B3.4 Algebraic Number Theory: Condensed version.

This document contains the basic definitions and results from the course, in condensed form with no examples or proofs. It should be more-or-less sufficient for attempting the example sheets. Of course, you can refer to the full notes if you need to.

Chapter 1: Algebraic numbers

Algebraic numbers. Minimal polynomials.

- A complex number α is *algebraic* if it is the solution to some polynomial equation with coefficients in $\mathbb{Q}$. The set of all algebraic numbers is denoted by $\overline{\mathbb{Q}}$.
- Suppose that $\alpha \in \overline{\mathbb{Q}}$. Then there is a unique nonzero monic irreducible polynomial $m_\alpha(X)$ satisfied by α, which we call the *minimal polynomial* of α. If $f \in \mathbb{Q}[X]$ is any other polynomial satisfied by α then $m_\alpha | f$.
- Let $\alpha \in \mathbb{C}$. Then α is algebraic if, and only if, $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$. Suppose that α *is* algebraic. Then $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. Suppose that m_α, the minimal polynomial for α, has degree n. Then a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$ is $1, \alpha, \ldots, \alpha^{n-1}$, that is to say $\mathbb{Q}(\alpha)$ may be identified with the polynomials in α of degree $< n$, and hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m_\alpha = n$.
- Suppose that α satisfies an equation of degree n over $\mathbb{Q}$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant n$.
- Suppose that α, β are algebraic. Then $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leqslant [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]$. The algebraic numbers $\overline{\mathbb{Q}}$ are a field.

Number fields.

- A *number field* K is a subfield of $\mathbb{C}$ which is a finite degree extension of $\mathbb{Q}$.
- Let $\alpha \in \mathbb{C}$. Then α is algebraic if and only if it lies in some number field K.
- (Primitive element theorem) Every number field K is of the form $\mathbb{Q}(\theta)$ for some algebraic number θ.
- Quadratic fields: every field of degree 2 over $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{d})$ for d a squarefree integer (not necessarily positive). These fields are all distinct.

Conjugates and embeddings.

- Suppose that α is an algebraic number with minimal polynomial m_α of degree n. Then the roots of m_α are called the *conjugates* of α. The conjugates are distinct.

- An *embedding* $\sigma : K \to \mathbb{C}$ is a(n injective) field homomorphism.
- Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. Then any embedding $\sigma : K \to \mathbb{C}$ maps θ to one of its conjugates θ_i. Conversely, for each i there is a unique embedding $\sigma_i : K \to \mathbb{C}$ with $\sigma(\theta) = \theta_i$. In particular, K has exactly n distinct embeddings. We will always denotes them $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$, with σ_1 being the identity.

Norm.

- If $\alpha \in K$, we define the *norm* $\mathbf{N}_{K/\mathbb{Q}}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha)$.
- Basic facts: $\mathbf{N}_{K/\mathbb{Q}}(\alpha\beta) = \mathbf{N}_{K/\mathbb{Q}}(\alpha)\mathbf{N}_{K/\mathbb{Q}}(\beta)$, $\mathbf{N}_{K/\mathbb{Q}}(\gamma) = 0$ if and only if $\gamma = 0$; $\mathbf{N}_{K/\mathbb{Q}}(q) = q^n$ for $q \in \mathbb{Q}$
- The norm takes values in $\mathbb{Q}$.
- $\mathbf{N}_{K/\mathbb{Q}}(\alpha)$ is the determinant of the multiplication-by-α map as a linear map.

Trace.

- If $\alpha \in K$, we define the *trace* $\mathbf{N}_{K/\mathbb{Q}}(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha)$.
- The trace takes values in $\mathbb{Q}$.

Discriminants.

