Part II Number Fields

Tom Fisher

Lent 2012
Contents

1 Algebraic Numbers & Algebraic Integers 3
2 Ideals 12
3 The Class Group & Units 21
4 Cyclotomic Fields 32
5 Acknowledgements 35
1 Algebraic Numbers & Algebraic Integers

Definition

\( \alpha \in \mathbb{C} \) is an algebraic number if \( f(\alpha) = 0 \) for some nonzero polynomial \( f \in \mathbb{Q}[X] \).

It is an algebraic integer if, furthermore \( f \in \mathbb{Z}[X] \) and \( f \) is monic.

Lemma 1.1

If \( \alpha \in \mathbb{Q} \) then \( \alpha \) is an algebraic integer if and only if \( \alpha \in \mathbb{Z} \).

Remark

Sometimes the phrase ‘algebraic integer’ is abbreviated to just ‘integer’; to avoid confusion, we will refer to elements of \( \mathbb{Z} \) as ‘rational integers.’

Remark

Let \( R \subseteq S \) be rings and \( \alpha_1, \ldots, \alpha_m \in S \). Then we write \( R[\alpha_1, \ldots, \alpha_m] \) to denote the subring of \( S \) generated \( R \) and \( \alpha_1, \ldots, \alpha_m \).

Theorem 1.2

The algebraic numbers form a field.

Theorem 1.3

The algebraic integers form a ring.

Lemma 1.4

Let \( R \subseteq S \) be rings. Suppose \( S \) is finitely generated as an \( R \)-module, so that for some finite subset of \( S \), each element of \( S \) is an \( R \)-linear combination of elements of this subset.
Then every \( x \in S \) is integral over \( R \), by which we mean that
\[
x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0
\]
for some \( a_0, \ldots, a_{n-1} \in R \).

**Definition**

Let \( L/K \) be a field extension. The *minimal polynomial* of \( \alpha \in L \) over \( K \) is the monic polynomial \( g \) of least degree such that \( g(\alpha) = 0 \).

**Recall**

\( g \) is unique and irreducible.

**Proposition 1.5**

Let \( \alpha \in \mathbb{C} \) be algebraic with minimal polynomial \( g \) over \( \mathbb{Q} \). Then:

(i) For \( f \in \mathbb{Q}[X] \), \( f(\alpha) = 0 \Leftrightarrow g|f \);

(ii) \( \alpha \) is an algebraic integer \( \Leftrightarrow g \in \mathbb{Z}[X] \).

**Definition**

A field extension \( L/K \) is *finite* if \( L \) is finite-dimensional as a \( K \)-vector space. The *degree* of \( L \) over \( K \) is
\[
[L : K] = \dim_K L
\]

**Definition**

A *number field* is a finite extension of \( \mathbb{Q} \).
Remark

Let $L/K$ be a field extension and $\alpha_1, \ldots, \alpha_m \in L$. Then we write

$$K(\alpha_1, \ldots, \alpha_m) = \text{Frac } K[\alpha_1, \ldots, \alpha_n]$$

to be the subfield of $L$ generated by $K$ and $\alpha_1, \ldots, \alpha_n$.

If $K$ is a number field then $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ for some $\alpha_1, \ldots, \alpha_m \in K$; in fact, by the primitive element theorem, we can take $m = 1$.

Example

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

Remark

The choice of $\alpha$ such that $K = \mathbb{Q}(\alpha)$ is highly non-unique.

Let $K = \mathbb{Q}(\alpha)$ be a number field and $g \in \mathbb{Q}[X]$ the minimal polynomial of $\alpha$. The ring homomorphism $\mathbb{Q}[X] \to K$ given by $f \mapsto f(\alpha)$ has kernel $\langle g \rangle$ and image $\mathbb{Q}[\alpha]$.

By the first ring isomorphism theorem, we therefore have

$$\frac{\mathbb{Q}[X]}{\langle g \rangle} \cong \mathbb{Q}[\alpha]$$

Remark

$$\frac{\mathbb{Q}[X]}{\langle g \rangle}$$ is a field since $\langle g \rangle$ is maximal by irreducibility of $g$, and so $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

Lemma 1.6

Let $K$ be a number field of degree $n$. Then there are exactly $n$ distinct field embeddings $K \hookrightarrow \mathbb{C}$. 

5
Remark

The minimal polynomial of the generator of a number field has real coefficients, so $n = r + 2s$ where $r$ is the number of real embeddings and $s$ is the number of complex conjugate pairs of embeddings.

Then $n, r, s$ depend only on $K$ and not on the choice of $\alpha$. If we demand that $K \subseteq \mathbb{C}$ then one of the embeddings must be the identity map.

Theorem 1.7

If $K \subseteq L \subseteq M$ are fields, then

$$[M : K] = [M : L][L : K]$$

This result is known as the ‘tower law’.

Lemma 1.8

Let $K$ be a number field and let $\beta \in K$ have minimal polynomial $g$ over $\mathbb{Q}$.

Let $\beta_1, \ldots, \beta_m \in \mathbb{C}$ be the roots of $g$.

Then

$$d_i = |\{ (\sigma : K \hookrightarrow \mathbb{C}) : \sigma(\beta) = \beta_i \}|$$

is independent of $i$.

Definition

In the above lemma, $\beta_1, \ldots, \beta_m$ are called the conjugates of $\beta$.

Definition

Let $L/K$ be a finite field extension.

If $x \in L$ then there is a $K$-linear map

$$\varphi_x : L \to L, \quad y \mapsto xy$$

Then

(i) The trace of $x$ is $\text{tr}_{L/K} x = \text{tr} \varphi_x \in K$
(ii) The norm of $x$ is $\mathcal{N}_{L/K} x = \det \varphi_x \in K$

**Remark**

The norm is multiplicative, i.e.

$$
\mathcal{N}_{L/K} (x_1 x_2) = \mathcal{N}_{L/K} (x_1) \mathcal{N}_{L/K} (x_2)
$$

and the trace is a $K$-linear map.

