Math 3704 Lecture Notes

Minhyong Kim, based on notes by Richard Hill

October 13, 2008

Please let me (minhyong.kim@ucl.ac.uk) know of any misprints or mistakes that you find.

Contents

Lecture 1

1 Introduction

Three fields that occur in nature are $\mathbb{Q}$, the field of rational numbers, the field $\mathbb{R}$ of real numbers, and the field $\mathbb{C}$ of complex numbers. The first field is eventually forced on you as you proceed through arithmetic operations on counting numbers. The latter two arise in describing rigorously the continuous objects of the universe, as well as the microscopic world. In spite of many outstanding problems in number theory, the *internal structure* of $\mathbb{Q}$ is in some sense well-motivated and clear. However, the construction of $\mathbb{R}$ and $\mathbb{C}$ are mysterious. These are extremely large objects comprising many layers of complexity that are constructed, in some sense, all at one go starting from the rationals. Eventually, there arises a need to bridge the enormous gap visible in the inclusion

$$\mathbb{Q} \subset \mathbb{C}.$$

One way to think about this issue is in terms of various intermediate objects

$$\mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset \mathbb{C}$$

that we try to construct at a slower pace, keep track of various properties as we go. Many such intermediate fields are of great interest, but a good starting point is to consider intermediate fields consisting of algebraic numbers. Algebraic numbers are special or even *universal* in that copies of these numbers exist inside any sufficiently rich number system wherein we can count naturally.

A number $\alpha \in \mathbb{C}$ is said to be algebraic if there is a non-zero polynomial $f \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$. An *algebraic number field* is a field of the form

$$\mathbb{Q}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \mathbb{Q}[X], g(\alpha) \neq 0 \right\},$$

i.e. the field generated by $\mathbb{Q}$ and α. For example

$$\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} : x, y \in \mathbb{Q}\},$$

$$\mathbb{Q}(\sqrt[3]{2}) = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} : x, y \in \mathbb{Q}\}.$$

In any algebraic number field k there is a ring of *algebraic integers* $\mathfrak{o}$. An algebraic number is called an algebraic integer, if it is a zero of a monic polynomial with integer coefficients. Examples of these rings of algebraic integers are:

$$\mathbb{Z}[\sqrt{2}] \subset \mathbb{Q}(\sqrt{2}),$$

where

$$\mathbb{Z}[\alpha] = \{f(\alpha) : f \in \mathbb{Z}[X]\}.$$

The sort of questions that we'll deal with in this course are:

- Does the ring $\mathfrak{o}$ have unique factorization?
- Is $\mathfrak{o}$ a principal ideal domain?
- If $\mathfrak{o}$ is not a principal ideal domain, then how far is it from being a principal ideal domain?
- If p is a prime number, how does p factorize in $\mathfrak{o}$? For example in $\mathbb{Z}[i]$ we have $5 = (2+i)(2-i)$, but 7 does not factorize in $\mathbb{Z}[i]$.
- What are the units in $\mathfrak{o}$? For example in $\mathbb{Z}[\sqrt{2}]$ we have $(\sqrt{2}+1)(\sqrt{2}-1) = 1$, so $\sqrt{2}+1$ is a unit. On the other hand the only units in $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1.

Instead of factorizing elements of $\mathfrak{o}$ we shall factorize ideals. If $\mathfrak{o}$ is a principal ideal domain then this is the same thing. We shall show that every ideal of $\mathfrak{o}$ can be uniquely factorized into prime ideals of $\mathfrak{o}$. Therefore if $\mathfrak{o}$ is a principal ideal domain then we have uniqueness of factorization of elements.

If $\mathfrak{o}$ is not a principal ideal domain then we can measure how far it is from being a principal ideal domain by calculating the class group:

$$Cl = \{ideals\}/\{principal\ ideals\}.$$

This turns out to be a finite group that measures the complexity of the field k and the ring $\mathfrak{o}$ in pretty much the same way that the homology groups in algebraic topology measure the complexity of a space. A rather specific aim of the course is for you to be able to calculate this group for some simple algebraic number fields. Eventually, you should try to produce yourself fields of various complexity.

1.1 Prerequisites for the course

Elementary linear algebra. Group theory and ring theory from MATH 7202, in particular ideals, quotient rings, polynomial rings over a field. A willingness to think flexibly with diverse mathematical notions.

1.2 Course Books

There are many books on algebraic number theory. The one by Stewart and Tall listed on the syllabus is a rather elementary introduction intended to be user-friendly at the undergraduate level. There is a book by Ireland and Rosen 'A classical invitation to modern number theory' that attempts to reach a similar readership, but contains a more sophisticated viewpoint. A book called 'Fermat's Dream' by Kazuya Kato et. al. adopts a highly inspirational approach emphasizing the role of zeta functions. 'A course in arithmetic' by J.-P. Serre deals with some rather sophisticated topics in a self-contained way. There is a set of online notes by James Milne available at www.jamesmilne.org that develops algebraic number theory in a fairly systematic manner at the post-graduate level.

2 Background Material

2.1 Polynomial Rings

In this course all rings will be commutative rings with 1. Let k be a field. We shall write $k[X]$ for the ring of polynomials in the variable X with coefficients in k. Recall that in any ring R there are three kinds of elements:

- The units;
- The reducible elements;
- The irreducible elements.

1 Proposition *$k[X]$ is an integral domain*

Proof. Let $f(X)$ and $g(X)$ be non-zero. Then they have the form

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

and

$$g(X) = b_0 + b_1X + \cdots + b_mX^m$$

with $a_n \neq 0$ and $b_m \neq 0$. But then the highest term of $f(X)g(X)$ is $a_nb_m \neq 0$. So $f(X)g(X) \neq 0$. □

We will frequently take a polynomial $f(X) \in \mathbb{Z}[X]$ and consider its *reduction modulo* p for a prime p. This is the polynomial $\bar{f}(X) \in \mathbb{F}_p[X]$ obtained by reducing all the coefficients of f mod p. For example, if $f(X) = 5X^4 + 9X^3 + 2X + 3$, then for the prime 3, we have

$$\bar{f} = [2]X^4 + [2]X \in \mathbb{F}_3[X].$$

Here, we are writing [2] for the congruence class in $\mathbb{F}_3$ of 2. But much of the time, we will omit the square brackets when the context makes the reduction clear. Also, in the notation $\bar{f}$, we will not indicate the prime p separately. It also will be indicated by the context.

For any polynomial $f(X) \in \mathbb{Q}[X]$, we will denote by $f_1(X) \in \mathbb{Z}[X]$ the unique constant multiple of f with the property that

(1) f_1 is *primitive*, that is, its coefficients are coprime.

(2) Its leading coefficient is positive.

One obtains $f_1(X)$ from $f(X)$ by first multiplying f by an integer c so that $cf(X) \in \mathbb{Z}[X]$. One then divides by the highest common factor r of the coefficients of cf to obtain $(c/r)f(X) \in \mathbb{Z}[X]$ primitive. One then multiplies $(c/r)f$ by 1 or -1 in order to make its leading coefficient positive. For example, if

$$f(X) = (-4)X^2 + (2/3)X + 10,$$

then one goes to

$$(-12)X^2 + 2X + 30$$

to

$$-6X^2 + X + 15$$

to

$$f_1 = 6X^2 - X - 15.$$

Exercise: Given $f \in \mathbb{Q}[X]$ show that $f_1(X)$ with the two properties above is unique.

In the ring $k[X]$ the units are the non-zero constant polynomials, i.e. the elements of $k^\times$. There are various ways of deciding whether elements of $\mathbb{Q}[X]$ are irreducible or not.

2 Gauss' Lemma *Suppose $f \in \mathbb{Z}[X]$ and assume that f is not constant. If f is irreducible as an element of $\mathbb{Z}[X]$ then f is irreducible as an element of $\mathbb{Q}[X]$.*

Proof. Suppose $f(X) = g(X)h(X)$ in $\mathbb{Q}[X]$. We have $g = ag_1$ and $h = bh_1$ for some constants $a, b \in \mathbb{Q}$, so that

$$f(X) = abg_1(X)h_1(X).$$

Claim: $g_1(X)h_1(X)$ is primitive.

Suppose some p divided all the coefficients of $g_1(X)h_1(X)$. Then

$$\bar{g}_1(X)\bar{h}_1(X) = 0 \in \mathbb{F}_p[X].$$

So either $\bar{g}_1(X) = 0$ or $\bar{h}_1(X) = 0$. But then, p would divide all the coefficients of either g_1 or h_1, contrary to the fact that they are both primitive. This proves the claim.

For each coefficient c_i of g_1h_1, we must have $abc_i \in \mathbb{Z}$, since $f \in \mathbb{Z}[X]$. But by Bezout's Lemma, there are integers n_i so that

$$\sum_i n_i c_i = 1.$$

Therefore,

$$\sum_i n_i abc_i = ab \sum_i n_i c_i = ab \in \mathbb{Z}.$$

From this, we get a decomposition

$$f = (abg_1)(h_1)$$

in $\mathbb{Z}[X]$. Therefore, either abg_1 or h_1 must be a unit in $\mathbb{Z}[X]$. And hence, one of g or h must be a unit in $\mathbb{Q}[X]$. □

In fact, the proof shows:

3 Refined Gauss Lemma *Suppose $f(X) \in \mathbb{Z}[X]$ and we can write $f(X) = g(X)h(X)$ in $\mathbb{Q}[X]$. Then there are constant multiples $g_{\mathbb{Z}}$ of g and $h_{\mathbb{Z}}$ of h such that $g_{\mathbb{Z}}, h_{\mathbb{Z}} \in \mathbb{Z}[X]$ and*

$$f(X) = g_{\mathbb{Z}}(X)h_{\mathbb{Z}}(X).$$

4 Corollary *Let $f \in \mathbb{Z}[X]$ have the form*

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

with $a_n \neq 0$. If r/s written in reduced form is a rational root of $f(X)$, then $r|a_0$ and $s|a_n$.

Proof. We have

$$f(X) = (X - r/s)g(X)$$

in $\mathbb{Q}[X]$. Thus, there must be constant multiples $a(X - r/s)$ and $bg(X)$ in $\mathbb{Z}[X]$ such that

$$f(X) = a(X - r/s)bg(X).$$

Now, since $aX - ar/s \in \mathbb{Z}[X]$, we have $a \in \mathbb{Z}$ and $ar/s \in \mathbb{Z}$. Since s is coprime to r, then we must have $s|a$. Since a is the leading term of $aX - ar/s$, it must divide the leading term of f, i.e., a_n. So $s|a_n$. Similarly, $ar/s = (a/s)r$ must divide the constant term of $f(X)$, i.e. a_0. So $r|a_0$. □

This result is interesting from the perspective of the theory of Diophantine equations, i.e., finding integral or rational solutions to polynomial equations, say,

$$2X^{10} + 3Y^{10} = 5Z^{10}.$$

In general, procedures for finding rational solutions are rare. But this corollary says that for polynomials in one variable, there is a clear-cut algorithm.

5 Corollary *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial. If $f(X)$ has a rational root a, then $a \in \mathbb{Z}$ and*

$$f(X) = (X - a)g(X)$$

with $g(X) \in \mathbb{Z}[X]$.

Proof. An immediate consequence of the previous corollary and its proof. □

If f is reducible in $k[x]$, then $f = gh$ for g, h of degree strictly less than $\deg f$. A *factorization* of f will refer to any product expression

$$f = f_1 f_2 \cdots f_n$$

with at least two f_i non-units of degree strictly less than $\deg f$. Sometimes we speak of a *proper* factorization, or a non-trivial factorization, as opposed trivial factorizations where all but one f_i are units.

6 Corollary *Let $f \in \mathbb{Z}[X]$ be monic of degree 2 or 3. If f factorizes in $\mathbb{Q}[X]$, then f has a root in $\mathbb{Z}$, which is a factor of the constant term of f.*

Proof. A factorization of f would look like $f = gh$ where both g and h have degree strictly less than f. But then, either g or h will have degree one, and f will have a rational root. Therefore, it will have an integral root. □

Thus, to check irreducibility of monic $f(X)$ of degree ≤ 3, we just need to evaluate $f(a)$ for $a \in \mathbb{Z}$ dividing the constant term of $f(X)$.

7 Example $X^3 + X + 1$ is irreducible, since any root would have to be a factor of 1.

Exercise: Generalize the previous corollary to $f \in \mathbb{Z}[x]$ of degree ≤ 3 that is not necessarily monic.

8 Eisenstein's Criterion *Let $f(X) = a_0 + a_1X + \ldots + a_nX^n$. If there is a prime number p such that*

- *p divides all but the leading coefficient of f;*
- *p^2 does not divide the constant coefficient of f;*

then f is irreducible.

9 Example $X^6 + 4X + 6$ is irreducible, since it satisfies Eisenstein's Criterion with the prime number 2.

10 Reduction modulo p *Let $f \in \mathbb{Z}[X]$ and let p be a prime number. We shall write $\bar{f} \in \mathbb{F}_p[X]$ for the reduction of f modulo p. Assume that f and $\bar{f}$ have the same degree. If $\bar{f}$ is an irreducible element of $\mathbb{F}_p[X]$ then f is irreducible over $\mathbb{Q}$. (Note that in $\mathbb{F}_p[X]$ there are only finitely many possibilities for factors since $\mathbb{F}_p$ is finite.)* $X^4 + X^3 + 1$ is irreducible, since $\overline{X^4 + X^3 + 1}$ is irreducible in $\mathbb{F}_2[X]$ (why?).

11 Change of Variable *Let $f \in \mathbb{Z}[X]$ and let $a \in \mathbb{Z}$. Then $f(X)$ is irreducible iff $f(X + a)$ is irreducible.*

Lecture 2

2.1.1 Euclid's Algorithm

For $f, g \in k[X]$ there is an highest common factor of f and g. This is the monic polynomial h of highest degree, which divides both f and g. If k also divides f and g then k is a factor of h. The highest common factor is calulated using the Euclidean algorithm: We divide f by g with remainder:

$$f = qg + r,$$

And then $\text{hcf}(f, g) = \text{hcf}(g, r)$. Also $\text{hcf}(f, 0) = f$.

