave in L as $\mathbb{Z}$ behaves in $\mathbb{Q}$.

Definitions (Number field and $\mathcal{O}_L$). A number field is a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_L$ be the set of algebraic integers in L.

[Auxiliary definitions]

Theorem. Let $R \subseteq S$ as rings. If S is finitely generated over R, then S is integral over R.
Proof sketch. Take generators $\alpha = 1, \alpha_2, \ldots, \alpha_n$ for S over R. Consider the map $m_s : S \to S$, $x \mapsto sx$, and write $m_s(\alpha_i) = s\alpha_i = \sum b_{ij}\alpha_j$ for some $(b_{ij}) = B$. Check that

$$(sI - B)\begin{pmatrix}\alpha_1 \\ \vdots \\ \alpha_n\end{pmatrix} = 0.$$

Then use $\operatorname{adj}(X)X = \det(X)I$ to get $\det(sI - B) = 0$, which gives a polynomial that s is a root of, so it is integral. □

Lecture 2

This introduces a few results, working towards showing that any number field must have an integral basis.

Proposition. Let $L/\mathbb{Q}$ be a number field. Then $\alpha \in \mathcal{O}_L$ if and only if $N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Proposition. For $L = K(\sqrt{d})$

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \bmod 4 \end{cases}$$

Definition (Integral basis). A basis $\{\alpha_1, \ldots, \alpha_n\}$ of L as a $\mathbb{Q}$-vector space is an integral basis if

$$\mathcal{O}_L = \left\{ \sum_{i=1}^{n} m_i\alpha_i \,\middle|\, m_i \in \mathbb{Z} \right\}.$$

This basically corresponds to $\{\alpha_1, \ldots, \alpha_n\}$ being "a $\mathbb{Q}$-basis for L and a $\mathbb{Z}$-basis for $\mathcal{O}_L$".

Lecture 3
Prove that any number field has an integral basis. Establish the basis-invariant property of the discriminant Δ.

Definition/Proposition (Gram matrix and discriminant). Let $\alpha_1, \ldots, \alpha_n$ be a basis for L/K. Then define

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)).$$

If $\sigma_i : L \to \bar{K}$ are the n distinct K-homomorphisms and S is a matrix with $S_{ij} = \sigma_i(\alpha_j)$, then

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det S)^2.$$

Theorem. Every number field $L/\mathbb{Q}$ has an integral basis.
Proof sketch. It's quick to check there exists a basis $\{\alpha_i\}$ in $\mathcal{O}_L$. Pick one with $|\Delta(\alpha_1, \ldots, \alpha_n)|$ minimal. Then write $x \in \mathcal{O}_L$ in terms of these, suppose a coefficient isn't an integer, then get a contradiction of minimality using $\Delta(\alpha'_1, \ldots, \alpha'_n) = (\det A)^2 \Delta(\alpha_1, \ldots, \alpha_n)$. □

Remark. Note that Δ is effectively a function of a basis, and determined by L (L determines $\{\sigma_i\}$, which determines S and hence Δ). A basis corresponding to minimal Δ is integral (recall the idea of "algebraic" really meaning "finite", from lectures).

It follows quickly that $\Delta(\alpha_1, \ldots, \alpha_n)$ is independent of the choice of integral basis, so we define this as the discriminant D_L of L.

Lecture 4-5 (and end of lecture 3)
We want to measure the failure of unique factorisation by studying (products of) ideals. It turns out that in a number field, every ideal factors uniquely into a product of prime ideals.

Definition (Product of ideals). Let $\mathfrak{a}, \mathfrak{b} \triangleleft \mathcal{O}_L$. Define product $\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i b_i \middle| a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$.

Proposition. For K a number field, $\mathcal{O}_K$ is a Dedekind domain, i.e.
(i) $\mathcal{O}_K$ is an integral domain
(ii) $\mathcal{O}_K$ is a Noetherian ring
(iii) if $x \in K$ is integral over $\mathcal{O}_K$ then $x \in \mathcal{O}_K$
(iv) every nonzero prime ideal is maximal (Krull dimension of 1).

Proposition (Containment and division). Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Then $\mathfrak{b} | \mathfrak{a}$ if and only if $\mathfrak{a} \subseteq \mathfrak{b}$.

Theorem. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ be a nonzero ideal. Then $\mathfrak{a}$ can be written uniquely as a product of prime ideals.

Corollary. The nonzero fractional ideals form a group I_k under multiplication (a free abelian group generated by the prime ideals $\mathfrak{p}$). Observe that $K^* \to I_K$, $\alpha \mapsto \langle \alpha \rangle$ is a group homomorphism, with kernel ${\mathcal{O}_K}^*$. The image of this homomorphism is the principal ideals p_k.

Definition. The class group Cl_K of K is $\mathrm{Cl}_K = I_k / p_k$.

Theorem. The following are equivalent: (i) $\mathcal{O}_K$ is a PID, (ii) $\mathcal{O}_K$ is a UFD, (iii) Cl_K is trivial.