**Remark**

If $f \in K[X]$ and $\varphi_x$ is as above, then $f(\varphi_x) = \varphi_{f(x)}$.

**Theorem 1.9**

Let $K$ be a number field of degree $n$ with distinct embeddings

$$
\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}
$$

For $\beta \in K$ the characteristic polynomial of the $\mathbb{Q}$-linear map

$$
\varphi_{\beta} : K \to K, \quad y \mapsto y\beta
$$

is given by

$$
 f(X) = \prod_{i=1}^{n} (X - \sigma_i(\beta))
$$

In particular,

$$
\text{tr}_{K/\mathbb{Q}} (\beta) = \sum_{i=1}^{n} \sigma_i(\beta), \quad \mathcal{N}_{K/\mathbb{Q}} (\beta) = \prod_{i=1}^{n} \sigma_i(\beta)
$$

**Corollary 1.10**

If $\beta$ is an algebraic integer then $\text{tr}_{K/\mathbb{Q}} (\beta), \mathcal{N}_{K/\mathbb{Q}} \in \mathbb{Z}.$
Definition

If $K$ is a number field, then the ring of integers of $K$ is

$$\mathcal{O}_K = \{ x \in K : x \text{ is an algebraic integer} \}$$

Note that this is a ring by (1.3).

Lemma 1.11

$x \in \mathcal{O}_K$ is a unit if and only if $N_{K/Q}(x) = \pm 1$.

Lemma 1.12

If $\beta \in K$ then there exists $0 \neq c \in \mathbb{Z}$ such that $c\beta \in \mathcal{O}_K$.

In particular, $K = \text{Frac} \mathcal{O}_K$.

Definition

Let $K$ be a number field with $[K : \mathbb{Q}] = n$ and $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ distinct embeddings.

For $x_1, \ldots, x_n \in K$, we define

$$\Delta(x_1, \ldots, x_n) = \det (\sigma_i(x_j))^2 = \det (\text{tr}_{K/Q}(x_i x_j)) \in \mathbb{Q}$$

Remark

If $x'_i = \sum_{j=1}^n a_{ij} x_j$ for $a_{ij} \in \mathbb{Q}$, and $A = (a_{ij})$, then

$$\Delta(x'_1, \ldots, x'_n) = (\det A)^2 \Delta(x_1, \ldots, x_n)$$
Recall

The discriminant of \( f(X) = \prod_{i=1}^{n}(X - \alpha_i) \) is

\[
\text{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2
\]

Lemma 1.13

Let \( K = \mathbb{Q}(\alpha) \) be a number field of degree \( n \) and let \( f \) be the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \). Then

(i) \( \Delta(1, \alpha, \ldots, \alpha^{n-1}) = \text{disc}(f) \);

(ii) \( \{x_1, \ldots, x_n\} \) is a basis for \( K \) over \( \mathbb{Q} \) if and only if \( \Delta(x_1, \ldots, x_n) \neq 0 \).

Definition

A basis \( \{x_1, \ldots, x_n\} \) for \( K \) over \( \mathbb{Q} \) is called an integral basis if

\[
\mathcal{O}_K = \left\{ \sum_{i=1}^{n} \lambda_i x_i : \lambda_i \in \mathbb{Z} \right\}
\]

Theorem 1.14

Every number field \( K \) has an integral basis.

In particular, \( \mathcal{O}_K \cong \mathbb{Z}^n \) as a group under +.

Definition

The discriminant of a number field \( K \) is

\[
D_K = \Delta(x_1, \ldots, x_n)
\]

where \( \{x_1, \ldots, x_n\} \) is an integral basis.
Quadratic fields

Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 0, \pm 1$ is a squarefree integer; then

$$K = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}$$

Then

$$\text{tr}_{K/\mathbb{Q}}(x + y\sqrt{d}) = (x + y\sqrt{d}) + (x - y\sqrt{d}) = 2x$$

$$\mathcal{N}_{K/\mathbb{Q}}(x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

Proposition 1.15

For a quadratic field $K = \mathbb{Q}(\sqrt{d})$,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

Remark

The discriminant $D_K$ of $K$ is given by

$$D_K = \begin{cases} \det \left( \begin{array}{cc} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{array} \right)^2 = 4d & \text{if } d \equiv 2, 3 \pmod{4} \\ \det \left( \begin{array}{cc} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{array} \right)^2 = d & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

Lemma 1.16

Let $M \subseteq \mathbb{Z}^n$ be any subgroup. Then $M \cong \mathbb{Z}^r$ for some $r \leq n$.

If $r = n$ and $A$ is an $n \times n$ matrix whose rows are a $\mathbb{Z}$-basis for $M$, then

$$[\mathbb{Z} : M] = |\det A|$$
Note

Taking a different choice of $A$ in the above lemma will only change $\det A$ up to a sign, so this is well-defined.

Corollary 1.17

If $\{x_1, \ldots, x_n\} \subseteq \mathcal{O}_K$ is a basis for $K$ over $\mathbb{Q}$, then

$$\Delta(x_1, \ldots, x_n) = [\mathcal{O}_K : M]^2 D_K$$

where $M = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$. 
2 Ideals

Throughout this section, $K$ denotes a number field and $\mathcal{O}_K$ denotes its ring of integers.

Example

$$K = \mathbb{Q}(\sqrt{-5}), \mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$$

$\mathcal{O}_K$ is not a unique factorization domain, since

$$3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

but $3$, $7$ and $1 \pm 2\sqrt{-5}$ are irreducible and not associates.

To show that $3$ is irreducible, write $3 = \alpha \beta$, where $\alpha, \beta \in \mathcal{O}_K$.

Then $N(\alpha)N(\beta) = 9$, so if they are reducible and $\alpha = x + y\sqrt{-5}$ for $x, y \in \mathbb{Z}$, then we’d have $x^2 + 5y^2 = \pm 3$. This clearly has no solutions for $x, y \in \mathbb{Z}$, so we must have that $\alpha$ or $\beta$ is a unit.

A similar process shows that $1 \pm 2\sqrt{-5}$ are irreducible.