For example take $f(X) = X^2 + 5X + 6$, $g(X) = X^3 - 4X$.

etc

12 Definition Any ring with a Euclidean algorithm is called a Euclidean ring. For example $\mathbb{Z}$ and $k[X]$ are Euclidean rings.

2.1.2 Ideals

Let R be a ring. An *ideal* of R is a non-empty subset $I \subseteq R$ such that:

- if $x, y \in I$ then $x + y \in I$;
- if $x \in I$ and $\lambda \in R$ then $\lambda x \in I$.

For example define for $x \in R$:

$$(x) = \{\lambda x : \lambda \in R\}.$$

ideals of this form are called *principal ideals.*

More generally,

$$(x_1, \ldots, x_n) = \left\{\sum \lambda_i x_i\right\}$$

is the ideal generated by $x_1, \ldots x_n$.

It is often the case that two generators can be replaced by one, for example in $\mathbb{Z}$

$$(4, 6) = (2), \quad (a, b) = (\text{hcf}(a, b)).$$

so $(4, 6)$ is a principle ideal. If every ideal of a ring R is principal then R is called a *principal ideal domain.*

13 Theorem *E very Euclidean ring is a principal ideal domain.*

Proof. Let I be an ideal and assume $I \neq (0)$. Choose $0 \neq x \in I$ of smallest possible degree. We show that every element of I is a multiple of x. Indeed if $y \in I$ then by the Euclidean algorithm we can write $y = qx + r$, where r has smaller degree than x. It follows that $r \in I$ so by choice of x we have $r = 0$. □

14 Corollary *$k[X]$ and $\mathbb{Z}$ are principal ideal domains.*

Proof. Both these rings have Euclidean algorithms. □

An ideal $I \subseteq R$ is a *maximal ideal* if

- $I \neq R$;
- If J is another ideal of R and $I \subseteq J$, then either $J = I$ or $J = R$.

Note that for principle ideals we have:

$$(a) \subseteq (b) \text{ iff } b|a.$$

From this we obtain:

15 Proposition *The maximal ideals of $k[X]$ are of the form (p), where p is an irreducible polynomial.*

2.1.3 Quotient rings

16 Definition Let I be an ideal of a ring R. We define R/I to be the set of additive cosets $a + I$ of I in R. We make R/I into a ring by defining

$$(a + I) + (b + I) := (a + b) + I,$$

$$(a + I)(b + I) := (ab) + I,$$

17 Theorem *Let R be a ring and let I be an ideal of R. Then I is maximal if and only if R/I is a field.*

2.1.4 Homomorphisms of rings

18 Definition Let R and S be rings. A homomorphism from R to S is a function $\phi : R \to S$ such that

- $\phi(a + b) = \phi(a) + \phi(b)$,
- $\phi(ab) = \phi(a)\phi(b)$,
- $\phi(1) = 1$.

19 Lemma *The kernel of a ring homomorphism is an ideal.*

Proof. Let $x, y \in \ker \phi$ and $\lambda \in R$. We have $\phi(x) = \phi(y) = 0$. Therefore $\phi(x + y) = 0 + 0 = 0$ and $\phi(\lambda x) = \phi(\lambda) \times 0 = 0$. This shows that $x + y \in \ker \phi$ and $\lambda x \in \ker \phi$. □

20 Lemma *If k is a field then $\{0\}$ and k are the only two ideals of k.*

Proof. Let I be a non-zero ideal and let $x \in I$ be a non-zero element of I. Since x has an inverse in K, we have for any element $y \in k$,

$$y = (yx^{-1})x \in I,$$

so $I = k$. □

21 Corollary *Let k be a field and $\phi : k \to R$ a ring homomorphism. Then ϕ is injective.*

Proof. $\ker(\phi)$ is an ideal of k, so is either 0 or k. Since $\phi(1) = 1$, we have $\ker(\phi) \neq k$. Therefore $\ker(\phi) = 0$. □

Lecture 3

2.2 Field extensions

22 Definition Let $k \subset L$ be two fields. We call k a subfield of L, and L an extension of k.

For example $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is an extension of $\mathbb{Q}$. On the other hand we have field extensions of the form $k[X]/(f)$, where f is an irreducible polynomial. We'll see that these two kinds of example are in fact the same.

23 Definition Let L be a field extension of k. An element $\alpha \in L$ is algebraic over k if there is a non-zero polynomial $f \in k[X]$ such that $f(\alpha) = 0$.

If α is algebraic over k we define the ring generated by α over k:

$$k[\alpha] = \{f(\alpha) : f \in k[X]\},$$

and the field generated by α:

$$k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in k[X], g(\alpha \neq 0 \right\}.$$

So we have

$$k \subseteq k[\alpha] \subseteq k(\alpha) \subseteq L.$$

We also define

$$I(\alpha) = \{f \in k[X] : f(\alpha) = 0\}.$$

24 Lemma *$I(\alpha)$ is an ideal of $k[X]$.*

25 Definition By the minimal polynomial of α we shall mean the monic polynomial m such that $I(\alpha) = (m)$.

26 Lemma *$I(\alpha)$ is maximal. Equivalently, m is irreducible.*

Proof. Suppose $m = ab$. We have

$$a(\alpha)b(\alpha) = m(\alpha) = 0.$$

therefore w.l.g. $a(\alpha) = 0$. Hence $a \in (m)$, so $m|a$. This implies $\deg m = \deg a$ and b is a constant. Hence m is irreducible. □

27 Lemma *m is the minimal polynomial of α if and only if ($m(\alpha) = 0$ and m is monic and irreducible).*

Proof. One direction is already proved. Assume m is monic and irreducible and $m(\alpha) = 0$. Then $m \in I(\alpha)$ so the real minimal polynomial must be a factor of m. Since m is irreducible, it is the minimal polynomial. □

28 Theorem *Let α be algebraic over k. Then $k(\alpha) = k[\alpha]$ and there is an isomorphism of fields:*

$$\Phi : k[X]/(m) \to k(\alpha), \qquad f + (m) \mapsto f(\alpha).$$

Proof.

1. We first show that Φ is well defined. If $f \equiv g \bmod I(\alpha)$ then $f - g \in I(\alpha)$, so $f(\alpha) - g(\alpha) = 0$. Hence $f(\alpha) = g(\alpha)$.
2. It is easy to check that Φ is a ring homomorphism. For example,
$$\Phi(f + g + I(\alpha)) = (f + g)(\alpha) = f(\alpha) + g(\alpha) = \Phi(f + I(\alpha)) + \Phi(g + I(\alpha)).$$
$$\Phi(fg + I(\alpha)) = (f \times g)(\alpha) = f(\alpha)g(\alpha) = \Phi(f + I(\alpha))\Phi(g + I(\alpha)).$$
3. The image if Φ is clearly $k[\alpha]$.
4. Since $I(\alpha)$ is maximal, $k[X]/I(\alpha)$ is a field, so Φ must be injective.
5. Therefore Φ is an isomorphism between $k[X]/I(\alpha)$ and $k[\alpha]$.
6. Since $k[X]/I(\alpha)$ is a field, it follows that $k[\alpha]$ is a field, so in fact $k(\alpha) = k[\alpha]$.

□

Lecture 4

29 Example Let $\alpha = \sqrt{2} + \sqrt{3}$. We have $\alpha^2 = 5 + 2\sqrt{6}$. Therefore $(\alpha^2 - 5)^2 - 24 = 0$. Thus α is a zero of the polynomial $m(X) = X^4 - 10X^2 + 1$. To show that m is the minimal polynomial we need to show that it is irreducible. Any linear factor would have to be of the form $X - a$ where $a$is a factor of 1 (by the Gauss Lemma). Since $m(1)$ and $m(-1)$ are non-zero, m has no linear factors over $\mathbb{Q}$, so we just need to check for quadratic factors. Suppose

$$m(X) = (X^2 + aX + b)(X^2 + cX + d), \quad a, b, c, d \in \mathbb{Z}.$$

Equating coefficients we have

$$a + c = 0, \quad ac + b + d = -10, \quad ad + bc = 0, \quad bd = 1.$$

For first and 4th equations give $c = -a$ and $b = d = \pm 1$. Then the second equation gives $a^2 = 10 \pm 2$, which is impossible since neither 8 nor 12 is a square. The theorem gives an isomorphism

$$\mathbb{Q}[X]/(X^4 - 10X^2 + 1) \cong \mathbb{Q}(\alpha).$$

The isomorphism takes $a + bX + cX^2 + dX^3 \bmod m$ to $a + b\alpha + c\alpha^2 + d\alpha^3$.

2.3 Degrees of extensions

30 Definition Let L be an extension of k. We can think of L as just a vector space over k be forgetting how to multiply two elements of L together. The dimension of L as a vector space over k is called the *degree of the extension.* This is written $[L : k]$.

31 Example $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$, so $[\mathbb{C} : \mathbb{R}] = 2$.

32 Example Let $f \in k[X]$ be an irreducible polynomial of degree d. Then $\{1, X, \ldots, X^{d-1}\}$ is a basis for $k[X]/(f)$. Therefore

$$[k[X]/(f) : k] = \deg(f).$$

33 Example Let α be algebraic over k and let m_α be its minimal polynomial over k. By the theorem, $k(\alpha)$ is isomorphic to $k[X]/(m)$, so by the previous example we have

$$[k(\alpha) : k] = \deg(m_\alpha).$$

34 Proposition *α is algebraic over k if and only if $[k(\alpha) : k] < \infty$.*

Proof. If α is algebraic over k then we've already proved this, since the degree of the extension is just the degree of it's minimal polynomial, which is finite. Conversely, suppose that $[k(\alpha) : k] = d < \infty$. Then the $d + 1$ vectors $1, \alpha, \ldots, \alpha^d$ cannot be linearly dependent over k. Thus there exist $\lambda_0, \ldots \lambda_d \in k$ not all zero such that $\sum \lambda_i \alpha^i = 0$. In other words α is algebraic over k. □

35 Tower Theorem *Suppose we have three fields $k \subset L \subset M$. Then $[M : k] = [M : L][L : k]$.*

Proof. Let $\{a_i\}$ be a basis for L over k and let $\{b_j\}$ be a basis for M over L. We'll show that $\{a_i b_j\}$ is a basis for M over k.

(Spanning) Let $v \in M$. then we can find $\lambda_j \in L$ such that $v = \sum \lambda_j b_j$. Similarly for each λ_j we can find $\mu_{i,j} \in k$ such that $\lambda_j = \sum_i \mu_{i,j} a_i$. Hence $v = \sum_{i,j} \mu_{i,j} a_i b_j$.

(Linear independence) Suppose we have $\mu_{i,j} \in k$ with $\sum_{i,j} \mu_{i,j} a_i b_j = 0$. Let $\lambda_j = \sum_i \mu_{i,j} a_i$, so $\lambda_j \in L$ and $\sum_j \lambda_j b_j = 0$. Since $\{b_j\}$ is linearly independent over L, it follows that the λ_j are all 0. Then since $\{a_i\}$ is linearly independent over k, it follows that the $\mu_{i,j}$ are all 0. □

36 Corollary *Let L be a field extension of k and let L^{alg} be the set of elements of L, which are algebraic over k. Then L^{alg} is a field.*

Proof. Let α, β be algebraic over k. Note that β is also algebraic over $k(\alpha)$. Therefore the degrees $[k(\alpha, \beta) : k(\alpha)]$ and $[k(\alpha) : k]$ are both finite, so by the tower theorem $[k(\alpha, \beta) : k]$ is finite. Let γ be one of the numbers $\alpha + \beta$, $\alpha\beta$, α/β. Since $\gamma \in k(\alpha, \beta)$ it follows that $[k(\gamma) : k]$ is finite, and hence γ is algebraic over k. This shows that L^{alg} is closed under the field operations, so is a subfield of L. □

37 Corollary *The algebraic numbers form a subfield of $\mathbb{C}$.*

Proof. This is a special case of the previous corollary with $k = \mathbb{Q}$ and $L = \mathbb{C}$. □

Lecture 5

Here are two results about subfields of $\mathbb{C}$.

38 Galois' Separability Theorem *Let k be a subfield of $\mathbb{C}$ and let $f \in k[X]$ be irreducible. Then f has no repeated roots in $\mathbb{C}$, i.e. $f(X) = \prod_{i=1}^{d}(X - \alpha_i)$ with $\alpha_i \in \mathbb{C}$ distinct.*

Proof. Suppose α is a repeated root, so we have over $\mathbb{C}$:

$$f(X) = (X - \alpha)^2 g(X).$$

Then $f'(X) = 2(X - \alpha)g(X) + (X - \alpha)^2 g'(X)$. Hence $f'(\alpha) = 0$, so $f' \in I(\alpha)$. However, since f is irreducible, it is the minimal polynomial of α, so we've shown that $f | f'$. This is impossible since f' has smaller degree than f. □

39 Remark This proof fails in fields containing $\mathbb{F}_p$, since in such fields f' can be zero. For example the polynomial $X^p - a$ has derivative 0 for any constant a.

40 Primitive element theorem *Let L be a finite degree extension of k, and assume that $k \subset L \subset \mathbb{C}$. Then there exists an element $\theta \in L$ such that $L = k(\theta)$.*

The generator $\theta \in L$ is called a *primitive element.*

41 Example The element $\sqrt{2} + \sqrt{3}$ is primitive in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. To see this, we note that $\sqrt{2} + \sqrt{3}$ has minimal polynomial $X^4 - 10X^2 + 1$, which has degree 4. Therefore $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. On the other hand by the tower theorem, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq 4$.

Proof. We can certainly find $\alpha_1, \ldots \alpha_n \in L$ such that $L = k(\alpha_1, \ldots, \alpha_n)$, so it is sufficient to show that in any field extension of the form $L = k(\alpha, \beta)$ there is a primitive element.