- Let $e_1, \ldots, e_n$ be a basis for K over $\mathbb{Q}$. Then we define the *discriminant* $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n)$ to be $(\det M)^2$, where $M = M(e_1, \ldots, e_n)$ is the matrix with $M_{ij} = \sigma_i(e_j)$.
- $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n) \neq 0$.
- We have $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n) = \det((\mathrm{tr}_{K/\mathbb{Q}}(e_i e_j)_{i,j})$.
- Consequently, $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n) \in \mathbb{Q}$.
- Suppose that $e_1, \ldots, e_n$ and $e'_1, \ldots, e'_n \in K$ are related by $e'_j = \sum_k A_{kj} e_k$, where the matrix A has rational entries. Then

$$\mathrm{disc}_{K/\mathbb{Q}}(e'_1, \ldots, e'_n) = (\det A)^2 \, \mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n).$$

Chapter 2: Algebraic integers

Algebraic integers.

- Suppose that $\alpha \in \overline{\mathbb{Q}}$ is an algebraic number. Then α is an *algebraic integer* if it satisfies a *monic* polynomial in $\mathbb{Z}[X]$. The set of algebraic integers is denoted by $\mathcal{O}$.
- Let α be an algebraic number. Then α is an algebraic integer if and only if its minimal polynomial m_α has integer coefficients. In particular, a rational number is an algebraic integer if and only if it is an integer, that is to say $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.
- The algebraic integers $\mathcal{O}$ form a ring.

- Suppose that $\alpha \in \overline{\mathbb{Q}}$. Then some integer multiple of α is an algebraic integer.
- Let K be a number field. $\mathcal{O}_K := \mathcal{O} \cap K$.
- Let $\sigma_1, \ldots, \sigma_n \to \mathbb{C}$ be the embeddings of K. Suppose that $\alpha \in \mathcal{O}_K$. Then $\sigma_i(\alpha)$ is an algebraic integer.
- If $\alpha \in \mathcal{O}_K$ then $\mathbf{N}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.
- Suppose that $e_1, \ldots, e_n \in \mathcal{O}_K$. Then $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n) \in \mathbb{Z}$.

Units.

- Let K be a number field, and $\mathcal{O}_K$ its ring of integers. Note that $\mathcal{O}_K$ (being contained in a field) is an integral domain. A *unit* is an element u for which there is $v \in \mathcal{O}_K$ with $uv = 1$. Equivalently, the inverse u^{-1} (in the field K) in fact lies in $\mathcal{O}_K$. It is easy to see that the units form a group under multiplication. We will sometimes write $U(\mathcal{O}_K)$ for the group of units in $\mathcal{O}_K$.
- $u \in \mathcal{O}_K$ is a unit if and only if $\mathbf{N}_{K/\mathbb{Q}}(u) = \pm 1$.

Integral bases. Theorem: Suppose K has degree n. Then $\mathcal{O}_K$ is a *free abelian group of rank* n, by which we mean that there are $e_1, \ldots, e_n$ such that $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}e_i$ (that is, the e_i lie in $\mathcal{O}_K$ and every element of $\mathcal{O}_K$ is an integer combination of the e_i in precisely one way). In this situation, $e_1, \ldots, e_n$ is called an *integral basis* for $\mathcal{O}_K$.

Discriminant of a number field. $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n)$ does not depend on the choice of integral basis $e_1, \ldots, e_n$, and therefore it is an invariant of the number field. It is called the discriminant of K and denoted Δ_K.

Quadratic fields. Let $K = \mathbb{Q}(\sqrt{d})$, $d \neq 1$ squarefree. The we have the following proposition. An integral basis for K is given by

- 1 and $\sqrt{d}$ if $d \equiv 2, 3 (\mathrm{mod}\, 4)$;
- 1 and $\frac{1}{2}(1 + \sqrt{d})$ if $d \equiv 1 (\mathrm{mod}\, 4)$.

The discriminant Δ_K is given as follows:

- $4d$ if $d \equiv 2, 3 (\mathrm{mod}\, 4)$;
- d if $d \equiv 1 (\mathrm{mod}\, 4)$.