Ideals were used by Kummer, Dedekind, . . . , to restore the property of unique factorization.

Recall

We say $a \subseteq \mathcal{O}_K$ is an ideal, and write $a \subseteq \mathcal{O}_K$, if:

(i) $a$ is an additive subgroup of $\mathcal{O}_K$;

(ii) for all $r \in \mathcal{O}_K$ and $s \in a$, we have $rs \in a$.

Every number field has an integral basis, so $\mathcal{O}_K \cong \mathbb{Z}^n$ as an abelian group. So if $a \subseteq \mathcal{O}_K$ is an ideal then $a$ is finitely-generated as a $\mathbb{Z}$-module; so it is finitely-generated as an $\mathcal{O}_K$-module.

We have therefore shown:

Lemma 2.1

$\mathcal{O}_K$ is a Noetherian ring.
Recall

\[ \langle \alpha_1, \ldots, \alpha_r \rangle = \left\{ \sum_{i=1}^{r} \lambda_i \alpha_i : \lambda_i \in \mathcal{O}_K \right\} \]

**Definition**

The *product* of two ideals \( a, b \in \mathcal{O}_K \) is given by

\[ ab = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in a, b_i \in b, \, n \in \mathbb{N} \right\} \]

**Remark**

If \( a = \langle \alpha_1, \ldots, \alpha_n \rangle \) and \( b = \langle \beta_1, \ldots, \beta_s \rangle \) then

\[ ab = \langle \{ \alpha_i \beta_j : 1 \leq i \leq r, 1 \leq j \leq s \} \rangle \]

**Definition**

We say \( b \) *divides* \( a \) if there exists an ideal \( c \) such that \( a = bc \)

**Recall**

An ideal \( a \subseteq \mathcal{O}_K \) is a *principal ideal* if there is some \( \alpha \in \mathcal{O}_K \) such that \( a = \langle \alpha \rangle \).

If \( \langle \alpha \rangle = \langle \beta \rangle \) then \( \frac{\alpha}{\beta} \in \mathcal{O}_K^\times \), and we say that \( \alpha \) and \( \beta \) are *associates*.

**Theorem 2.2**

For any ideal \( a \subseteq \mathcal{O}_K \) there is a nonzero ideal \( b \subseteq \mathcal{O}_K \) such that \( ab \) is principal.
Example

Let $K = \mathbb{Q} \sqrt{d}$ with $d \in \mathbb{Z}$ nonsquare, and let $a = \langle a, \beta \rangle$ for some $a \in \mathbb{Z}$ and $\beta = u + v\sqrt{d} \in \mathcal{O}_K$.

Then

$$\langle a, \beta \rangle \langle a, \bar{\beta} \rangle = \langle a^2, a\beta, a\bar{\beta}, \beta \bar{\beta} \rangle = \langle a^2, a\beta, a(\beta + \bar{\beta}), \beta \bar{\beta} \rangle = \langle a^2, a\beta, \text{tr}_{K/\mathbb{Q}}(\beta), \text{N}_{K/\mathbb{Q}}(\beta) \rangle = \langle c, a\beta \rangle$$

where $c = \gcd (a^2, a \text{tr}_{K/\mathbb{Q}}(\beta), \text{N}_{K/\mathbb{Q}}(\beta))$.

Let $x = \frac{a\beta}{c}$. Then

$$\begin{align*}
\text{tr}_{K/\mathbb{Q}}(x) &= \frac{a}{c} \text{tr}_{K/\mathbb{Q}}(\beta) \in \mathbb{Z} \\
\text{N}_{K/\mathbb{Q}}(x) &= \frac{a^2}{c^2} \text{N}_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}
\end{align*}$$

but $x$ is a root of the equation

$$X^2 - \text{tr}_{K/\mathbb{Q}}(x)X + \text{N}_{K/\mathbb{Q}}(x) = 0$$

Therefore $x \in \mathcal{O}_K$.

So $\langle a, \beta \rangle \langle a, \bar{\beta} \rangle = \langle c \rangle$.

Lemma 2.3

For $a \nsubseteq \mathcal{O}_K$ nonzero,

(i) $a \cap \mathbb{Z} \neq 0$;

(ii) $\frac{\mathcal{O}_K}{a}$ is finite.

Recall

An ideal $p \nsubseteq \mathcal{O}_K$ is prime if $\frac{\mathcal{O}_K}{p}$ is an integral domain. Equivalently, if $p \neq \mathcal{O}_K$ and if $a, b \in \mathcal{O}_K$ with $ab \in p$ then $a \in p$ or $b \in p$. 
Lemma 2.4

Let $p$ be a prime ideal. If $a, b$ are ideals and $ab \subseteq p$, then either $a \subseteq p$ or $b \subseteq p$.

Lemma 2.5

Every nonzero prime ideal $p \subseteq \mathcal{O}_K$ is a maximal ideal.

Remark

In this course, we take all prime ideals to be nonzero.

Lemma 2.6

Every nonzero ideal $a \subseteq \mathcal{O}_K$ contains a product of prime ideals.

Lemma 2.7

Let $a \subseteq \mathcal{O}_K$. Then there exists $x \in K \setminus \mathcal{O}_K$ with $xa \subseteq \mathcal{O}_K$.

Lemma 2.8

Let $a \subseteq \mathcal{O}_K$ be a nonzero ideal. If $x \in K$ with $xa \subseteq a$, then $x \in \mathcal{O}_K$.

Definition

A subset $a \subseteq K$ is a fractional ideal if there is some $0 \neq c \in K$ such that $ca \subseteq \mathcal{O}_K$ is an ideal.

Remark

$a$ is an ideal $\nRightarrow$ $a$ is a fractional ideal.
Lemma 2.9

Let $a \subseteq K$ be a subset. Then $a$ is a fractional ideal if and only if $a$ is a finitely-generated $\mathcal{O}_K$-module.

Remark

To contrast with a notion of a fractional ideal, we call ideals integral ideals.

Definition

A fractional ideal $a$ is invertible if there is a fractional ideal $b$ such that $ab = (1) = \mathcal{O}_K$.