Let p be the minimal polynomial of α and let q be the minimal polynomial of β. Let $\alpha_1, \ldots, \alpha_n$ be the zeros of p (with $\alpha_1 = \alpha$) and let $\beta = \beta_1, \beta_2, \ldots, \beta_m$ be the zeros of q. The trick is to choose $c \in k$ so that $\alpha + c\beta \neq \alpha_i + c\beta_j$ unless $i = j = 1$. This is possible since k is infinite and each of these equations has at most one solution.

Now let $\theta = \alpha + c\beta$; we'll show that $k(\alpha, \beta) = k(\theta)$. For this it's sufficient to show that $\beta \in k(\theta)$. Define $r \in k(\theta)[X]$ by:

$$r(X) = p(\theta - cX).$$

We note that $r(\beta) = p(\alpha) = 0$; furthermore, by our choice of c, $r(\beta_j) \neq 0$ for $j \neq 1$. Thus β is the only common zero of q and r.

Let m be the minimal polynomial of β over $k(\theta)$. Since $q(\beta) = 0$ we know that $m | q$. Similarly $m | r$. Hence any zero of m would be a common zero of q and r.

We've shown that β is the only zero of m. By Galois' Separability Theorem, m has no repeated roots, so $m(X) = X - \beta$. Thus $\beta \in k(\theta)$. □

Lecture 6

2.4 Symmetric polynomials

42 Definition Let k be a field and let $f \in k[X_1, \ldots, X_n]$. Then f is called a symmetric polynomial if for all permutations $\sigma \in S_n$ we have

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n).$$

43 Example For example $X + Y$, XY, $X^2 + 3XY + Y^2$ are symmetric polynomials in 2 variables.

The elementary symmetric polynomials are

$$s_1 = X_1 + \ldots + X_n,$$

$$s_2 = \sum_{1 \le i < j \le n} X_i X_j$$

$$s_3 = \sum_{1 \le i < j < k \le n} X_i X_j X_k.$$

etc. up to

$$s_n = X_1 X_2 \cdots X_n.$$

These arise as follows: if

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

Then expanding this we obtain

$$f(X) = X^n - s_1(\alpha) X^{n-1} + \ldots + (-1)^n s_n(\alpha).$$

44 Newton's Theorem *The ring of symmetric polynomials is generated as a ring over k by the elementary symmetric polynomials.*

Proof. The idea is to order the monimials lexicographically:

$$X_1^{a_1} \cdots X_n^{a_n} > X_1^{b_1} \cdots X_n^{b_n}$$

iff $a_1 > b_1$ or $a_1 = b_1$ and $a_2 > b_2$ ... etc. We can therefore define the leading term of a polynomial in n variables. If f is symmetric then its leading term satisfies $a_1 \ge a_2 \ge$ etc.

There is also a monomial in the symmetric polynomials with the same leading term:

$$s_n^{a_n} s_{n-1}^{a_{n-1} - a_n} \cdots.$$

After subtracting a multiple of this expression we obtain something with smaller leading term. The proof proceeds by induction. □

45 Example Let $f(X) = X^3 + Y^3 + Z^3$. We have

$$\begin{aligned} X^3+Y^3+Z^3 &= (X+Y+Z)^3 \\ &\quad -3(X^2Y+Y^2Z+Z^2X+XY^2+YZ^2+ZX^2) \\ &\quad -6XYZ \\ &= s_1^3 \\ &\quad -3((X+Y+Z)(XY+YZ+ZX)-3XYZ) \\ &\quad -6s_3 \\ &= s_1^3 - 3(s_1s_2-3s_3) - 6s_3 \\ &= s_1^3 - 3s_1s_2 + 3s_3. \end{aligned}$$

So if α, β, γ are the zeros of the polynomial $X^3 + 3X^2 + 6X + 15$ then

$$\alpha^3 + \beta^3 + \gamma^3 = (-3)^3 - 3(-3 \times 6) + 3 \times (-15) = -27 + 54 - 45 = -18.$$

46 Example Let

$$\Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

We'll express this in terms of

$$\Sigma\alpha = \alpha + \beta + \gamma, \quad \Sigma\alpha\beta = \alpha\beta + \beta\gamma + \gamma\alpha, \quad \Pi\alpha = \alpha\beta\gamma.$$

etc.

47 Example

$$\begin{aligned} x^4+y^4+z^4 &= (x+y+z)^4 - 6(x^2y^2+y^2z^2+z^2x^2) \\ &\quad -4(x^3y+y^3z+z^3x+xy^3+yz^3+zx^3) - 12(x^2yz+xy^2z+xyz^2) \\ &= s_1^4 - 6((xy+yz+zx)^2 - 2(x^2yz+xy^2z+xyz^2)) \\ &\quad -4((x^2+y^2+z^2)(xy+yz+zx) - (x^2yz+xy^2z+xyz^2)) - 12s_1s_3 \\ &= s_1^4 - 6(s_2^2 - 2s_1s_3) \\ &\quad -4(((x+y+z)^2 - 2(xy+yz+zx))s_2 - s_1s_3) - 12s_1s_3 \\ &= s_1^4 - 6s_2^2 + 12s_1s_3) \\ &\quad -4((s_1^2 - 2s_2)s_2 - s_1s_3) - 12s_1s_3 \\ &= s_1^4 - 6s_2^2 - 4s_1^2s_2 + 8s_2^2 + 4s_1s_3 \\ &= s_1^4 - 4s_1^2s_2 + 2s_2^2 + 4s_1s_3. \end{aligned}$$

2.5 k-Homomorphisms *

48 Definition Suppose L and M are two field extensions of k. A k-homomorphism from L to M is a map $\phi : L \to M$ such that

- ϕ is a ring homomorphism;
- if $x \in k$ then $\phi(x) = x$.

49 Example Let α be algebraic over k with minimal polynomial m. We've shown that there is an isomorphism $k[X]/(m) \cong k(\alpha)$ which takes $f + (m)$ to $f(\alpha)$. This is clearly a k-homomorphism.

50 Lemma *Suppose $\phi : L \to M$ is a k-homomorphism. Then for any polynomial $f \in k[X]$ and any $\alpha \in L$, $f(\phi(\alpha)) = \phi(f(\alpha))$.*

51 Definition Let α, β be algebraic over k. Then α and β are said to be k-conjugate if they have the same minimal polynomial over k.

52 Corollary *Suppose $\phi : L \to M$ is a k-homomorphism. Then for any $\alpha \in L$, $\phi(\alpha)$ is k-conjugate to α.*

53 Corollary *Let $\phi : k(\alpha_1, \ldots, \alpha_n) \to L$ be a k-homomorphism. Then ϕ is determined by the values $\phi(\alpha_1), \ldots, \phi(\alpha_n)$.*

2.6 Splitting fields and Galois groups *

54 Definition Let k be a subfield of $\mathbb{C}$ and let $f \in k[X]$ be any polynomial. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be the zeros of f. By the *splitting field* of f we shall mean the field $k(\alpha_1, \ldots, \alpha_n)$.

55 Corollary *Let k be a subfield of $\mathbb{C}$ and let L be a finite extension of k. Then there are exactly $[L : k]$ k-homomorphisms from L to $\mathbb{C}$.*

56 Corollary *Let k be a subfield of $\mathbb{C}$ and let L be a splitting field over k. Then there are exactly $[L : k]$ k-automorphisms of L.*

57 Definition Let L be a splitting field over k. The *Galois group* of L over k is the group of k-automorphisms of L. This is written $\mathrm{Gal}(L/k)$.

So we have proved:

58 Main theorems of Galois Theory *For any splitting field L over k we have $\mathrm{Gal}(L/k) = [L : k]$.*

59 Definition If L is a field and G is a group of automorphisms of L then we define the *fixed field* of G by

$$L^G = \{\alpha \in L : \forall \phi \in G,\ \phi(\alpha) = \alpha\}.$$

Note that L^G is a subfield of L, since if α and β are fixed by ϕ then so are $\alpha + \beta$, $\alpha\beta$, α/β, etc.

60 Corollary *If L is a splitting field over k then $L^{\mathrm{Gal}(L/k)} = k$.*

Proof. Let $G = \mathrm{Gal}(L : k)$. Every element of G fixes k, so

$$k \subseteq L^G \subseteq L.$$

Furthermore L is a splitting field over L^G (with the same polynomial as over k). By definition, every element of G fixes L^G, so we have

$$\mathrm{Gal}(L/k) = \mathrm{Gal}(L/L^G).$$

Hence by the main theorem of Galois theory,

$$[L : k] = [L : L^G].$$

Hence by the tower theorem,

$$[L^G : k] = 1.$$

□

2.7 Calculating Galois groups *

quadratic fields. cubic fields.

Lecture 7

3 Algebraic Number Fields

3.1 Field embeddings

61 Definition An *algebraic number field* is a finite degree extension of $\mathbb{Q}$.

62 Remark By the primitive element theorem, every algebraic number field is of the form $k = \mathbb{Q}(\alpha)$ for some algebraic number α. The degree of the extension is the degree of the minimal polynomial m of α. Furthermore k is isomorphic to $\mathbb{Q}[X]/(m)$. The isomorphism takes α to $X + (m)$.

63 Definition If k is an algebraic number field then a *field embedding* is a homomorphism $\sigma : k \to \mathbb{C}$. Note that since k is a field, the field embeddings are all injective.

64 Lemma *If $\sigma : k \to \mathbb{C}$ is an embedding then for any $x \in \mathbb{Q}$ we have $\sigma(x) = x$.*

65 Lemma *If $f \in \mathbb{Q}[X]$ and $\sigma : k \to \mathbb{C}$ is an embedding then for any $x \in k$ we have $f(\sigma(x)) = \sigma(f(x))$.*

Proof. Let $f(X) = \sum a_n X^n$ with $a_n \in \mathbb{Q}$. Since σ is a ring homomorphism we have:

$$\begin{aligned} \sigma(f(x)) &= \sigma\left(\sum a_n x^n\right) \\ &= \sum \sigma(a_n)\sigma(x)^n \\ &= \sum a_n \sigma(x)^n \\ &= f(\sigma(x)). \end{aligned}$$

□

66 Lemma *If $k = \mathbb{Q}(\alpha)$ and $\sigma : k \to \mathbb{C}$ is an embedding then σ is determined by $\sigma(\alpha)$.*

Proof. Let $x \in k$. We have $x = g(\alpha)$ for some $g \in \mathbb{Q}[X]$. But then by the previous lemma, $\sigma(x) = g(\sigma(\alpha))$. □

67 Definition Two algebraic numbers α, β are $\mathbb{Q}$-conjugate if they have the same minimal polynomial over $\mathbb{Q}$.

68 Lemma *If $\sigma : k \to \mathbb{C}$ is an embedding then for any $x \in k$, $\sigma(x)$ and x are $\mathbb{Q}$-conjugate.*

Proof. Let m be the minimal polynomial of x. Then m is irreducible over $\mathbb{Q}$ and $m(\sigma(x)) = \sigma(m(x)) = \sigma(0) = 0$. Therefore m is the minimal polynomial of $\sigma(x)$. □

69 Theorem *Let $d = [k : \mathbb{Q}]$. Then there are exactly d field embeddings $\sigma_1, \ldots \sigma_d : k \to \mathbb{C}$.*

Proof. Let $k = \mathbb{Q}(\alpha)$; let m be the minimal polynomial of α and let $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ be the conjugates of α. For each conjugate α_i there is at most one field embedding such that $\sigma(\alpha) = \alpha_i$. We must prove that this field embedding actually exists. We construct it as the composition of the field isomorphisms which we already have:

$$\begin{array}{ccccccc} \mathbb{Q}(\alpha) & \to & \mathbb{Q}[X]/(m) & \to & \mathbb{Q}(\alpha_i) & \subset & \mathbb{C} \\ \alpha & \mapsto & X + (m) & \mapsto & \alpha_i & & \end{array}$$

□

70 Example Let $k = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. The two field embeddings are

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}, \quad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}.$$

71 Example Let $k = \mathbb{Q}(\alpha)$ where α is a zero of $m(X) = X^3 + 2X + 2$. Note that m is irrediculble by Eisenstein's criterion, so $[k : \mathbb{Q}] = 3$ and we have

$$k = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}.$$

Let β, γ be the other two zeroes of f. The three field embeddings are

$$\sigma_1(a + b\alpha + c\alpha^2) = a + b\alpha + c\alpha^2, \quad \sigma_2(a + b\alpha + c\alpha^2) = a + b\beta + c\beta^2, \quad \sigma_2(a + b\alpha + c\alpha^2) = a + b\gamma + c\gamma^2.$$

Lecture 8

3.2 Norm, Trace and Discriminant

72 Definition Let k be an algebraic number field of degree d over $\mathbb{Q}$ and let $\sigma_1, \ldots, \sigma_d$ be the field embeddings of k. For $x \in k$ we define the *norm* and *trace* of x by

$$\mathrm{N}(x) = \prod \sigma_i(x), \quad \mathrm{Tr}(x) = \sum \sigma_i(x).$$

From the definition, it appears that the norm and trace are simply complex numbers. However we have:

73 Proposition *For $x \in k$, the norm and trace of x are in $\mathbb{Q}$.*

Proof. Let $k = \mathbb{Q}(\alpha)$ and let $\alpha_1, \ldots, \alpha_d$ be the conjugates of α in $\mathbb{C}$. We have $x = g(\alpha)$ for some $g \in \mathbb{Q}[X]$. Therefore

$$\mathrm{N}(x) = \prod \sigma_i(g(\alpha)) = \prod g(\sigma_i(\alpha)) = \prod g(\alpha_i).$$

This is clearly a symmetric polynomial in $\alpha_1, \ldots, \alpha_d$, so is in $\mathbb{Q}$. Similarly

$$\mathrm{Tr}(x) = \sum g(\alpha_i) \in \mathbb{Q}.$$

□

74 Proposition $N(xy) = N(x)N(y)$ *and* $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$.

Proof. easy. □

75 Example Let $k = \mathbb{Q}(\sqrt{2})$. We have

$$\mathrm{N}(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2,$$

$$\mathrm{Tr}(a + b\sqrt{2}) = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a.$$

76 Definition Let $\mathcal{B}$ be a basis for an algebraic number field k as a vector space over $\mathbb{Q}$. The *disriminant* of $\mathcal{B}$ is defined to be

$$\Delta(\mathcal{B}) = \det(\mathrm{Tr}(b_i b_j))_{i,j=1}^{d}, \quad \mathcal{B} = \{b_1, \ldots, b_d\}$$

Since Tr takes rational values, the discriminant is always a rational number. Note that we have a bilinear form $f : k \times k \to \mathbb{Q}$ defined by

$$f(v, w) = \mathrm{Tr}(vw).$$

We see that the discriminant of $\mathcal{B}$ is simply the determinant of the matrix of f with respect to $\mathcal{B}$.