Lecture 6

Start working with norms of ideals, working towards Dedekind's criterion and factorisation of principal ideals.

Definition (Norm of ideal). Let $[L:\mathbb{Q}] = n$ and $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ be an ideal. Then $N(\mathfrak{a}) = |\mathcal{O}_L/\mathfrak{a}|$.

Lemma (Pre-Dedekind lemmas).
(i) If $\alpha \in \mathcal{O}_L$ with $\alpha \neq 0$, then $N(\langle\alpha\rangle) = |N_{L/\mathbb{Q}}(\alpha)|$
(ii) Let $\mathfrak{p} \trianglelefteq \mathcal{O}_L$ be a prime ideal, then $\exists! p \in \mathbb{Z}$ prime s.t. $\mathfrak{p} | \langle p \rangle = p\mathcal{O}_L$
This shows that every prime ideal in $\mathcal{O}_L$ is a factor of some $p\mathcal{O}_L = \langle p \rangle$, p a prime.

Lecture 7-8

State and work with Dedekind's criterion for factorising principal ideals.

Theorem (Dedekind's criterion). Let $\alpha \in \mathcal{O}_L$ with minimal polynomial $g(x) \in \mathbb{Z}[x]$. Suppose $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ has finite index coprime to p i.e. $|\mathcal{O}_L/\mathbb{Z}[\alpha]| < \infty$ and $p \nmid |\mathcal{O}_L/\mathbb{Z}[\alpha]|$. Let $\bar{g}(x) = g(x) \pmod p$ factorise over $F_p(x)$ into irreducibles as $\bar{g}(x) = \bar{\phi}_1^{e_1} \dots \bar{\phi}_r^{e_r}$. Then $\langle p \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i = \langle p, \phi_i(\alpha) \rangle$ are such that ϕ_i reduces to $\bar{\phi}_i$ mod p.

Definition. Let $\langle p \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. Then we say p ramifies if some $e_i > 1$, p is inert if $r = 1 = e_1$, and p splits if $r = [L:\mathbb{Q}]$ and all $e_i = 1$.

Lemma. 2 ramifies in L iff $d \equiv 2$ or 3 mod 4, 2 is inert iff $d \equiv 5$ mod 8, and 2 splits iff $d \equiv 1$ mod 8.

Lecture 9

Use Minkowski's lemma and the geometry of numbers to establish the finiteness of the class group.

Work with the lattice $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 \subseteq \mathbb{R}^2$. If $v_i = a_i e_1 + b_i e_2$, then let $A(\Lambda) = \left|\det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}\right|$.

Lemma (Minkowski's lemma). Let a closed disc S centred on 0 have area at least $4A(\Lambda)$. Then S contains a nonzero point of Λ.
(In particular, $\exists \alpha \in \Lambda$ with $0 < |\alpha|^2 \leq 4A(\Lambda)/\pi$.)

Lemma. $A(\mathcal{O}_L) = \frac{1}{2}\sqrt{|D_L|}$ and $A(\mathfrak{a}) = N(\mathfrak{a})A(\mathcal{O}_L)$.
(This follows from checking $A(\mathfrak{a}) = \frac{1}{2}|\Delta(\alpha_1, \alpha_2)|^2$ where α_1, α_2 are an integral basis for $\mathfrak{a}$.)

Sketch for the next theorem. To prove that the class group is finite, we use Minkowski's lemma to show that any element of the class group C_L has an ideal representative of smaller norm than some constant C_L which depends only on L itself.

Theorem. The class group Cl_L is finite and is generated by the class of prime ideals dividing $\langle p\rangle$ for some prime $p < 2\sqrt{|D_L|}/\pi =: C_L$.

Proof sketch. Minkowski's lemma implies there is some $0 \neq \alpha \in \alpha$ with $N(\alpha) \leq 4A(\mathfrak{a})/\pi =: N(\mathfrak{a})C_L$. But $\alpha \in \mathfrak{a}$ so $\langle\alpha\rangle \subseteq \mathfrak{a}$ so for some ideal $\mathfrak{b}$, $\langle\alpha\rangle = \mathfrak{a}\mathfrak{b}$.
Hence $N(\alpha) = N(\langle\alpha\rangle) = N(\mathfrak{a})N(\mathfrak{b})$ so $N(\mathfrak{b}) \leq C_L$ by the Minkowski result. Therefore $[\mathfrak{b}] = [\mathfrak{a}^{-1}] \in \mathrm{Cl}_L$.
Replacing $\mathfrak{a}$ with $\mathfrak{a}^{-1}$ we've shown that for *all* $[\mathfrak{a}] \in \mathrm{Cl}_L$, there is a representative $\mathfrak{b}$ of $[\mathfrak{a}]$ with

$$N(\mathfrak{b}) \leq \frac{2\sqrt{|D_L|}}{\pi} = C_L.$$

But for all $m \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ in $\mathcal{O}_L$ with $N(\mathfrak{a}) = m$. □