Remark

Theorem (2.4) is equivalent to the statement:

Every nonzero fractional ideal is inverible.

Remark

If $a$ is an invertible fractional ideal then

$$a^{-1} = \{x \in K : xa \subseteq \mathcal{O}_K\}$$

Corollary 2.10

Let $a, b, c$ be integral ideals with $c \neq 0$. Then

(i) $b \subseteq a \iff bc \subseteq ac$;
(ii) $a|b \iff ac|bc$;
(iii) $a|b \iff b \subseteq a$ ("to contain is to divide")
Theorem 2.11

Every nonzero ideal \( \mathfrak{a} \subseteq \mathcal{O}_K \) can be written uniquely as a product of prime ideals.

Theorem 2.12

The nonzero fractional ideals of \( K \) form a group \( I_K \) under ideal multiplication. It is a free abelian group generated by the prime ideals, i.e. we can write each \( a \in I_K \) in the form

\[
a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}
\]

with \( p_1, \ldots, p_r \) distinct prime ideals and \( \alpha_1, \ldots, \alpha_r \in \mathbb{Z} \).

Remark

With the notation of the above theorem, \( \mathfrak{a} \subseteq \mathcal{O}_K \Leftrightarrow \alpha_i \geq 0 \) for all \( i \)

Remark

There is a group homomorphism

\[
K^\times \to I_K, \quad x \mapsto \langle x \rangle
\]

whose kernel is the group of units \( \mathcal{O}_K^\times \).

Denote its image by \( P_K \). Then \( P_K \leq I_K \) is the (normal) subgroup consisting of principal fractional ideals.

Definition

The class group \( \text{Cl}_K \) is the quotient \( I_K / P_K \).

Remark

A more intuitive definition of the class group is the set of equivalence classes of integral ideals under the equivalence relation \( \sim \) given by

\[
a \sim b \Leftrightarrow \text{there exist nonzero } \gamma, \delta \in \mathcal{O}_K \text{ such that } \gamma a = \delta b
\]
Then we can write \([a]\) for the equivalence class of \(a\) under \(\sim\) and endow \(\text{Cl}_K\) with a group structure by defining \([a] \cdot [b] = [ab]\).

**Proposition 2.13**

The following are equivalent:

(i) \(O_K\) is a principal ideal domain;
(ii) \(O_K\) is a unique factorization domain;
(iii) \(\text{Cl}_K\) is trivial.

**Remark**

For \(a, b \subseteq O_K\),

\[
a + b = \{x + y : x \in a, y \in b\}
\]

It is the smallest ideal containing \(a\) and \(b\). Since “to contain is to divide” (2.10), we have that

\[
a + b = \gcd(a, b)
\]

We may think of a finitely-generated ideal as the greatest common divisor of its generators.

**Norms of ideals**

**Definition**

Let \(a \subseteq O_K\) be a nonzero ideal. If

\[
\alpha, \beta \in O_K \quad \text{and} \quad \alpha - \beta \in a
\]

then we say \(\alpha\) is congruent to \(\beta\) modulo \(a\), and write

\[
\alpha \equiv \beta \pmod{a}
\]

The *ideal norm* \(N a\) is the number of equivalence classes under congruence modulo \(a\), i.e.

\[
N a = \left| \frac{O_K}{a} \right|
\]
Remark

By Lagrange’s theorem, we have that

\[ 0 \neq \mathcal{N} a \in a \cap \mathbb{Z} \]

Proposition 2.14

For \( a, b \in O_K \),

\[ \mathcal{N}(ab) = (\mathcal{N} a)(\mathcal{N} b) \]

Lemma 2.15

Let \( a \trianglelefteq O_K \) be a nonzero ideal. Then there exists a \( \mathbb{Q} \)-basis \( \{\gamma_1, \ldots, \gamma_n\} \) for \( K \) such that

\[ a = \left\{ \sum_{i=1}^{n} \lambda_i \gamma_i : \lambda_i \in \mathbb{Z} \right\} \]

and moreover

\[ \Delta(\gamma_1, \ldots, \gamma_n) = (\mathcal{N} a)^2 D_K \]

Proposition 2.16

If \( 0 \neq \alpha \in O_K \) then

\[ \mathcal{N}(\alpha) = |\mathcal{N}_{K/\mathbb{Q}}(\alpha)| \]

Corollary 2.17

Suppose \( p \trianglelefteq O_K \) is a prime ideal. Then there is a unique rational prime \( p \in \mathbb{Z} \) such that \( p \mid (p) \). Moreover, \( \mathcal{N} p \) is a power of \( p \).
Remark

We have $p \cap \mathbb{Z} = p\mathbb{Z}$; in particular, if $p|(a)$ for some $a \in \mathbb{Z}$ then $p|a$.

Definition

Let $p \in \mathbb{Z}$ be a rational prime. Let $p_1, \ldots, p_r \subseteq \mathcal{O}_K$ be distinct prime ideals and $e_1, \ldots, e_r, f_1, \ldots, f_r$ be positive integers such that

$$\langle p \rangle = p\mathcal{O}_K = p_1^{e_1} \cdots p_r^{e_r}$$

with $N(p_j) = p^{f_j}$ for $1 \leq j \leq r$. Then

(i) $e_1, \ldots, e_r$ are the ramification indices of $p$;
(ii) $f_1, \ldots, f_r$ are the residue class degrees of $p$.

Corollary 2.18

With the notation as in the above definition,

$$\sum_{i=1}^{r} e_if_i = [K : \mathbb{Q}]$$

Definition

Let $p \in \mathbb{Z}$ be a rational prime with ramification indices $e_1, \ldots, e_r$ and corresponding residue class degrees $f_1, \ldots, f_r$. We say:

(i) $p$ ramifies in $K$ if some $e_i > 1$;
(ii) $p$ is inert in $K$ if $\langle p \rangle$ is a prime ideal;
(iii) $p$ splits completely in $K$ if $e_i = f_i = 1$ for each $1 \leq i \leq r$. 