77 Proposition *Let $\sigma_1, \ldots, \sigma_d : k \to \mathbb{C}$ be the field embeddings of k. For any basis $\mathcal{B} = \{b_1, \ldots, b_d\}$ we have:*

$$\Delta(\mathcal{B}) = \det(\sigma_i(b_j))^2.$$

Proof. Let $A = (\sigma_i(b_j))$. The i,j-entry of A^tA is given by

$$(A^tA)_{i,j} = \sum_k \sigma_k(b_i)\sigma_k(b_j) = \mathrm{Tr}(b_ib_j).$$

Therefore $\Delta\mathcal{B} = \det(A^tA) = \det(A)^2$. □

78 Example Let $k = \mathbb{Q}(\sqrt{2})$. Then we have

$$\Delta\{1, \sqrt{2}\} = \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix} = 8.$$

79 Remark Note that we have a symmetric bilinear form $f : k \times k \to \mathbb{Q}$ defined by

$$f(v, w) = \mathrm{Tr}(vw).$$

We see that the discriminant of $\mathcal{B}$ is simply the determinant of the matrix of f with respect to $\mathcal{B}$.

80 Corollary *If $\mathcal{C}$ is another basis and Λ is the transition matrix from $\mathcal{B}$ to $\mathcal{C}$ (i.e. $c_i = \sum \lambda_{i,j} b_j$) then*

$$\Delta(\mathcal{C}) = \det(\Lambda)^2 \cdot \Delta(\mathcal{B}).$$

Proof. This follows from the basis change formula for symmetric bilinear forms. □

81 Vandermonde Determinants

$$\det \begin{pmatrix} 1 & X_1 & \ldots & X_1^{d-1} \\ 1 & X_2 & \ldots & X_2^{d-1} \\ \vdots & & & \vdots \\ 1 & X_d & \ldots & X_d^{d-1} \end{pmatrix} = \prod_{i>j} (X_i - X_j).$$

Proof. By induction on n. If $n = 1$ then this is easy. Assume the result in the $(n-1) \times (n-1)$ case.

can do the following row and column operations:

$$\begin{aligned}
\det\begin{pmatrix} 1 & X_1 & \dots & X_1^{d-1} \\ \vdots & & & \vdots \\ 1 & X_d & \dots & X_d^{d-1} \end{pmatrix} &= \det\begin{pmatrix} 0 & X_1 - X_d & \dots & X_1^{d-1} - X_d^{d-1} \\ \vdots & & & \vdots \\ 0 & X_{d-1} - X_d & \dots & X_{d-1}^{d-1} - X_d^{d-1} \\ 1 & X_d & \dots & X_d^{d-1} \end{pmatrix} \\
&= (-1)^{d-1} \det\begin{pmatrix} X_1 - X_d & \dots & X_1^{d-1} - X_d^{d-1} \\ \vdots & & \vdots \\ X_{d-1} - X_d & \dots & X_{d-1}^{d-1} - X_d^{d-1} \end{pmatrix} \\
&= (-1)^{d-1} \prod_{i=1}^{d-1} (X_i - X_d) \det\begin{pmatrix} 1 & X_1 + X_d & \dots & X_1^{d-2} + \ldots + X_d^{d-2} \\ \vdots & & & \vdots \\ 1 & X_{d-1} + X_d & \dots & X_{d-1}^{d-2} + \ldots + X_d^{d-2} \end{pmatrix} \\
&= \prod_{i=1}^{d-1} (X_d - X_i) \det\begin{pmatrix} 1 & X_1 \dots & X_1^{d-2} \\ \vdots & & \vdots \\ 1 & X_{d-1} \dots & X_{d-1}^{d-2} \end{pmatrix} \\
&= \prod_{i=1}^{d-1} (X_d - X_i) \prod_{1 \le i < j \le d-1} (X_j - X_i) \\
&= \prod_{1 \le i < j \le d} (X_j - X_i)
\end{aligned}$$

□

82 Corollary *Let $k = \mathbb{Q}(\alpha)$ be an algebraic number field and let $\alpha_1, \dots, \alpha_d$ be the conjugates of α. Then*

$$\Delta\{1, \alpha, \dots, \alpha^{d-1}\} = \prod_{i>j} (\alpha_i - \alpha_j)^2.$$

Proof. By the proposition, we can see that the discriminant is a square of a Vandermonde determinant. □

83 Corollary *For any basis $\mathcal{B}$, we have $\Delta\mathcal{B} \neq 0$.*

Proof. This follows from the previous corollary in the case $\mathcal{B} = \{1, \alpha, \dots, \alpha^{d-1}\}$. The general case follows from the basis change formula. □

Lecture 9

3.3 Algebraic Integers

84 Definition Let L be a field extension of $\mathbb{Q}$. An element $\alpha \in L$ is called an *algebraic integer* if there is a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.

85 Example $\sqrt{2}$ is an algebraic integer; the monic polynomial is $X^2 - 2$.

86 Lemma *α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group.*

Proof. Suppose α is an algebraic integer, and let $f(\alpha) = 0$, where

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0, \quad a_0, \ldots, a_{d-1} \in \mathbb{Z}.$$

Clearly $\mathbb{Z}[\alpha]$ is generated as a group by $\{\alpha^i : i \geq 0\}$. We shall show that it is in fact generated by $\{1, \alpha, \ldots, \alpha^{m-1}\}$. To show this, it is sufficient to prove that for $m \geq n$, we have $\alpha^m \in \text{span}_{\mathbb{Z}}\{1, \alpha, \ldots, \alpha^{m-1}\}$. Since $f(\alpha) = 0$, it follows that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_0.$$

Therefore

$$\alpha^m = -a_{n-1}\alpha^{m-1} - \ldots - a_0\alpha^{m-n} \in \text{span}_{\mathbb{Z}}\{1, \alpha, \ldots, \alpha^{m-1}\}.$$

Conversely, suppose

$$\mathbb{Z}[\alpha] = \text{span}_{\mathbb{Z}}\{b_1, \ldots, b_n\}.$$

Each b_i can be expanded in terms of α:

$$b_i = \sum_{j=0}^{N-1} a_{i,j}\alpha^j, \qquad a_{i,j} \in \mathbb{Z}.$$

Since $\alpha^N \in \mathbb{Z}[\alpha]$, it can be expanded in terms of $\{b_1, \ldots, b_n\}$:

$$\alpha^N = \sum_{i=1}^{n} x_i b_i, \qquad x_i \in \mathbb{Z}$$

Substituting the previous equation, we have

$$\alpha^N = \sum_{i=1}^{n} \sum_{j=0}^{N-1} x_i a_{i,j} \alpha^j.$$

Rearranging this, we can see that α is a zero of a monic polynomial with integer coefficients. □

87 Corollary *Let L be any field containing $\mathbb{Q}$. The algebraic integers in L form a subring of L. (i.e. they are closed under addition and multiplication).*

Proof. Let α and β be algebraic integers, and assume

$$\mathbb{Z}[\alpha] = \text{span}_{\mathbb{Z}}\{g_1, \ldots g_n\}, \quad \mathbb{Z}[\alpha] = \text{span}_{\mathbb{Z}}\{h_1, \ldots h_m\}.$$

Then clearly every monomial is in the additive group generated by the products:

$$\alpha^i \beta^j \in \text{span}_{\mathbb{Z}}\{g_i h_j\}.$$

Therefore

$$\mathbb{Z}[\alpha, \beta] \subset \mathrm{span}_{\mathbb{Z}}\{g_i h_j\}.$$

It follows that $\mathbb{Z}[\alpha, \beta]$ is a finitely generated additive group. Now suppose $\gamma = \alpha\beta$ or $\alpha + \beta$. Then we have $\mathbb{Z}[\gamma] \subset \mathbb{Z}[\alpha, \beta]$ so $\mathbb{Z}[\gamma]$ is also finitely generated. By the lemma it follows that γ is an algebraic integer. □

88 Definition For an algebraic number field k, we shall write $\mathfrak{o}_k$ for the ring of algebraic integers in k.

89 Lemma *Let α have minimal polynomial m_α. Then α is an algebraic integer if and only if $m_\alpha \in \mathbb{Z}[X]$.*

Proof. If m_α has integer coefficients then clearly α is an algebraic integer. Conversely, assume $f(\alpha) = 0$ for some monic polynomial $f \in \mathbb{Z}[X]$. By definition, we have $f \in I(\alpha) = (m_\alpha)$. Therefore $f = qm_\alpha$ for some $q \in \mathbb{Q}[X]$. However by the Gauss Lemma, there is a constant $c \in \mathbb{Q}^\times$ such that both $c \times q$ and $c^{-1} \times m_\alpha$ have integer coefficients. Since both f and q are monic, it follows that q is monic. Hence both c and c^{-1} are integers, so $c = \pm 1$. This implies that $m_\alpha \in \mathbb{Z}[X]$. □

Using the lemma we easily determine whether an element is an algebraic integer or not.

90 Example $\mathfrak{o}_{\mathbb{Q}} = \mathbb{Z}$. This follows because the minimal polynomial of a rational number α is always $X - \alpha$.

91 Example Let $k = \mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$. Suppose $\alpha = a + ib$ is an algebraic integer with $b \neq 0$. The minimal polynomial of α is

$$m(X) = (X - \alpha)(X - \bar{\alpha}) = X^2 - 2aX + (a^2 + b^2).$$

Therefore $\alpha \in \mathfrak{o}_k$ if and only if both $2a$ and $a^2 + b^2$ are in $\mathbb{Z}$. The only way this can happen is if both a and b are in $\mathbb{Z}$. Hence

$$\mathfrak{o}_k = \mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}.$$

92 Corollary *Let $x \in \mathfrak{o}_k$. Then $N(x), \mathrm{Tr}(x) \in \mathbb{Z}$. If $\mathcal{B}$ is a basis for k over $\mathbb{Q}$ and $\mathcal{B} \subset \mathfrak{o}_k$ then $\Delta(\mathcal{B}) \in \mathbb{Z} \setminus \{0\}$*

Proof. The images $\sigma_i(x)$ are conjugates of x so have the same minimal polynomial. By the lemma, they must also be algebraic integers. Since the algebraic integers in $\mathbb{C}$ form a ring, the norm and trace of x must also be algebraic integers. However the norm and trace are also rational numbers, and we have already seen that $\mathfrak{o}_{\mathbb{Q}} = \mathbb{Z}$. This shows that the norms and traces of algebraic integers are integers. The discriminant of a basis of algebraic integers is therefore the determinant of a matrix of integers, so is also an integer. We have already proved that the discriminant is non-zero. □

Lecture 10

3.4 Integral Bases

93 Definition Let $\mathcal{B} = \{b_1, \ldots, b_d\}$ be a basis for k over $\mathbb{Q}$. We shall cal $\mathcal{B}$ an *integral basis* if

$$\mathfrak{o}_k = \left\{ \sum_{i=1}^{d} x_i b_i : x_1, \ldots x_d \in \mathbb{Z} \right\}.$$

94 Example $\{1\}$ is an integral basis in $\mathbb{Q}$.

95 Example $\{1, i\}$ is an integral basis in $\mathbb{Q}(i)$.

We'll prove that integral bases always exist and describe an algorithm for calculating them.

96 Lemma *For any $\alpha \in k$ there is an $N \in \mathbb{N}$ such that $N\alpha \in \mathfrak{o}_k$.*

Proof. Let m be the minimal polynomial of α, and suppose $d = \deg(m)$. Then $N^d m(X/N)$ is the minimal polynomial of $N\alpha$ ($N\alpha$ is a zero of this polynomial, and it is also monic and irreducible, so must be the minimal polynomial). The coefficients of $N^d m(X/N)$ are $N^{d-i}a_i$. We may choose N so that these rational numbers are all integers. □

97 Corollary *There is a basis $\mathcal{B}$ for k over $\mathbb{Q}$ such that $\mathcal{B} \subset \mathfrak{o}_k$.*

Proof. Choose any basis and multiply the basis vectors by natural numbers to make them algebraic integers. □

98 Theorem *Let k be an algebraic number field. Then there is an integral basis of k. More precisely if $\mathcal{B} \subset \mathfrak{o}_k$ is chosen so that $|\Delta\mathcal{B}|$ is as small as possible then $\mathcal{B}$ is an integral basis.*

Proof. Since $\mathcal{B} \subset \mathfrak{o}_k$ we clearly have

$$\mathrm{span}_{\mathbb{Z}}\mathcal{B} \subseteq \mathfrak{o}_k.$$

Suppose $\mathcal{B}$ is not an integral basis, so there is an algebraic integer

$$\theta = \sum x_i b_i, \quad x_i \in \mathbb{Q},$$

with x_i not all in $\mathbb{Z}$. By subtracting a suitable algebraic integer we may assume that $0 \leq x_i < 1$ for all i. Without loss of generality we assume that $x_1 \neq 0$. Now consider the new basis

$$\mathcal{C} = \{\alpha, b_2, \ldots, b_d\}.$$

The transition matrix from $\mathcal{B}$ to $\mathcal{C}$ is

$$M = \begin{pmatrix} x_1 & & & & \\ x_2 & 1 & & & \\ x_3 & & 1 & & \\ \vdots & & & \ddots & \\ x_d & & & & 1 \end{pmatrix}.$$

Since $\det M = x_1 \neq 0$ it follows that $\mathcal{C}$ genuinely is a basis. Now by the basis change formula for discriminants we have

$$\Delta(\mathcal{C}) = x_1^2 \Delta(\mathcal{B}).$$

Since $0 < x_i < 1$ we have $|\Delta\mathcal{C}| < |\Delta\mathcal{B}|$. However $\mathcal{C} \subset \mathfrak{o}_k$, so this contradicts our choice of $\mathcal{B}$. □

By looking at the proof of this theorem we can find an algorithm for finding an integral basis.