Computing an integral basis. The following lemma is useful. Suppose that K is a number field and that $e_1, \ldots, e_n$ are elements of $\mathcal{O}_K$, independent over $\mathbb{Q}$, which do not form an integral basis. Then there exists a prime p with $p^2 | \mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n)$ and integers $m_1, \ldots, m_n \in \{0, \ldots, p-1\}$, not all zero, such that $\frac{1}{p}(m_1 e_1 + \cdots + m_n e_n) \in \mathcal{O}_K$. In particular, if $e_1, \ldots, e_n \in \mathcal{O}_K$ and $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n)$ is nonzero and squarefree, $e_1, \ldots, e_n$ are an integral basis for $\mathcal{O}_K$.

Chapter 3: Irreducibles and factorisation

- An element $x \in \mathcal{O}_K$ is *irreducible* if it is not a unit and if, whenever $x = yz$ with $y, z \in \mathcal{O}_K$, then one of y, z is a unit.
- Every $x \in \mathcal{O}_K$ may be factored into irreducibles in at least one way.
- $\mathcal{O}_K$ is a *unique factorisation domain* (UFD) if factorisation into irreducibles is unique, up to units and ordering of the factors.
- $\mathcal{O}_K$ is a UFD for various small examples such as $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$, but need not be in general. For instance, $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ is not a UFD.

Chapter 4: Ideals and their basic properties

Ideals.

- An ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is a subset which is a subgroup under addition, and which is closed under multiplication by elements of $\mathcal{O}_K$. We will sometimes write $\text{Ideals}(\mathcal{O}_K)$ for the set of ideals in $\mathcal{O}_K$. Given $\alpha \in \mathcal{O}_K$, we may form the *principal ideal* $(\alpha) := \{\alpha x : x \in \mathcal{O}_K\}$.
- The map $\iota : \mathcal{O}_K \to \text{Ideals}(\mathcal{O}_K)$ which associates $\alpha \in \mathcal{O}_K$ to the principal ideal (α) is "an embedding up to units". (More precisely, ι induces an injective map $\mathcal{O}_K/U(\mathcal{O}_K) \to \text{Ideals}(\mathcal{O}_K)$.)
- If the map $\iota : \mathcal{O}_K \to \text{Ideals}(\mathcal{O}_K)$ is surjective, that is to say if every ideal is a principal ideal, then $\mathcal{O}_K$ is said to be a principal ideal domain (PID). (Groups, Rings and Modules) A PID is a UFD, but the converse is not true in general.
- (Chapter 6) The converse *is* true in number fields: if $\mathcal{O}_K$ is a UFD, then it is a PID.

Basic properties.

- Let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_K$. Then $\mathfrak{a}$ contains a non-zero rational integer a, and thus the principal ideal (a) is contained in $\mathfrak{a}$.
- Let $\mathfrak{a}$ be a nonzero ideal. Then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite. In particular, $\mathfrak{a}$ is a finite-index $\mathbb{Z}$-submodule of $\mathcal{O}_K$.
- Every nonzero ideal $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

Norms of ideals.

- Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$. Then we define the norm $N(\mathfrak{a})$ to be $|\mathcal{O}_K/\mathfrak{a}|$.
- Suppose that $\mathfrak{a} = (\alpha)$ is a principal ideal, for some $\alpha \in \mathcal{O}_K \setminus \{0\}$. Then $N(\mathfrak{a}) = |\mathbf{N}_{K/\mathbb{Q}}(\alpha)|$.
- (Chapter 7) For any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ we have $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.
- (Chapter 7) For any ideal $\mathfrak{a}$ we have $\mathfrak{a}|(N(\mathfrak{a}))$.

Multiplying ideals. Prime ideals.