20
3 The Class Group & Units

Definition

A subset $X \subseteq \mathbb{R}^n$ is discrete if

$$\forall x \in X \ \exists \varepsilon > 0 \ \text{s.t.} \ X \cap B(x; \varepsilon) = \{x\}$$

Equivantly, $X$ is discrete if it inherits the discrete topology from the Euclidean topology on $\mathbb{R}^n$.

Lemma 3.1

Let $\Lambda \subseteq \mathbb{R}^n$. Then the following are equivalent:

(i) $\Lambda = \left\{ \sum_{i=1}^{m} a_i x_i, \ a_i \in \mathbb{Z} \right\}$ for some $\mathbb{R}$-linearly independent $x_1, \ldots, x_m \in \mathbb{R}^n$;

(ii) $\Lambda$ is a discrete subgroup of $(\mathbb{R}^n, +)$.

Definition

If the conditions of (3.1) are satisfied then we say $\Lambda$ is a lattice.

Recall

If $A$ is a finitely-generated abelian group, then

$$A \cong T \times \mathbb{Z}^r$$

for some finite abelian group $T$ and some $r \geq 0$. We say $r$ is the rank of $A$.

Remark

Let $K$ be a number field with $[K : \mathbb{Q}] = n = r + 2s$, where $r$ is the number of distinct real embeddings

$$\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$$

and $2s$ is the number of distinct complex embeddings

$$\sigma_{r+1}, \sigma_{r+1}, \ldots, \sigma_{r+s}, \sigma_{r+s} : K \hookrightarrow \mathbb{C}$$
There is a group homomorphism

\[ L : \mathcal{O}_K \rightarrow \mathbb{R}^{r+s} \]

given by

\[ L(u) = (\log |\sigma_1(u)|, \ldots, \log |\sigma_{r+s}(u)|) \]

Lemma 3.2

If \( B \subseteq \mathbb{R}^{r+s} \) is bounded then \( L^{-1}B \) is finite.

Remark

By (3.2), \( \ker L \) is finite, and hence consists of roots of unity as it is a subgroup, and \( \operatorname{im} L \) is discrete. And by (3.1), \( \mathcal{O}_K^\times \) is a finitely-generated abelian group of rank \( \leq r+s \).

By (1.10), for \( u \in \mathcal{O}_K^\times \),

\[ \mathcal{N}_{K/\mathbb{Q}}(u) = \prod_{i=1}^{n} \sigma_i(u) = \pm 1 \]

so

\[ \operatorname{im} L \subseteq \left\{ (x_1, \ldots, x_r, y_1, \ldots, y_s) \in \mathbb{R}^{r+s} : \sum_{i=1}^{r} x_i + 2 \sum_{j=1}^{s} y_j = 0 \right\} \]

So in fact we have:

Proposition 3.3

\( \mathcal{O}_K^\times \) has rank \( \leq r + s - 1 \).

Remark

In fact, we have equality in (3.3) (Dirichlet’s units theorem).

More explicitly, write \( \rho = r + s - 1 \). Then there exist units \( \varepsilon_1, \ldots, \varepsilon_\rho \) such that we can write any unit \( u \in \mathcal{O}_K^\times \) in the form

\[ u = \zeta \varepsilon_1^{m_1} \ldots \varepsilon_\rho^{m_\rho} \]

where \( \zeta \) is a root of unity and \( m_1, \ldots, m_\rho \in \mathbb{Z} \).
Definition

We call $\varepsilon_1, \ldots, \varepsilon_\rho$ a set of fundamental units.

Note that these are not unique.

Units in quadratic fields

In this subsection, take $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z} \setminus \{0, \pm 1\}$ is squarefree.

Note that

$$O_K^\times = \begin{cases} \{x + y\left(\frac{1+\sqrt{d}}{2}\right) : x, y \in \mathbb{Z}, (x + \frac{y}{2})^2 - \frac{d}{4}y^2 = \pm 1\} & \text{if } d \equiv 1 \pmod{4} \\ \{x + y\sqrt{d} : x, y \in \mathbb{Z}, x^2 - dy^2 = \pm 1\} & \text{if } d \equiv 2, 3 \pmod{4} \end{cases}$$

If $d < 0$ then Dirichlet’s units theorem tells us that $O_K^\times$ has rank 0. Furthermore:

(i) if $d = -1$ then $O_K = \mathbb{Z}[i]$ and $O_K^\times = \{\pm 1, \pm i\}$

(ii) if $d = -3$ then $O_K = \mathbb{Z}[\omega]$ and $O_K^\times = \{\pm 1, \pm \omega, \pm \omega^2\}$, where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$

(iii) if $d \neq -1, -3$ then $O_K^\times = \{\pm 1\}$

If $d > 0$ then Dirichlet’s units theorem tells us that $O_K^\times$ has rank 1. As $K$ is embedded in \(\mathbb{R}\), the only roots of unity in $K$ are $\pm 1$, and so

$$O_K^\times = \{\pm \varepsilon^m : m \in \mathbb{Z}\}$$

for some $\varepsilon$ (a fundamental unit); w.l.o.g. $\varepsilon > 0$.

Example

Take $K = \mathbb{Q}(\sqrt{2})$ and let $\varepsilon = 1 + \sqrt{2}$. Then $\mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = -1$, so $\varepsilon \in O_K^\times$. We claim $\varepsilon$ is a fundamental unit.

If not, then there exist $a, b \in \mathbb{Z}$ such that $u = a + b\sqrt{2}$ is a unit with $1 < u < \varepsilon$.

Let $\bar{u} = a - b\sqrt{2}$. Then $u\bar{u} = \pm 1$, and so $|\bar{u}| < 1$.

Hence $u \pm \bar{u} > 0$, so $a, b > 0$. But we have

$$a + b\sqrt{2} < 1 + \sqrt{2}$$

and there are only finitely many choices of $a, b$ that might have been able to satisfy this, but none of them satisfy

$$a^2 - 2b^2 = \pm 1$$
so we deduce that $\varepsilon$ is a fundamental unit, and hence

$$O_K^\times = \left\{ \pm (1 + \sqrt{2})^m : m \in \mathbb{Z} \right\}$$

Remark

For $K$ a real quadratic field, (3.3) tells us that $\frac{O_K^\times}{\{\pm 1\}}$ is either trivial or infinite cyclic, as illustrated in the above example.