1. Start with any basis $\mathcal{B} \subset \mathfrak{o}$.
2. Calculate $\Delta(\mathcal{B})$ and let N be the largest natural number whose square divides $\Delta(\mathcal{B})$.
3. For each element of the form

$$\theta = \frac{1}{N} \sum a_i b_i, \quad a_i \in \{0, \ldots, N-1\} \text{ not all } 0,$$

   determine whether θ is an algebraic integer. If it is then replace one of the basis vectors by θ to get a new basis with discriminant of smaller absolute value, and go back to step 2.
4. If none of the θ are algebraic integers (or in $N = 1$) then $\mathcal{B}$ is an integral basis.

99 Example $k = \mathbb{Q}(\sqrt{-3})$.

Lecture 11

3.5 Integral bases in quadratic fields

We've seen that in $\mathbb{Q}(i)$ the basis $\{1, i\}$ is an integral basis, whereas in $\mathbb{Q}(\sqrt{-3})$ the basis $\{1, \frac{1+\sqrt{-3}}{2}\}$ is an integral basis. We'll now describe a result which generalizes these two examples.

100 Definition An algebraic number field k is called a *quadratic field* if $[k : \mathbb{Q}] = 2$.

If k is a quadratic field then by the primitive element theorem we have $k = \mathbb{Q}(\alpha)$, where α has minimal polynomial $m(X) = X^2 + bX + c$, $a, b \in \mathbb{Q}$. This means $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$, so we have $k = \mathbb{Q}(\sqrt{b^2 - 4c})$. Therefore every quadratic field is of the form $\mathbb{Q}(\sqrt{x})$ with $x \in \mathbb{Q}^\times$ not a perfect square. Obviously for $y \in \mathbb{Q}^\times$ we have $\mathbb{Q}(\sqrt{y^2 x}) = \mathbb{Q}(\sqrt{x})$ so we may also assume that x is a square-free integer. We therefore have:

101 Proposition *If k is a quadratic field then $k = \mathbb{Q}(\sqrt{n})$ for some square-free $n \in \mathbb{Z} \setminus \{0, 1\}$.*

We can now describe an integral basis in each quadratic field.

102 Theorem *Let $n \in \mathbb{Z} \setminus \{0, 1\}$ be square-free and let $k = \mathbb{Q}(\sqrt{n})$.*

- *If $n \not\equiv 1 \bmod 4$ then $\{1, \sqrt{n}\}$ is an integral basis in k.*
- *If $n \equiv 1 \bmod 4$ then $\left\{1, \frac{1+\sqrt{n}}{2}\right\}$ is an integral basis in k.*

Proof. First suppose $n \not\equiv 1 \bmod 4$. The basis $\mathcal{B} = \{1, \sqrt{n}\}$ is contained in $\mathfrak{o}_k$, and we have $\Delta(\mathcal{B}) = 4n$. Since n is square-free, we take $N = 2$ in the algorithm. We need to check that none of the elements:

$$\frac{1}{2}, \quad \frac{\sqrt{n}}{2}, \quad \frac{1+\sqrt{n}}{2}$$

are algebraic integers. Clearly $\frac{1}{2} \notin \mathfrak{o}_k$ since $\mathfrak{o}_\mathbb{Q} = \mathbb{Z}$. We have

$$N\left(\frac{\sqrt{n}}{2}\right) = \frac{-n}{4}.$$

This is not an integer since n is square-free. Therefore $\frac{\sqrt{n}}{2}$ is not an algebraic integer. Finally

$$N\left(\frac{1+\sqrt{n}}{2}\right) = \frac{1-n}{4}.$$

This is not an integer since $n \not\equiv 1 \bmod 4$. Therefore $\frac{1+\sqrt{n}}{2}$ is not an algebraic integer. Hence $\mathcal{B}$ is an integral basis.

Next suppose $n \equiv 1 \bmod 4$ and let $\mathcal{B} = \{1, \alpha\}$, where $\alpha = \frac{1+\sqrt{n}}{2}$. We have $\left(\alpha - \frac{1}{2}\right)^2 = \frac{n}{4}$. Therefore α is a zero of the polynomial

$$X^2 - X + \frac{1-n}{4}.$$

Since $n \equiv 1 \bmod 4$ this has integer coefficients, so $\mathcal{B} \subset \mathfrak{o}_k$. On the other hand $\Delta(\mathcal{B}) = n$, which is square-free, so $\mathcal{B}$ must be an integral basis. □

3.6 Cubic fields

103 Definition An algebraic number field k is called a *cubic field* if $[k : \mathbb{Q}] = 3$.

Let $k = \mathbb{Q}(\alpha)$ be a cubic field, where α has minimal polynomial $m(X) = X^3 + aX^2 + bX + c$. We define the normalized cubic to be the polynomial $m(X - \frac{a}{3})$. This is the minimal polynomial of $\theta = \alpha + \frac{a}{3}$, and we clearly also have $k = \mathbb{Q}(\theta)$. By multiplying θ by a suitable natural number we may ensure that it is an algebraic integer without changing the field which it generates. We therefore have:

104 Proposition *If k is a cubic field then $k = \mathbb{Q}(\alpha)$ for some element α with minimal polynomial*

$$m(X) = X^3 + aX + b, \quad a, b \in \mathbb{Z}.$$

To calculate an integral basis in a cubic field we will need the following result on discriminants.

105 Proposition *Let $k = \mathbb{Q}(\alpha)$ where α has minimal polynomial $m(X) = X^3 + aX + b$ $a, b \in \mathbb{Q}$. Then*

$$\Delta\{1, \alpha, \alpha^2\} = -27b^2 - 4a^3.$$

The proof of this requires a general result on discriminants:

106 Theorem *Let $k = \mathbb{Q}(\alpha)$ be an algebraic number field with $[k : \mathbb{Q}] = d$ and let m be the minimal polynomial of α. Then*

$$\Delta\{1, \alpha, \ldots, \alpha^{d-1}\} = (-1)^{\frac{d(d-1)}{2}} N(m'(\alpha)).$$

Proof. Let $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ be the zeros of m_α. Recall that the left hand side is the square of a Vandermonde determinant:

$$\Delta\{1, \alpha, \ldots, \alpha^{d-1}\} = \prod_{i<j} (\alpha_j - \alpha_i)^2 = (-1)^{\frac{d(d-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

We shall now calculate the right hand side: We have

$$N(m'(\alpha)) = \prod_i m'(\alpha_i).$$

On the other hand,

$$m(X) = \prod (X - \alpha_j),$$

so

$$m'(X) = \sum_j \prod_{k \neq j} (X - \alpha_k).$$

This implies

$$m'(\alpha_i) = \prod_{k : k \neq i} (\alpha_k - \alpha_i)).$$

Therefore

$$N(m'(\alpha)) = \prod_{i,k : i \neq k} (\alpha_k - \alpha_i).$$

□

Proof. We have

$$m'(X) = 3X^2 + a.$$

Therefore

$$\Delta\{1, \alpha, \alpha^2\} = -(3\alpha^2 + a)(3\beta^2 + a)(3\gamma^2 + a).$$

When we expand this out we have:

$$-27(\alpha\beta\gamma)^2 - 9a(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2) - 3a^2(\alpha^2 + \beta^2 + \gamma^2) - a^3.$$

We know that $\alpha + \beta + \gamma = 0$, $\Sigma\alpha\beta = a$ and $\prod \alpha = -b$. This implies

$$\alpha^2\beta^2\gamma^2 = b^2,$$

$$\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 = (\Sigma\alpha\beta)^2 - 2(\Sigma\alpha)(\Pi\alpha) = a^2,$$

$$\alpha^2 + \beta^2 + \gamma^2 = (\Sigma\alpha)^2 - 2\Sigma\alpha\beta = -2a.$$

Hence

$$\Delta = -27b^2 - 9a^3 + 6a^3 - a^3 = -27b^2 - 4a^3.$$

□

Lecture 12

Proof of the Theorem. The polynomial m is irreducible over $\mathbb{Q}$, but over k it factorizes (by the remainder theorem) as

$$m(X) = (X - \alpha)g(X), \quad g \in k[X].$$

Furthermore over $\mathbb{C}$ it is a product of linear factors:

$$m(X) = (X - \alpha_1) \dots (X - \alpha_d).$$

For each conjugate α_i we have a field embedding $\sigma_i : k \hookrightarrow \mathbb{C}$ with $\sigma_i(\alpha) = \alpha_i$. Since $g(X) = \frac{m(X)}{X-\alpha}$, we have $\sigma_i(g) = g_i$ in $\mathbb{C}[X]$, with

$$g_i(X) = \frac{m(X)}{X - \alpha_i} = \prod_{j \neq i}(X - \alpha_j).$$

We shall now simply calculate the right hand side of the formula in the theorem. Differentiating m we have:

$$m'(X) = g(X) + (X - \alpha)g'(X),$$

and hence

$$m'(\alpha) = g(\alpha).$$

Taking the norm of this we have:

$$\begin{aligned} N(m'(\alpha)) &= \prod_{i=1}^{d} \sigma_i(g(\alpha)) \\ &= \prod_{i=1}^{d} g_i(\alpha_i) \\ &= \prod_{i \neq j}(\alpha_i - \alpha_j) \\ &= \prod_{i<j}(\alpha_i - \alpha_j)(\alpha_j - \alpha_i) \\ &= (-1)^{\frac{d(d-1)}{2}} \prod_{i<j}(\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{d(d-1)}{2}} \Delta\{1, \alpha, \dots, \alpha^{d-1}\}. \end{aligned}$$

□

Proof of the Proposition. Let $m(X) = X^3 + aX + b$ factorize over $\mathbb{C}$ as $(X - \alpha)(X - \beta)(X - \gamma)$, so we have

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta + \beta\gamma + \gamma\alpha = a, \quad \alpha\beta\gamma = -b.$$

On the other hand, by the theorem we have:

$$\Delta\{1, \alpha, \alpha^2\} = -N(m'(\alpha)).$$

We shall calculate the right hand side here by expressing $N(m'(\alpha))$ in terms of the elementary symmetric

polynomials above. Clearly $m'(X) = 3X^2 + a$ and hence

$$\begin{aligned}
N(m'(\alpha)) &= (3\alpha^2 + a)(3\beta^2 + a)(3\gamma^2 + a) \\
&= 27\alpha^2\beta^2\gamma^2 \\
&\quad +9a(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2) \\
&\quad +3a^2(\alpha^2 + \beta^2 + \gamma^2) \\
&\quad +a^3 \\
&= 27(\alpha\beta\gamma)^2 \\
&\quad +9a\left((\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2(\alpha\beta\gamma^2 + \alpha^2\beta\gamma + \alpha\beta^2\gamma)\right) \\
&\quad +3a^2\left((\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha)\right) \\
&\quad +a^3 \\
&= 27(\alpha\beta\gamma)^2 \\
&\quad +9a\left((\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma)\right) \\
&\quad +3a^2\left((\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha)\right) \\
&\quad +a^3 \\
&= 27b^2 + 9a\left(a^2\right) + 3a^2\left(-2a\right) + a^3 \\
&= 27b^2 + 9a^3 - 6a^3 + a^3 \\
&= 27b^2 + 4a^3.
\end{aligned}$$

□

107 Example $m(X) = X^3 + ...$

108 Example $m(X) = X^3 + 2X + 2$. This is irreducible by Eisenstein's criterion with $p = 2$, so a root α generates a cubic field.

Another corollary to the above theorem is:

109 Corollary *Let $k = \mathbb{Q}(\alpha)$ and let $d = [k : \mathbb{Q}]$. The for any $\theta = \alpha + x$ with $x \in \mathbb{Q}$ we have:*

$$\Delta\{1, \alpha, \ldots, \alpha^{d-1}\} = \Delta\{1, \theta, \ldots, \theta^{d-1}\}.$$

Proof. Let m_α be the minimal polynomial of α. Then the minimal polynomial of θ is

$$m_\theta(X) = m_\alpha(X - x).$$

By the chain rule we have

$$m'_\theta(X) = m'_\alpha(X - x).$$

Therefore

$$m'_\theta(\theta) = m'_\alpha(\theta - x) = m'_\alpha(\alpha).$$

Hence by the theorem we have:

$$\begin{aligned}
\Delta\{1, \theta, \ldots, \theta^{d-1}\} &= (-1)^{\frac{d(d-1)}{2}} N(m'_\theta(\theta)) \\
&= (-1)^{\frac{d(d-1)}{2}} N(m'_\alpha(\alpha)) \\
&= \Delta\{1, \alpha, \ldots, \alpha^{d-1}\}.
\end{aligned}$$

□

Lecture 13

3.7 More tricks for calculating integral bases

First trick Note that if there is an algebraic integer of the form $\frac{1}{N}\sum a_i b_i$ with not all the a_i divisible by N, then for some prime factor $p|N$ the coefficients a_i are not all zero mod $\frac{N}{p}$. Hence the element $\frac{1}{p}\sum a_i b_i$ is an algebraic integer. It is therefore sufficient to check for each prime p with $p^2|\Delta\mathcal{B}$ that none of these elements are algebraic integers.

second trick Whan calculating norms and traces it s useful to note that

$$N(ab) = N(a)N(b), \quad \mathrm{Tr}(a+b) = \mathrm{Tr}(a) + \mathrm{Tr}(b).$$

third trick This trick is an easy way of calculating the norms of certain elements.