- Let $\mathfrak{a}, \mathfrak{b}$ be ideals in $\mathcal{O}_K$. Then we define the product $\mathfrak{ab}$ to consist of all finite sums $\sum_{i=1}^{k} a_i b_i$ with $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Let $\mathfrak{a}, \mathfrak{b}$ be two ideals in $\mathcal{O}_K$. Then we say that $\mathfrak{b}|\mathfrak{a}$ if there is an ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{bc}$.
- If $\mathfrak{b}|\mathfrak{a}$ then $\mathfrak{a} \subseteq \mathfrak{b}$. (The converse is also true: see Chapter 5.)
- An ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is prime if it is not $\mathcal{O}_K = (1)$, and if $xy \in \mathfrak{p}$ implies that either x or y lies in $\mathfrak{p}$.
- An ideal $\mathfrak{p}$ is prime if and only if the following is true: whenever $\mathfrak{ab} \subseteq \mathfrak{p}$, either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.
- In $\mathcal{O}_K$, all prime ideals are maximal. In particular, if $\mathfrak{p}$ and $\mathfrak{q}$ are two prime ideals with $\mathfrak{p} \subseteq \mathfrak{q}$, then $\mathfrak{p} = \mathfrak{q}$.

Chapter 5: Unique factorisation into prime ideals

Theorem: Let K be a number field with ring of integers $\mathcal{O}_K$. Then any non-zero proper ideal $\mathfrak{a}$ admits a unique factorisation $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ into prime ideals.

Other related facts about ideals in $\mathcal{O}_K$.

- ("Inverses") $\mathfrak{a} \subset \mathfrak{b}$ if and *only if* $\mathfrak{b}|\mathfrak{a}$.
- (Containment is the same as division) Let $\mathfrak{a}$ be an ideal. Then there is an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal.
- (Cancellation) Suppose that $\mathfrak{ac} = \mathfrak{ac}'$. Then $\mathfrak{c} = \mathfrak{c}'$.
- Let $\mathfrak{p}$ be a prime ideal, and suppose that $\mathfrak{p}|\mathfrak{ab}$. Then $\mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$.
- Every prime ideal $\mathfrak{p}$ occurs as the prime factor of a unique (p), where p is some rational prime.

Chapter 9: Factoring into prime ideals in practice

Let p be a rational prime. Suppose $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ for *distinct* prime ideals $\mathfrak{p}_i$ and positive integer exponents e_i. Each $N(\mathfrak{p}_i)$ must equal some power p^{f_i} of p. We have $n = \sum_{i=1}^{r} e_i f_i$.

Basic language:

- If $r = n$ (so all the e_i, f_i are equal to 1), p is said to *split completely* in K.
- If $e_i > 1$ for some i then p is said to *ramify*.
- If $r = 1$ and $e_1 = n$ (so $f_1 = 1$) then p is said to be *totally ramified* in K.
- If $r = 1$ and $e_1 = 1$ (so $f_1 = n$) then p is said to be *inert* in K. In this case (p) is itself a prime ideal.

Dedekind's lemma: Let K be a number field of degree n. Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α. Let $m(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α. Let $\overline{m}(X) \in \mathbb{F}_p[X]$ be the reduction of m mod p, and suppose that this factors into distinct irreducible polynomials (over $\mathbb{F}_p$) as $\overline{g}_1(X)^{e_1} \cdots \overline{g}_r(X)^{e_r}$, where the $\overline{g}_i(X)$ are distinct. Then the factorisation of (p) into distinct prime ideals is $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i = (p, g_i(\alpha))$, and here g_i is an arbitrary lift of $\overline{g}_i$ to $\mathbb{Z}[X]$. Moreover, $N(\mathfrak{p}_i) = p^{\deg \overline{g}_i}$.

Strategy for factoring a general ideal $\mathfrak{a}$.