Remark

Finding units in $\mathbb{Z}[\sqrt{d}]$ is equivalent to solving $Pell’s$ equation

$$x^2 - dy^2 = 1$$

and, where possible, the $negative$ $Pell$ equation

$$x^2 - dy^2 = -1$$

These equations can be solved using continued fractions (see number theory).

Lemma 3.4

If $d \equiv 1 \pmod{4}$ then

$$\mathbb{Z}[\sqrt{d}]^\times \leq \mathbb{Z} \left[ \frac{1 + \sqrt{d}}{2} \right]^\times$$

is a subgroup of index 1 or 3.

Example

Take $d = 5$, and set $\varphi = \frac{1 + \sqrt{5}}{2}$. Then $\varphi^2 = \frac{3 + \sqrt{5}}{2}$ and $\varphi^3 = 2 + \sqrt{5}$, which lies in $\mathbb{Z}[\sqrt{5}]^\times$. This demonstrates (3.4).
Definition

Let $\Lambda$ be a lattice spanned by the rows of some $A \in \text{GL}_n(\mathbb{R})$.

The determinant if $\Lambda$ is $d(\Lambda) = |\det A|$.

(Note that this depends only on $\Lambda$ and is independent of the choice of matrix $A$.)

Definition

Let $X \subseteq \mathbb{R}^n$. We say $X$ is convex if, whenever $x,y \in X$, we have

$$(1 - \lambda)x + \lambda y \in X$$

for all $\lambda \in [0,1]$.

We say $X$ is symmetric about 0 if

$-x \in X$ for all $x \in X$.

Theorem 3.5 – Minkowski’s theorem

Let $S$ be a measurable subset of $\mathbb{R}^n$ that is convex and symmetric about 0.

Suppose that either

(i) $\text{vol}(S) > 2^nd(\Lambda)$;

(ii) $\text{vol}(S) \geq 2^nd(\Lambda)$ and $S$ is compact.

Then $S$ contains an element of $\Lambda$ other than 0.

Theorem 3.6 – Blichfeldt’s theorem

If $X$ is a measurable subset of $\mathbb{R}^n$ with $\text{vol}(X) > d(\Lambda)$, then there exist distinct $x,y \in X$ such that $x - y \in \Lambda$.

Remark

Blichfeldt’s theorem $\Rightarrow$ Minkowski’s theorem.
For case (i), take $X = \frac{1}{2} S$.

For case (ii), construct a sequence $x_n \in \Lambda$ by applying (i) to $(1 + \frac{1}{n}) S$. This sequence has a convergent subsequence by compactness of $S$ and discreteness of $\Lambda$, and the limit must lie in $\Lambda \cap S$.

**Theorem 3.7**

Let $K$ be a number field with $[K : \mathbb{Q}] = n = r + 2s$ ($r, s$ as before).

If $a \subseteq \mathcal{O}_K$ is a nonzero ideal, then there exists some $0 \neq \alpha \in a$ such that

$$|\mathcal{N}_{K/\mathbb{Q}}(\alpha)| \leq c \cdot N a \cdot \sqrt{|D_K|}$$

where $c$ depends only on $n, r, s$.

**Theorem 3.8**

Every ideal class contains an ideal $b$ with

$$\mathcal{N} b \leq c \cdot \sqrt{|D_K|}$$

where $c$ is as in (3.7)

**Remark**

We prove (3.7) and (3.8) using $c = \left(\frac{2}{\pi}\right)^s n!$. In fact, they hold with

$$c = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$$

This is called the Minkowski constant.

**Definition**

The class number $h_K$ of $K$ is the order of $\mathcal{C}l_K$.  

26
Example

Let \( K = \mathbb{Q}(\sqrt{-5}) \), so that \( \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] \).

Every ideal class contains an ideal \( b \) with

\[
\mathcal{N} b \leq \left( \frac{4}{\pi} \right) \frac{2!}{2^2} \sqrt{|4(-5)|} = \frac{2\sqrt{20}}{\pi} < \frac{4\sqrt{5}}{3} < 3
\]

(i) If \( \mathcal{N} b = 1 \) then \( b = (1) = \mathcal{O}_K \).

(ii) If \( \mathcal{N} b = 2 \) then \( b/(2) = p^2 \), where \( p = (2, 1 + \sqrt{-5}) \), and so \( b = p \).

\( p \) is not principal, since there do not exist integers \( x, y \) with \( x^2 + 5y^2 = \pm 2 \).

Hence \( \text{Cl}_K \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \) and \( h_K = 2 \).

Factoring primes

Let \( p \) be a rational prime. We aim to factor \( (p) = p\mathcal{O}_K \) as a product of prime ideals.

Consider the quotient map

\[
q : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K
\]

There is a bijection

\[
\left\{ \text{(prime) ideals of } \mathcal{O}_K/p\mathcal{O}_K \right\} \leftrightarrow \left\{ \text{(prime) ideals of } \mathcal{O}_K \text{ containing } p \right\}
\]

given by

\[
I \mapsto q^{-1}I
\]

The ring \( \mathcal{O}_K/p\mathcal{O}_K \) is finite, so we could compute its prime ideals by testing all of its subsets; but fortunately, we can do better.

Theorem 3.9 – Dedekind’s criterion

Let \( \alpha \in \mathcal{O}_K \) with minimal polynomial \( g \in \mathbb{Z}[X] \). Suppose \( \mathbb{Z}[(\alpha)] \subseteq \mathcal{O}_K \) has finite index coprime to \( p \).