110 Proposition *Let $k = \mathbb{Q}(\alpha)$ and let m be the minimal polynomial of α. Then for all $x \in \mathbb{Q}$ we have:*

$$N(x - \alpha) = m(x).$$

Proof. easy. □

fourth trick Suppose m_α satisfies Eisenstein's criterion with the prime p. Then $m(X) \equiv X^d \bmod p$ so we have $m'(X) \equiv dX^{d-1} \bmod p$. This implies

$$N(m'(\alpha)) \equiv N(d\alpha^{d-1}) \bmod p \ \text{ in } \mathfrak{o}_{\mathbb{C}}.$$

Since both sides of this equation are in $\mathbb{Z}$ we have

$$N(m'(\alpha)) \equiv N(d\alpha^{d-1}) \bmod p \ \text{ in } \mathbb{Z}.$$

Furthermore $N(\alpha)$ is a multiple of p so we have

$$N(m'(\alpha)) \equiv 0 \bmod p.$$

Hence p is a factor of $\Delta\{1, \alpha, \ldots, \alpha^{d-1}\}$. However the next theorem tells us that we will never need to worry about this factor when calculating an integral basis.

111 Theorem *Let $k = \mathbb{Q}(\alpha)$; let $d = [k : \mathbb{Q}]$ and assume that m_α satisfies Eisenstein's Criterion with the prime p. Let*

$$\theta = \frac{1}{p}\sum_{i=0}^{d-1} a_i \alpha^i, \quad a_i \in \{0, \ldots, p-1\} \text{ not all } 0.$$

Then θ is not an algebraic integer.

Proof. Suppose $\theta \in \mathfrak{o}_k$ and let a_n be the first non-zero coefficient. We therefore have:

$$\theta = \frac{1}{p}\sum_{i=n}^{d-1} a_i \alpha^i \in \mathfrak{o}_k.$$

We can write this as

$$\theta = \frac{1}{p}\left(a_n\alpha^n + \alpha^{n+1}\delta\right), \quad \delta \in \mathfrak{o}_k.$$

Multiplying through by α^{d-1-n} we still have an element of $\mathfrak{o}_k$:

$$\alpha^{d-1-n}\theta = \frac{a_n\alpha^{d-1}}{p} + \frac{\alpha^d\delta}{p} \in \mathfrak{o}_k.$$

On the other hand since m satisfies Eisenstein's criterion we have

$$\alpha^d = pg(\alpha), \quad g \in \mathbb{Z}[X].$$

It follows that

$$\frac{a_n\alpha^{d-1}}{p} + g(\alpha)\delta \in \mathfrak{o}_k.$$

On the other hand since $g(\alpha)\delta \in \mathfrak{o}_k$ we have

$$\frac{a_n\alpha^{d-1}}{p} \in \mathfrak{o}_k.$$

We shall calculate the norm of this to get a contradiction:

$$N\left(\frac{a_n\alpha^{d-1}}{p}\right) = \frac{a_n^d N(\alpha)^{d-1}}{p^d}.$$

By Eisenstein's criterion the constant coefficient of m is divisible by p but not by p^2 Therefore $N(\alpha) = pr$, where $p \not| r$, and we have

$$N\left(\frac{a_n\alpha^{d-1}}{p}\right) = \frac{a_n^d p^{d-1} r^{d-1}}{p^d} = \frac{a_n^d r^{d-1}}{p}.$$

However this cannot be an integer, since neither a_n nor r is a multiple of p. This gives the contradiction. □

3.8 More examples of integral bases

Now that we know more tricks we can calculate integral bases much more easily.

some cubic fields.

$X^3 - 2$.

$X^p - p$.

Lecture 14

3.9 Prime Cyclotomic Fields

112 Definition Let $n \in \mathbb{Z}$. A number ζ is called an n-th root of unity of $\zeta^n = 1$. If there is no $1 \leq r < n$ with $\zeta^r = 1$ then ζ is called a *primitive n-th root of unity.*

For example $\exp(\frac{2\pi i}{n})$ is a primitive n-th root of unity.

113 Remark Roots of unity are always algebraic integers since they are zeros of the polynomial $X^n - 1$.

114 Remark The polynomials $X^n - 1$ are not irreducible, so are not the minimal polynomials of ζ. For example $X - 1$ is always a factor. More generally if $r|n$ then $X^r - 1$ is a factor.

We shall concentrate on the case $n = p$ for some prime number $p \geq 3$. Let ζ be a primitive p-th root of unity, and for convenience we let $\lambda = \zeta - 1$.

115 Proposition *The minimal polynomial of ζ is*

$$m_\zeta(X) = \frac{X^p - 1}{X - 1} = 1 + X + \ldots + X^{p-1}.$$

Equivalently the minimal polynomial of λ is

$$m_\lambda(X) = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}.$$

Proof. It is sufficient to check that m_λ is irreducible. This follows from the next result: □

116 Lemma *m_λ satisfies Eisenstein's criterion with the prime number p.*

Proof. The coefficients are $\frac{p!}{i!(p-i)!}$ with $1 \leq i \leq p$. Clearly the leading coefficient is 1 and the constant coefficient is p. For the other coefficients we have $2 \leq i \leq p - 1$. The denominator of the coefficient is coprime to p and the numerator is a multiple of p; hence the coefficient is a multiple of p. □

Now consider the field $k = \mathbb{Q}(\zeta) = \mathbb{Q}(\lambda)$. This is called the *prime cyclotomic field.* From the minimal polynomials of ζ and λ we have:

117 Proposition *Let $k = \mathbb{Q}(\zeta) = \mathbb{Q}(\lambda)$ be the prime cyclotomic field for an odd prime p.*

- $[k : \mathbb{Q}] = p - 1$.
- $N(\zeta) = 1$.
- $N(\lambda) = p$.

Proof.

- The degree of m_ζ is clearly $p - 1$.
- The constant term of m_ζ is 1 and the degree is even.
- The constant coefficient of m_λ is p and it's degree is even.

□

118 Theorem *We have*

$$\Delta\{1, \lambda, \ldots, \lambda^{p-2}\} = \Delta\{1, \zeta, \ldots, \zeta^{p-2}\} = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Furthermore $\{1, \lambda, \ldots, \lambda^{p-2}\}$ *is an integral basis in* k*. Hence*

$$\mathfrak{o}_k = \mathbb{Z}[\lambda] = \mathbb{Z}[\zeta].$$

Proof. We have by earlier theorems:

$$\Delta\{1, \lambda, \ldots, \lambda^{p-2}\} = \Delta\{1, \zeta, \ldots, \zeta^{p-2}\} = (-1)^{\frac{(p-1)(p-2)}{2}} N(m'_\zeta(\zeta)).$$

Since p is odd, we have $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{p-1}{2}}$. Furthermore, since $m_\zeta(X) = \frac{X^p-1}{X-1}$, we have

$$m'_\zeta(X) = \frac{pX^{p-1}(X-1) - (X^p-1)}{(X-1)^2}.$$

Therefore

$$m'_\zeta(\zeta) = \frac{p\zeta^{p-1}(\zeta-1) - (\zeta^p-1)}{(\zeta-1)^2} = \frac{p\zeta^{p-1}}{\lambda}.$$

Hence

$$N(m'_\zeta(\zeta)) = \frac{p^{p-1}N(\zeta)^{p-1}}{N(\lambda)} = p^{p-2}.$$

The only prime whose square divides this is p. However the minimal polynomial of λ satisfies Eisenstein's criterion at that prime. □

119 Remark If n is not prime and $k = \mathbb{Q}(\zeta)$, then it is still true that $\mathfrak{o}_k = \mathbb{Z}[\zeta]$; however the proof is harder. The degree of the extension is given by

$$[k : \mathbb{Q}] = \#(\mathbb{Z}/n)^\times.$$

This is the same as the number of primitive n-th roots of unity in k, since these are of the form ζ^a with a coprime to n. If $n = p^a$ for some prime p, then m_λ still satisfies Eisenstein's criterion for the prime p, and we again use this fact to prove that $\{\lambda^i\}$ is an integral basis. If n is not a power of a prime then m_λ does't satisfy Eisenstein's criterion, so the proof is quite different in this case.

Lecture 15

4 Factorization in $\mathfrak{o}_k$

4.1 Units and irreducible elements in $\mathfrak{o}_k$

Recall that in any commutative ring R with 1 there are three kinds of element:

- an element $x \in R$ is called a *unit* if there exists an $x^{-1} \in R$ such that $xx^{-1} = 1$;
- an element $x \in R$ is called *reducible* if there is a factorization $x = yz$ with neither y nor z a unit;
- an element $x \in R$ is called *irreducible* if it is neither a unit nor reducible.

120 Proposition *Let $x \in \mathfrak{o}_k$. Then x is a unit if and only if $N(x) = \pm 1$.*

121 Proposition *Let $x \in \mathfrak{o}_k$. If $N(x) = \pm p$ for a prime number p then x is irreducible.*

Note that the converse to this is false. For example 3 is irreducible in $\mathbb{Z}[i]$, but $N(3) = 9$. To see that 3 is irreducible we have to show that there is no element with norm ± 3. The norm of a general element of $\mathbb{Z}[i]$ is given by

$$N(x + iy) = x^2 + y^2,$$

and this is clearly never ± 3 for $x, y \in \mathbb{Z}$.

122 Theorem *Let $x \in \mathfrak{o} \setminus \{0\}$. Then there is a unit $u \in \mathfrak{o}^\times$ and irreducible elements $p_1, \ldots, p_r$ such that*

$$x = up_1 \ldots p_r.$$

Proof. By induction on $|N(x)|$. If $|N(x)| = 1$ then x is a unit. Assume the theorem is true for elements y with $|N(y)| < |N(x)|$. If x is irreducible then the theorem is true for x. If x is reducible then $x = yz$ and $|N(y)|, |N(z)| < |N(x)|$. Hence both y and z can be factorized into irreducibles; therefore so can x. □

123 Definition We say that a ring has unique factorization if whenever

$$p_1 \ldots p_r = q_1 \ldots q_s, \quad p_i, q_i \text{ irreducible},$$

we always have $r = s$ and (after reordering) there are units $u_1, \ldots, u_r$ such that $p_i = u_i q_i$ for $i = 1, \ldots r$.

124 Example The rings $\mathbb{Z}$ and $k[X]$ have unique factorization.

One of the main difficulties in algebraic number theory is that fact that $\mathfrak{o}_k$ does not usually have unique factorization.

125 Example Let $k = \mathbb{Q}(\sqrt{-10})$, so $\mathfrak{o}_k = \mathbb{Z}[\sqrt{-10}]$. We have two different factorizations of the number 10:

$$10 = 2 \times 5 = -\sqrt{-10} \times \sqrt{-10}.$$

Furthermore the elements 2, 5 and $\sqrt{-10}$ are all irreducible. To see this we calculate their norms:

$$N(2) = 4, \quad N(5) = 25, \quad N(\sqrt{-10}) = 10.$$

The norm of a general element of the ring is

$$N(x + y\sqrt{-10}) = x^2 + 10y^2.$$

Since this is never equal to ± 2 or ± 5, it follows that the above elements are irreducible, and none of them is a unit multiple of another. Therefore $\mathfrak{o}_k$ does not have unique factorization.

To get around this problem, we introduce the idea of factorization of ideals, to generalize factorization of elements.

126 Definition Let I and J be ideals of a commutative ring R with 1. We define the product ideal $I \times J$ by

$$I \times J = (xy : x \in I,\ y \in J).$$

I.e. $I \times J$ is the ideal generated by products of elements of I by elements of J.

127 Example For principal ideals we have

$$(x)(y) = (xy).$$

More generally,

$$(a, b)(c, d) = (ac, ad, bc, bd).$$

Later in the course, we shall prove the following theorem, which takes the place of uniqueness of factorization of elements:

128 Theorem *Let $I \subset \mathfrak{o}_k$ be a non-zero ideal. Then there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathfrak{o}_k$ such that $I = \mathfrak{p}_1 \ldots \mathfrak{p}_r$. Furthermore this factorization is unique up to reordering.*

We now return to the above example in $\mathbb{Z}[\sqrt{-10}]$. Consider the ideals

$$\mathfrak{p} = (2, \sqrt{-10}), \quad \mathfrak{q} = (5, \sqrt{-10}).$$

We have

$$\begin{aligned}
\mathfrak{pq} &= (2, \sqrt{-10})(5, \sqrt{-10}) \\
&= (10, 2\sqrt{-10}, 5\sqrt{-10}, -10) \\
&= (10, 2\sqrt{-10}, 5\sqrt{-10}, -10, \sqrt{-10}) \\
&= (\sqrt{-10}) \\
\mathfrak{p}^2 &= (2, \sqrt{-10})(2, \sqrt{-10}) \\
&= (4, 2\sqrt{-10}, -10) \\
&= (4, 2\sqrt{-10}, -10, 2) \\
&= (2) \\
\mathfrak{q}^2 &= (5, \sqrt{-10})(5, \sqrt{-10}) \\
&= (25, 5\sqrt{-10}, -10) \\
&= (25, 5\sqrt{-10}, -10, 5) \\
&= (5).
\end{aligned}$$

So our two distinct factorizations into elements can both be refined to the same factorization into ideals:

$$(10) = (2) \times (5) = \mathfrak{p}^2\mathfrak{q}^2, \quad (10) = (\sqrt{-10})^2 = (\mathfrak{pq})^2.$$

To understand the factorization of elements, as opposed to ideals, we need to find out which ideals are principal are which are not. For this purpose we define the *class group* of k to be the group

$$\mathrm{Cl}_k = \mathcal{I}_k/\mathcal{P}_k,$$

where $\mathcal{I}_k$ is the ideals of k, and $\mathcal{P}_k$ is the principal ideals. (In fact these are semi-groups, although the quotient is a group.) We shall prove that this is always a finite group, and calculate it in a lot of examples. If Cl_k is trivial then $\mathfrak{o}_k$ is a principal ideal domain, and has unique factorization.