- Pick some $\alpha \in \mathfrak{a}$. Then $\mathfrak{a}|(\alpha)$. Since $(\alpha)|(\mathbf{N}_{K/\mathbb{Q}}(\alpha))$, we have $\mathfrak{a}|(m)$ where $m = \mathbf{N}_{K/\mathbb{Q}}(\alpha)$ is a rational integer.
- Factor m into rational primes p_i, then apply Dedekind's lemma to each (p_i).
- We now have a prime ideal factorisation of a multiple of $\mathfrak{a}$. Now figure out which of these prime ideals actually occur as divisors of $\mathfrak{a}$.

Chapter 10: The class group

Definitions and key facts.

- Suppose that $\mathfrak{a}, \mathfrak{b}$ are ideals in $\mathcal{O}_K$. We write $\mathfrak{a} \sim \mathfrak{b}$ if there are principal ideals $(x), (y)$ such that $\mathfrak{a}(x) = \mathfrak{b}(y)$. This is an equivalence relation.
- The *ideal class group* $\mathrm{Cl}(K)$ is $\mathrm{Ideals}(\mathcal{O}_K)/\sim$. Equivalence classes are denoted by square brackets $[\mathfrak{a}]$, and these are called *ideal classes*. Note that all principal ideals lie in the same class.
- The product operation on ideals descends to give a well-defined product on ideal classes, thus $[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{ab}]$. This turns $\mathrm{Cl}(K)$ into a group, called the *ideal class group* of K.
- $\mathrm{Cl}(K)$ is trivial if and only if $\mathcal{O}_K$ is a PID (if and only if $\mathcal{O}_K$ is a UFD).
- The class group is finite. $h_K := |\mathrm{Cl}(K)|$ is called the *class number* of K.

The Minkowski constant M_K. Let K be a number field with embeddings $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$. Write r_1 for the number of real embeddings $\sigma_i : K \to \mathbb{C}$, and r_2 the number of pairs of conjugate complex embeddings $\sigma_i \to \mathbb{C}$. (An embedding is deemed real if its image is contained in $\mathbb{R}$, and complex otherwise). Note that $r_1 + 2r_2 = n$. Then we define the *Minkowski constant*

$$M_K := (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|},$$

where Δ_K is the discriminant of K.

The Minkowski constant for quadratic fields. Let $\mathbb{Q}(\sqrt{d})$, $d \neq 1$ a squarefree integer, be a quadratic field. Then M_K is given as follows:

(i) If $d > 0$ and $d \equiv 2, 3 (\mathrm{mod}\, 4)$, $M_K = \sqrt{d}$;

(ii) If $d > 0$ and $d \equiv 1 (\mathrm{mod}\, 4)$, $M_K = \frac{1}{2}\sqrt{d}$;
(iii) If $d < 0$ and $d \equiv 2, 3 (\mathrm{mod}\, 4)$, $M_K = \frac{4}{\pi}\sqrt{|d|}$;
(iv) If $d < 0$ and $d \equiv 1 (\mathrm{mod}\, 4)$, $M_K = \frac{2}{\pi}\sqrt{|d|}$.

Minkowski bound. Let K be a number field with Minkwoski constant M_K. Then every class in $\mathrm{Cl}(K)$ contains an ideal $\mathfrak{a}$ with $N(\mathfrak{a}) \leqslant M_K$. Thus $\mathrm{Cl}(K)$ is generated by (the identity and) the prime ideals $\mathfrak{p}$ dividing the principal ideals (p), where p is a rational prime of size at most M_K.

General procedure for computing class groups.

- Observe the basic features of K (ring of integers, integral basis, discriminant etc) and write down the Minkowski constant M_K. By the Minkowski bound, generators for $\mathrm{Cl}(K)$ may be found amongst the prime ideal divisors of (p), $p \leqslant M_K$.
- Factor all of the ideals (p), where $p \leqslant M_K$ is a rational prime, using Dedekind's lemma. This will give an explicit list of prime ideals generating $\mathrm{Cl}(K)$.
- Figure out what relations there are, in the ideal class group, between the prime ideals generated in this way (this can often be more an art than a science).
- See Chapter 11 for further discussion and many examples.