If \( \bar{g} \in \mathbb{F}_p[X] \) has factorization into irreducibles given by

\[
\bar{g} = \varphi_1 \cdots \varphi_r
\]
then \(\langle p \rangle\) factors into prime ideals as

\[
\langle p \rangle = p_{e_1} \cdots p_{e_r}
\]

where \(p_i = \langle p, \tilde{\varphi}_i(\alpha) \rangle\); \(\tilde{\varphi}\) is an arbitrary lifting of \(\varphi_i\) to \(\mathbb{Z}[X]\), the choice of which does not matter.

**Remark**

It is useful to note that if \(p_i\) is as in Dedekind’s criterion above, then

\[
\mathcal{N} p_i = \left| \frac{F_p[X]}{\langle \tilde{\varphi}_i \rangle} \right| = p^{f_i}
\]

where \(f_i = \deg \varphi_i\).

**Quadratic fields**

Let \(K = \mathbb{Q}(\sqrt{d})\), where \(d \neq 0, \pm 1\) is a squarefree integer.

Recall that \(\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K\) has index 1 or 2.

Let \(p\) be an odd prime. By applying Dedekind’s criterion, we have three cases:

(i) \(X^2 - d\) has two distinct roots modulo \(p\).

Then \(\langle p \rangle = pp'\), where \(p, p'\) are distinct prime ideals of norm \(p\).

In this case, we say \(p\) splits in \(K/\mathbb{Q}\).

(ii) \(X^2 - d\) has a repeated root modulo \(p\).

Then \(\langle p \rangle = p^2\), where \(p\) is a prime ideal of norm \(p\).

In this case, we say \(p\) ramifies in \(K/\mathbb{Q}\).

(iii) \(X^2 - d\) is irreducible modulo \(p\).

Then \(\langle p \rangle = p\), where \(p\) is a prime ideal of norm \(p^2\).

In this case, we say \(p\) is inert in \(K/\mathbb{Q}\).

**Lemma 3.10**

The prime \(p = 2\)

(i) splits in \(K/\mathbb{Q}\) \(\iff d \equiv 1 \pmod{8}\)

(ii) is inert in \(K/\mathbb{Q}\) \(\iff d \equiv 5 \pmod{8}\)

(iii) ramifies in \(K/\mathbb{Q}\) \(\iff d \equiv 2, 3 \pmod{4}\)
Remark

Recall that $K = \mathbb{Q}(\sqrt{d})$ has discriminant

$$D_K = \begin{cases} d & \text{if } d \equiv 1 \pmod{4} \\ 4d & \text{if } d \equiv 2, 3 \pmod{4} \end{cases}$$

So $p$ ramifies in $K/\mathbb{Q}$ if and only if $p|D_K$.

In fact, this holds in general, and not just for when $[K : \mathbb{Q}] = 2$.

Example

We compute the class group of $\mathbb{Q}(\sqrt{-17})$.

First note that $-17 \equiv 3 \pmod{4}$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$ and $D_K = 4(-17)$.

Minkowski’s bound tells us that every ideal class contains an ideal $b$ with

$$N b \leq \left(\frac{4}{\pi}\right)^n \frac{n!}{n^n} \sqrt{|D_K|} \leq 2 \cdot \frac{2 \sqrt{17}}{\pi} < \frac{4 \cdot 5}{3} < 7$$

So the class group is generated by primes dividing 2, 3, 5.

Let $f(X) = X^2 + 17$. Then, by Dedekind’s criterion,

- $f(X) \equiv (X + 1)^2 \pmod{2}$, so $\langle 2 \rangle = p^2$, $p = \langle 2, 1 + \sqrt{-17} \rangle$
- $f(X) \equiv (X + 1)(X - 1) \pmod{3}$, so $\langle 3 \rangle = q_+q_-$, $q_\pm = \langle 3, 1 \pm \sqrt{-17} \rangle$
- $f(X) \equiv X^2 + 2 \pmod{5}$, so $\langle 5 \rangle$ is inert

Furthermore, $N_{K/\mathbb{Q}}(1 + \sqrt{-17}) = 18 = 2 \cdot 3^2$, and so

$$\langle 1 + \sqrt{-17} \rangle = pq_+^2$$

We have

$$p^2 \sim q_+q_- \sim pq_+^2 \sim \langle 1 \rangle$$

where $a \sim b$ if $a$ and $b$ lie in the same ideal class.

Hence the class group is generated by $q_+$.

Also

$$q_+^4 \sim p^{-2} \sim 1$$
and \( p \sim q_+ \sim 1 \) since if not we’d have \( x^2 + 17y^2 = 2 = Np \) for some \( x, y \in \mathbb{Z} \).

So \([q_+]\) has order 4, and hence
\[
\text{Cl}_K \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \text{ and } h_K = 4
\]

**Remark**

If \( \mathcal{O}_K = \mathbb{Z}[\alpha] \) then Dedekind’s criterion shows that no prime \( p < [K : \mathbb{Q}] \) splits completely. So if 2 splits completely, then \( \mathcal{O}_K \neq \mathbb{Z}[\alpha] \) for any \( \alpha \).

**Example**

We seek all solutions \( x, y \in \mathbb{Z} \) to the equation \( y^2 + 5 = x^3 \).

Recall that \( K = \mathbb{Q}(\sqrt{-5}) \) has class number \( h_K = 2 \), and \( \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] \).

We have
\[
(y + \sqrt{-5})(y - \sqrt{-5}) = x^3
\]

Suppose \( p \mid \mathcal{O}_K \) is a prime ideal with \( p\langle y + \sqrt{-5} \rangle \) and \( p\langle y - \sqrt{-5} \rangle \).

Then \( p\langle2\sqrt{-5}\rangle \), so \( p\langle2\rangle \) or \( p\langle5\rangle \).

(i) If \( p\langle2\rangle \) then \( p\langle x^3 \rangle \), so \( x \) is even and \( y^2 \equiv 1 \pmod{4} \)

(ii) If \( p\langle5\rangle \) then \( p\langle x^3 \rangle \), so either \( p\langle1 \rangle \), or \( 5|x \) and \( y^2 \equiv -5 \pmod{25} \)

So \( \langle y + \sqrt{-5} \rangle \) and \( \langle y - \sqrt{-5} \rangle \) are coprime.