Lecture 16

4.2 Prime ideals

129 Definition Let R be a commutative ring with 1. An ideal $\mathfrak{p} \subset R$ is called a *prime ideal* if $\mathfrak{p} \neq R$ and for $x, y \in R$,

$$xy \in \mathfrak{p} \Rightarrow (x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}).$$

130 Definition A ring R is called an *integral domain* if it staisfies the condition

$$xy = 0 \Rightarrow (x = 0 \text{ or } y = 0).$$

In other words (0) is a prime ideal.

131 Example If k is a field then certainly k is an integral domain. More generally subrings of fields are integral domains. In fact the converse is also true: every integral domain is a subring of a field.

132 Lemma *$\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is an integral domain.*

133 Corollary *Every maximal ideal is prime.*

Proof. Every field is an integral domain. □

134 Remark The converse to this is false. For example if R is an integral domain but not a field, then (0) is a prime ideal but is not maximal.

135 Proposition *Every finite integral domain is a field.*

Proof. Let $x \in R \setminus \{0\}$. We have to show that x has an inverse in R. The numbers $x, x^2, \ldots$ cannot all be different, since R is finite. Therefore there exist $n > m \geq 0$ such that

$$x^n = x^m.$$

This implies

$$x^m(x^a - 1) = 0, \quad a = n - m \geq 1.$$

Since R is an integral domain and $x \neq 0$, it follows that $x^a - 1 = 0$. Hence $x^a = 1$, so x^{a-1} is the inverse of x. □

136 Proposition *If $I \subset \mathfrak{o}_k$ is a non-zero ideal then $\mathfrak{o}/I$ is finite.*

Proof. Let $x \in I \setminus \{0\}$. Clearly $N(x) = xy$ for some other algebraic integer y, so we have $N(x) \in I$. Let $n = |N(x)|$. It follows that $(n) \subset I$, so it is sufficient to show that $\mathfrak{o}_k/(n)$ is finite. However

$$\#\mathfrak{o}/(n) = \#\mathbb{Z}^d/n\mathbb{Z}^d = n^d.$$

□

137 Corollary *Every non-zero prime ideal of $\mathfrak{o}_k$ is maximal.*

Now let R be a commutative ring with 1. Recall that for two ideals $I, J \subseteq R$, we defined the product:

$$IJ = (xy : x \in I,\ y = inJ)\,.$$

For principal ideals this corresponds to multiplying the generators:

$$(x)(y) = (xy).$$

138 Lemma *Let $\mathfrak{p}$ be an ideal of R. Then $\mathfrak{p}$ is prime if and only if for all ideals $I, J \subset R$*

$$IJ \subseteq \mathfrak{p} \Rightarrow (I \subseteq \mathfrak{p} \text{ or } J \subseteq \mathfrak{p}).$$

Proof. Assume $\mathfrak{p}$ is prime and suppose $IJ \subseteq \mathfrak{p}$. We'll assume that $I \nsubseteq \mathfrak{p}$ and prove that $J \subseteq \mathfrak{p}$. Let $x \in I \setminus \mathfrak{p}$. For every $y \in J$ we have $xy \in AB$. Therefore $xy \in \mathfrak{p}$. Since $x \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, it follows that $y \in \mathfrak{p}$. Hence $J \subseteq \mathfrak{p}$.

Now assume $\mathfrak{p}$ satisfies the condition and suppose $xy \in \mathfrak{p}$. This implies $(xy) \subseteq \mathfrak{p}$. Therefore $(x)(y) \subseteq \mathfrak{p}$. By the assumption, we have $(x) \subseteq \mathfrak{p}$ or $(y) \subseteq \mathfrak{p}$. This implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. □

Lecture 17

4.3 Uniqueness of Factorization into ideals

139 Definition A ring R is called a Noetherian ring if it satisfies the following condition (called the *ascending chain condition*): For every ascending sequence of ideals of R:

$$I_1 \subseteq I_2 \subseteq \ldots,$$

there is an $N \in \mathbb{N}$ such that

$$I_N = I_{N+1} = I_{N+1} = \ldots.$$

140 Definition For a non-zero ideal $I \subseteq \mathfrak{o}_k$, we define the *norm* of I by

$$N(I) = |\mathfrak{o}_k/I|.$$

Recall that this is always a finite number.

141 Lemma *$\mathfrak{o}_k$ is Noetherian.*

Proof. If we have a sequence of ideals

$$I_1 \subseteq I_2 \subseteq \ldots,$$

then by the isomorphism theorem, we have an isomorphism of additive groups:

$$\mathfrak{o}/I_2 \cong (\mathfrak{o}/I_1)/(I_2/I_1).$$

Hence

$$N(I_2) = N(I_1)/|I_2/I_1|.$$

It follows that $N(I_2) < N(I_1)$ with equality if and only if $I_2 = I_1$. Hence we have a decreasing sequence of natural numbers:

$$N(I_1) \geq N(I_2) \geq \ldots.$$

Clearly there is an N such that

$$N(I_N) = N(I_{N+1}) = \ldots.$$

Hence $I_N = I_{N+1} = \ldots$. □

If R is a Noetherian ring then there is a strategy for provong results about ideals of R as follows: assume that the result if false. and suppose I_1 is a counterexample. We call I_1 a maximal counterexample if every ideal containing I_1 satisfies the theorem. If I_1 is not a maximal counterexample then choose a bigger counterexample I_2. If I_2 is not a maximal counterexample then choose a bigger counterexample I_3 etc. In this way we obtain a sequence of ideals which must end in a maximal counterexample. So we may always assume that if a theorem about ideals is false then there is a maximal counterexample. An example of this method is the following:

142 Lemma *Let $I \subseteq \mathfrak{o}_k$ be a non-zero ideal. Then there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I.$$

Proof. Suppose not and let I be a maximal counterexample. Clearly I is not a maximal ideal. Since I is non-zero, we know that I is not prime. Therefore there are ideals A, B such that $AB \subset I$ but neither A nor B is a subset of I. By replacing A and B by (A, I) and (B, I), we may assume that A and B both contain I. By the maximality of our counterexample, it follows that we can find maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq A, \quad \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq B.$$

Hence

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq AB \subseteq I.$$

□

143 Lemma *Let I be a non-zero ideal of $\mathfrak{o}_k$. If $x \in k$ satisfies $xI \subset I$ then $x \in \mathfrak{o}_k$.*

Proof. Since $I \subset \mathfrak{o}_k$ it follows that I is finitely generated as an abelian group. Let

$$I = \mathrm{span}_{\mathbb{Z}}\{b_1, \ldots, b_r\}.$$

Multiplication by x takes I to I, so we have

$$xb_i = \sum_j a_{i,j} b_j, \quad a_{i,j} \in \mathbb{Z}.$$

Hence

$$(A - xI_r) \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} = 0, \quad A = (a_{i,j}).$$

This means that x is an eigenvalue of A, so is an algebraic integer. □

144 Definition A *fractional ideal* of $\mathfrak{o}_k$ is a non-empty subset $I \subset k$ such that

- I is closed under addition.
- if $x \in \mathfrak{o}_k$ and $y \in I$ then $xy \in I$.
- There exists a non-zero $n \in \mathbb{N}$ such that $nI \subset \mathfrak{o}_k$.

We shall write $\mathcal{I}_k$ for the set of non-zero fractional ideals of $\mathfrak{o}_k$. We can define multiplication of fractional ideals in exactly the same was as for ideals. This is clearly associative, and $\mathfrak{o}_k = (1)$ is an identity element. We shall show that $\mathcal{I}_k$ is a group by proving that every element has an inverse.

145 Lemma $N(I) \in I$.

Proof. This follows by Lagrange's theorem on the additive group $\mathfrak{o}/I$. □

146 Lemma *Let I be a non-zero ideal and define*

$$I^{-1} = \{x \in k : xI \subseteq \mathfrak{o}_k\}.$$

Then I^{-1} is a fractional ideal.

Proof. The first two conditions are easy to check. If $x \in I$ then $xI^{-1} \subset \mathfrak{o}_k$, so the third condition is also true with $n = N(I)$. □

Lecture 18

Note that if $I \subseteq J$ then $J^{-1} \subseteq I^{-1}$. Hence for any ideal I we have $\mathfrak{o} \subseteq I^{-1}$

147 Lemma *If $I \subset \mathfrak{o}_k$ and $I \neq \mathfrak{o}$ then $I^{-1} \neq \mathfrak{o}_k$.*

Proof. It's sufficient to prove this for maximal ideals $\mathfrak{p}$. Obviously $\mathfrak{p}^{-1} \supseteq \mathfrak{o}$ so we need to show that $\mathfrak{p}^{-1} \neq \mathfrak{o}$.

Let $a \in \mathfrak{p} \setminus \{0\}$, and suppose $(a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ with r as small as possible and $\mathfrak{p}_i$ all prime. Hence $\mathfrak{p} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. It follows that $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. Since $\mathfrak{p}_i$ is maximal, we know that in fact $\mathfrak{p} = \mathfrak{p}_i$. Without loss of generality $i = 1$. Now $(a) \not\supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r$ (by minimality of r), so we can choose a $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a)$. We'll show that $\frac{b}{a} \in \mathfrak{p}^{-1} \setminus \mathfrak{o}$.

First note that $(b)\mathfrak{p} \subset \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a)$. Hence $\frac{b}{a}\mathfrak{p} \subset \mathfrak{o}$. This shows that $\frac{b}{a} \in \mathfrak{p}^{-1}$. Note also that $b \notin (a)$. This shows that $\frac{b}{a} \notin \mathfrak{o}$. □

148 Lemma *If $\mathfrak{p}$ is a maximal ideal of $\mathfrak{o}$ then $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}$.*

Proof. Clearly $\mathfrak{p}^{-1}\mathfrak{p} \subset \mathfrak{o}$ (by definition of $\mathfrak{p}^{-1}$). Therefore $\mathfrak{p}^{-1}\mathfrak{p}$ is an (integral) ideal. On the other hand, since $\mathfrak{o} \subset \mathfrak{p}^{-1}$ it follows that $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. By maximality of $\mathfrak{p}$ we have either $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}$ or $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. If the latter is the case then by an earlier lemma, we have $\mathfrak{p}^{-1} \subset \mathfrak{o}$, but this contradicts the previous lemma. □

149 Theorem *Let I be a non-zero ideal of $\mathfrak{o}$. Then there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ unique up to reordering, such that*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Proof. (existence): Suppose not, and let I be a maximal counterexample. Clearly I is not maximal, and hence not prime. On the other hand I is contained in some maximal ideal $\mathfrak{p}$. We have

$$I \subset \mathfrak{p}^{-1}I \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}.$$

Hence $\mathfrak{p}^{-1}I$ is an (integral) ideal containing I. Furthermore, $\mathfrak{p}^{-1}I \neq I$, since otherwise we would have $\mathfrak{p}^{-1} \subset \mathfrak{o}$. It follows that $\mathfrak{p}^{-1}I$ can be factorized into prime ideals:

$$\mathfrak{p}^{-1}I = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Hence by the previous lemma,

$$I = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

(uniqueness): Suppose

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Clearly $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is prime it follows that $\mathfrak{p}_i \subset \mathfrak{q}_1$ for some i. After reordering we may assume $i = 1$. By maximality of $\mathfrak{p}_1$ we have $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying both sides by $\mathfrak{p}^{-1}$ we have

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

We proceed by induction. □

150 Theorem *$\mathcal{I}_k$ is a group with the operation of multiplication of fractional ideals.*

Proof. Multiplication is clearly associative and $\mathfrak{o}$ is the identity element. We just have to show that every element has an inverse. Let I be a fractional ideal. There is an $x \in \mathfrak{o}_k$ such that $(x)I$ is an ideal. By the previous theorem we have $xI = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Hence

$$I^{-1} = (x)\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}.$$

□

151 Definition Let I, J be ideals of $\mathfrak{o}$. We'll say that I is a factor of J (and write $I|J$) if there is an ideal I' such that $J = II'$.

152 Corollary *$I|J$ if and only if $I \supseteq J$.*

Proof. If $J = II'$, then it's clear that $J \subset I$. Conversely suppose that $J \subset I$. There is certainly a fractional ideal I' such that $J = II'$. Since $I'I = J \subseteq I$ it follows that $I' \subset \mathfrak{o}$, so I' is an ideal. □

Lecture 19

4.4 Norms of ideals

153 Theorem *For any two ideals $I, J \subset \mathfrak{o}$ we have $N(IJ) = N(I)N(J)$.*

Proof. Since J may be factorized into maximal ideals, it is sufficient to prove this in the case $J = \mathfrak{p}$ is maximal. We an isomorphism of additive groups:

$$\mathfrak{o}/I \cong (\mathfrak{o}/I\mathfrak{p})/(I/I\mathfrak{p}).$$

Hence

$$N(I) = N(I\mathfrak{p})/|I/I\mathfrak{p}|.$$

It is therefore sufficient to show that

$$N(\mathfrak{p}) = |I/I\mathfrak{p}|.$$

Choose $a \in I \setminus I\mathfrak{p}$ and consider the map

$$\Phi : \mathfrak{o} \to I/I\mathfrak{p}, \quad \Phi(x) = ax + I\mathfrak{p}.$$

Since $\mathfrak{p}$ is maximal, there are no ideals between I and $I\mathfrak{p}$. Hence I is generated by a and $I\mathfrak{p}$. For this it follows that Φ is surjective. On the other hand if $x \in \mathfrak{p}$ then $ax \in I\mathfrak{p}$, so $\Phi(x) = 0 + I\mathfrak{p}$. This shows that $\mathfrak{p} \subset \ker \Phi$. Since $\mathfrak{p}$ is maximal, the kernel is either $\mathfrak{p}$ or $\mathfrak{o}$. However $\Phi(1) = a + I\mathfrak{p} \neq 0 + I\mathfrak{p}$, so $\ker \Phi = \mathfrak{p}$. Hence by the first isomorphism theorem, there is an isomorphism of additive groups

$$\mathfrak{o}/\mathfrak{p} \cong I/I\mathfrak{p}.$$

Hence $N(\mathfrak{p}) = |I/I\mathfrak{p}|$. □

154 Remark Suppose $\sigma : k \to k$ is a field homomorphism. Clearly σ takes $\mathfrak{o}$ to $\mathfrak{o}$ and takes ideals to ideals. It follows that if I is an ideal then

$$N(\sigma I) = |\mathfrak{o}/\sigma I| = |\sigma\mathfrak{o}/\sigma I| = N(I).$$

For example

$$N(2, 1 + \sqrt{3}) = N(2, 1 - \sqrt{3}).$$

Hence

$$N(2, 1 + \sqrt{3})^2 = N(4, 2 + 2\sqrt{3}, 2 - 2\sqrt{3}, -2) = N((2)) = 4.$$

We can often use this method to calculate norms.