By unique factorization into prime ideals,
\[
\langle y + \sqrt{-5} \rangle = \alpha^3 \text{ for some } \alpha \mid \mathcal{O}_K
\]

Since \( 3 \nmid h_K \) and \( \alpha^3 \) is principal, \( \alpha \) is principal.

Then \( y + \sqrt{-5} = u(a + b\sqrt{-5})^3 \) for some \( a, b \in \mathbb{Z} \) and \( u \in \mathbb{Z}[\sqrt{-5}]^\times \). The only units in \( \mathbb{Z}[\sqrt{-5}] \) are \( \pm 1 \), and by choice of sign of \( a, b \) we can take \( u = 1 \), so we have
\[
y + \sqrt{-5} = a^3 - 15ab^2 + (3ab^2 - 5b^3)\sqrt{-5}
\]
Then

\[
\begin{aligned}
  y &= a(a^2 - 15b^2) \\
  1 &= b(3a^2 - 5b^2)
\end{aligned}
\]

So \( b = \pm 1 \) and \( 3a^2 = 5 \pm 1 \).

So there are no integer solutions \( x, y \) to \( y^2 + 5 = x^3 \).

**Remark**

As an alternative to ruling out cases (i) and (ii) in the above example, we could instead have used the fact that 2 and 5 ramify in \( K \).

**Theorem 3.11 – Hermite’s theorem**

There are only finitely many number fields \( K \) of given degree \( n \) and discriminant \( D \).
4 Cyclotomic Fields

In this section we write $\zeta_n$ to denote a primitive $n^{\text{th}}$ root of unity. Since all our field extensions can be considered to be embedded in $\mathbb{C}$, we may take $\zeta_n = e^{\frac{2\pi i}{n}}$.

**Definition**

A rational prime $p \in \mathbb{Z}$ is **totally ramified** in $K/\mathbb{Q}$ if

$$p\mathcal{O}_K = p^{[K: \mathbb{Q}]}$$

for some prime ideal $p$.

**Proposition 4.1**

Let $K = \mathbb{Q}(\zeta_n)$ where $n = p^r$ is a prime power. Then

(i) $[K : \mathbb{Q}] = \varphi(n) = p^{r-1}(p - 1)$

(ii) $p$ is totally ramified in $K/\mathbb{Q}$.

**Theorem 4.2**

Let $K = \mathbb{Q}(\zeta_n)$ for some $n \not\equiv 2 \pmod{4}$. Then

$$p \text{ ramifies in } K \iff p | n$$

From now on, take $K = \mathbb{Q}(\zeta_p)$ for $p$ an odd prime, and write $\zeta = \zeta_p$.

**Lemma 4.3**

The roots of unity in $K$ are

$$\{ \pm \zeta^i : 0 \leq i < p \}$$

i.e. the $(2p)^{\text{th}}$ roots of unity.
Lemma 4.4

Let \( q \neq p \) be a prime. Then \( q \mathcal{O}_K \) factors as a product of \( r = \frac{p-1}{f} \) distinct prime ideals, each of norm \( p^f \), where \( f \) is the order of \( q \) in \( \left( \frac{\mathbb{Z}}{p\mathbb{Z}} \right)^\times \).

Lemma 4.5

Let \( K \) be a number field with embeddings \( \sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C} \).

If \( 0 \neq x \in \mathcal{O}_K \) with \( |\sigma_i(x)| \leq 1 \) for all \( 1 \leq i \leq n \), then \( x \) is a root of unity.

Lemma 4.6

Every unit \( \varepsilon \in \mathcal{O}_K^\times \) can be written in the form

\[ \varepsilon = \zeta^i u \]

for some \( 0 \leq i < p \) and \( u \in \mathbb{R} \).

Theorem 4.7 – Fermat’s last theorem

The equation

\[ x^n + y^n = z^n \quad (n \geq 3) \]

has no solutions \( x, y, z \in \mathbb{Z} \setminus \{0\} \).

Remark

It suffices to take \( n = p \) an odd prime and \( x, y, z \) pairwise coprime.

Remark

We can split Fermat’s last theorem into two cases:

(i) \( p \) does not divide \( xyz \) (‘Case I’)

(ii) \( p \) divides \( xyz \) (‘Case II’)
We will prove it for \( p \) a regular prime, i.e. \( p \nmid h_K \). This includes all primes less than 100 other than 37, 59 and 67.

**Theorem 4.8**

Let \( p \) be an odd regular prime. If there are integers \( x, y, z \) coprime to \( p \) with \( x^p + y^p = z^p \), then \( x \equiv y \pmod{p} \).

**Lemma 4.9**

Let \( p \) be an odd regular prime and \( \alpha \in O_K^\times \).

Then \( \alpha \) is a \( p \)th power (of another unit) if and only if \( \alpha \) is a \( p \)th power modulo \( \pi^p \), where \( \pi = 1 - \zeta \).

**Example**

Take \( p = 3 \) and \( K = \mathbb{Q}(\sqrt{-3}) \). Then we have an isomorphism

\[
\{ \pm 1, \pm \zeta, \pm \zeta^2 \} = O_K^\times \cong \left( \frac{O_K}{3O_K} \right)^\times
\]

**Theorem 4.10**

Let \( p \) be an odd regular prime and \( \alpha, \beta, \gamma \in O_K^\times \).

There are no solutions to the equation

\[
\alpha x^p + \beta y^p = \gamma z^p
\]

for \( x, y, z \in O_K \) with \( \pi \nmid x, y \) and \( \pi | z \).

**Proposition 4.11**

A prime \( p \) is regular if and only if the numerators of the Bernoulli numbers \( B_2, \ldots, B_{p-3} \) are not divisible by 3, where \( B_n \) is defined by

\[
\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n
\]
5 Acknowledgements

These notes were written by me (Clive Newstead) and were taken from my lecture notes from the Part II Number Fields lecture course as given by Tom Fisher in Lent Term 2012 at the University of Cambridge. Any errors are my own and, to that end, comments and corrections should be sent to me rather than the lecturer.