Now note the following theorem proved in another course:

155 Theorem *Let H be a subgroup of $\mathbb{Z}^d$ such that $|\mathbb{Z}^d/H| < \infty$. Then there exist $c_1, \ldots, c_d \in \mathbb{Z}^d$ linearly independent such that*

$$H = \operatorname{span}_{\mathbb{Z}}\{c_1, \ldots, c_d\}.$$

Furthermore $|\mathbb{Z}^d/H| = |\det(c_1, \ldots, c_d)|$.

We'll use this to prove:

156 Proposition *Let I be a non-zero ideal and assume*

$$I = \mathrm{span}_{\mathbb{Z}}\{c_1, \ldots, c_d\}.$$

Assume also that $\mathcal{B}$ is an integral basis. Then

$$N(I) = \sqrt{\frac{\Delta\mathcal{C}}{\Delta\mathcal{B}}}.$$

Proof. The theorem implies that the c_i exist. Let M be the transition matrix from $\mathcal{B}$ to $\mathcal{B}$. By the theorem,

$$N(I) = |\mathfrak{o}/I| = |\det M|.$$

On the other hand $\Delta\mathcal{C} = \det M^2 \Delta\mathcal{B}$. □

157 Corollary $N((a)) = |N(a)|$.

Proof. Let $\mathcal{B}$ be an integral basis. Then $(a) = \mathrm{span}_{\mathbb{Z}} a\mathcal{B}$. We have

$$\Delta a\mathcal{B} = \det(\sigma_i(ab_j))^2 = N(a)^2 \det(\sigma_i(b_j))^2 = N(a)^2 \Delta\mathcal{B}.$$

The result now follows from the previous proposition. □

158 Lemma $N(I) \in I$.

Proof. This follows from Lagrange's theorem applied to the additive group $\mathfrak{o}/I$. □

159 Corollary *There are only finitely many ideals with a given norm.*

Proof. If $N(I) = n$ then $I|(n)$. However by uniqueness of factorization, n has only finitely many factors. □

Lecture 20

4.5 Norms of prime ideals

160 Proposition *Let $R \subset S$ be commutative rings with 1 and let $\mathfrak{p}$ be a prime ideal of S. Then $\mathfrak{p} \cap R$ is a prime ideal of R.*

Proof. This is obvious from the definition. □

161 Definition Hence for any prime ideal $\mathfrak{p} \subset \mathfrak{o}$, the ideal $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, and is therefore of the form (p) for some prime number p. We say that $\mathfrak{p}$ *lies above* p and write $\mathfrak{p}|p$. If $\mathfrak{p}$ lies above p then $p \in \mathfrak{p}$. Hence $\mathfrak{p}|(p)$ as ideals of $\mathfrak{o}$. Therefore to find the maximal ideals of $\mathfrak{o}$ we simply have to factorize ideals generated by prime numbers.

162 Proposition *If $N(\mathfrak{p})$ is prime then $\mathfrak{p}$ is prime.*

Proof. This follows because norm is multiplicative. □

163 Proposition *If $\mathfrak{p}$ is prime then $N(\mathfrak{p}) = p^r$ for some prime number p and some $1 \leq r \leq d = [k : \mathbb{Q}]$.*

Proof. If $\mathfrak{p}$ lies above p then $p \in \mathfrak{p}$. Hence $(p) \subseteq \mathfrak{p}$, so $\mathfrak{p}|(p)$. Therefore $N(\mathfrak{p})|N((p)) = p^d$. □

164 Dedekind's Prime Factorization Theorem *Suppose $\mathfrak{o}_k = \mathbb{Z}[\alpha]$ for some element α. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α. Let p be a prime number and suppose f factorizes over $\mathbb{F}_p[X]$ as*

$$f \equiv f_1^{e_1} \cdots f_r^{e_r} \bmod p,$$

with f_i monic and irreducible, and $f_i \neq f_j$ unless $i = j$. Then the ideal (p) in $\mathfrak{o}_k$ factorizes as

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}, \qquad \mathfrak{p}_i = (p, f_i(\alpha)).$$

Each ideal $\mathfrak{p}_i$ is maximal and has norm $p^{\deg f_i}$. If $i \neq j$ then $\mathfrak{p}_i \neq \mathfrak{p}_j$.

165 Remark The condition $\mathfrak{o} = \mathbb{Z}[\alpha]$ is equivalent to saying that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis. There is not always such an α, but often there is in the examples which we've seen. The theorem can be modified in the case where no such α exists.

Proof. First note that since $\mathfrak{o} = \mathbb{Z}[\alpha]$, we have an isomorphism

$$\mathfrak{o} \equiv \mathbb{Z}[X]/(m), \qquad \alpha \mapsto X + (m).$$

This implies that there is an isomorphism

$$\mathfrak{o}/\mathfrak{p}_i \equiv \mathbb{Z}[X]/(m, p, m_i) \equiv \mathbb{F}_p[X]/(m, m_i) \equiv \mathbb{F}_p[X]/(m_i).$$

Since m_i is irreducible in $\mathbb{F}_p[X]$, it follows that (m_i) is a maximal ideal in $\mathbb{F}_p[X]$. Hence $\mathbb{F}_p[X]/(m_i)$ is a field. On the other hand this implies that $\mathfrak{o}/\mathfrak{p}_i$ is a field, so $\mathfrak{p}_i$ is a maximal ideal of $\mathfrak{o}$.

The norm of $\mathfrak{p}$ is the number of elements of $\mathbb{F}_p[X]/(m_i)$. This is equal to $p^{[\mathbb{F}_p[X]/(m_i):\mathbb{F}_p]} = p^{\deg m_i}$.

Next note that

$$\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \subseteq \left(p, \prod_{i=1}^{r} m_i(\alpha)^{e_i} \right).$$

On the other have

$$\prod_{i=1}^{r} m_i(\alpha)^{e_i} \equiv m(\alpha) \equiv 0 \bmod p,$$

so we have

$$\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \subseteq (p).$$

To prove that we have equality here, it is sufficient to prove that both sides of the equation have the same norm. This is true since

$$\begin{aligned} N\left(\prod_{i=1}^{r} \mathfrak{p}_i^{e_i}\right) &= \prod_{i=1}^{r} N(\mathfrak{p}_i)^{e_i} \\ &= \prod_{i=1}^{r} p^{e_i \deg m_i} \\ &= p^{\sum_{i=1}^{r} e_i \deg m_i} \\ &= p^{\deg\left(\prod_{i=1}^{r} m_i^{e_i}\right)} \\ &= p^{\deg m} \\ &= p^{[k:\mathbb{Q}]} = N((p)). \end{aligned}$$

It remains to show that the maximal ideals $\mathfrak{p}_i$ are distinct. Suppose $\mathfrak{p}_i = \mathfrak{p}_j$. Then we have $m_i(\alpha) \equiv 0 \bmod \mathfrak{p}_j$. Using the above isomorphism $\mathfrak{o}/\mathfrak{p}_j \cong \mathbb{F}_p[X]/(m_j)$, this implies in $\mathbb{F}_p[X]$:

$$m_i(X) \equiv 0 \bmod (m_j(X)).$$

Hence $m_j | m_i$ in $\mathbb{F}_p[X]$. Since m_i and m_j are monic and irreducible, this implies $m_i = m_j$, and hence $i = j$. □

166 Example Let $k = \mathbb{Q}(\sqrt{6})$. We have $\mathfrak{o}_k = \mathbb{Z}[\sqrt{6}]$, $f(X) = X^2 - 6$. Here are some values of f:

Table 1: default

X	$X^2 - 6$
0	-6
± 1	-5
± 2	-2
± 3	3
± 4	10
± 5	19

From the table we see that f factorizes modulo small primes as

$$\begin{aligned} X^2 - 6 &\equiv X^2 \bmod 2 \\ &\equiv X^2 \bmod 3 \\ &\equiv (X+1)(X-1) \bmod 5 \\ &\equiv X^2 - 6 \bmod 7 \\ &\equiv X^2 - 6 \bmod 11. \end{aligned}$$

Therefore the small primes factorize in $\mathfrak{o}_k$ as follows:

$$\begin{array}{rcll} (2) & = & \mathfrak{p}_2^2, & \mathfrak{p}_2 = (2, \sqrt{6}), \\ (3) & = & \mathfrak{p}_3^2, & \mathfrak{p}_3 = (3, \sqrt{6}), \\ (5) & = & \mathfrak{p}_5\mathfrak{p}_5', & \mathfrak{p}_5 = (5, \sqrt{6}+1), \quad \mathfrak{p}_5' = (5, \sqrt{6}-1). \end{array}$$

On the other hand (7) and (11) are prime in $\mathfrak{o}$. The norms of the ideals are also given by the theorem:

$$N(\mathfrak{p}_2) = 2, \quad N(\mathfrak{p}_3) = 3, \quad N(\mathfrak{p}_5) = N(\mathfrak{p}_5') = 5, \quad N((7)) = 49, \quad N((11)) = 121.$$

167 Example Let $k = \mathbb{Q}(\sqrt[3]{2})$. We've already shown that $\mathfrak{o}_k = \mathbb{Z}[\sqrt[3]{2}]$, so we can apply the theorem. The minimal polynomial is $m(X) = X^3 - 2$. To factorize this modulo primes p, we make a table of values of m:

Table 2: Maximal ideals in $\mathbb{Z}[\sqrt[3]{2}]$

X	X^3-2
0	-2
1	-1
-1	-3
2	6
-2	-10
3	25
-3	-29

$$\begin{array}{rcl} X^3 - 2 & \equiv & X^3 \bmod 2 \\ & \equiv & (X+1)^3 \bmod 3 \\ & \equiv & (X+2)(X^2+3X+4) \bmod 5 \\ & & \text{irreducible mod} 7 \end{array}$$

$$\begin{array}{lll} (2) = \mathfrak{p}_2^3, & \mathfrak{p}_2 = (2, \sqrt[3]{2}), & N\mathfrak{p}_2 = 2 \\ (3) = \mathfrak{p}_3^3, & \mathfrak{p}_2 = (3, \sqrt[3]{2}+1), & N\mathfrak{p}_3 = 3 \\ (5) = \mathfrak{p}_5\mathfrak{p}_{25}, & \mathfrak{p}_5 = (5, \sqrt[3]{2}+2), & N\mathfrak{p}_5 = 5 \\ & \mathfrak{p}_{25} = \left(5, \sqrt[3]{2}^2 + 3\sqrt[3]{2} + 4\right), & N\mathfrak{p}_{25} = 25, \\ (7) \text{ is maximal} & & N((7)) = 7^3. \end{array}$$

Note that the factor $X^2 + 3X + 4$ is irreducible modulo 5, because $b^2 - 4ac \equiv 3 \bmod 5$, and 3 is not a square modulo 5.

Lecture 21

4.6 Factorizing Ideals into Maximal Ideals

We are now able to factorize an ideal I of $\mathfrak{o}$ into maximal ideals:

- Calculate $N(I)$ and factorize it into primes.
- For each prime p dividing $N(I)$, factorize (p) into maximal ideals of $\mathfrak{o}$;
- Write down all ideals whose norm is equal to the norm of I (this is a finite list);
- To find out which factorization is correct, us the principle: $\mathfrak{p}|I$ iff the generators of I are in $\mathfrak{p}$.

168 Example Again let $k = \mathbb{Q}(\sqrt{6})$ as above. We'll factorize the ideal $(12 + 7\sqrt{6})$. First note that

$$N(12 + 7\sqrt{6}) = 144 - 6 \times 49 = 144 - 294 = -150.$$

Therefore

$$N((12 + 7\sqrt{6})) = 150 = 2 \times 3 \times 5^2.$$

However we already calculated the maximal ideals above 2, 3 and 5. Hence there are three ideals of norm 150:

$$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2, \quad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_5', \quad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5'^2.$$

Since $\mathfrak{p}_5\mathfrak{p}_5' = (5)$, and $12 + 7\sqrt{6}$ is not a multiple of 5, is follows that $(12 + 7\sqrt{6}) \neq \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_5'$. We are left with two possibilities. Since $12 + 7\sqrt{6} = 5 + 7(1 + \sqrt{6})$, it follows that $12 + 7\sqrt{6} \in \mathfrak{p}_5$. Hence

$$(12 + 7\sqrt{6}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2.$$

4.7 The Class Group

169 Definition Let $\mathcal{I}_k$ be the group of non-zero ideals of k, and let $\mathcal{P}_k$ be the subgroup o principal fractional ideals. The *class group* of k is defined by

$$\mathrm{Cl}_k = \mathcal{I}_k/\mathcal{P}_k.$$

Obviously if the class group is trivial then $\mathfrak{o}_k$ is a principal ideal domain and has unique factorization of elements. Therefore the size of the class group tells us how far $\mathfrak{o}_k$ is from bein a principal ideal domain.

170 Theorem Cl_k *is finite.*

The proof requires the following:

171 Key Lemma *There is a constant c defending only on k such that for any non-zero ideal I there is a non-zero $x \in I$ satisfying*

$$|N(x)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_k|} N(I).$$

The lemma will be proved later.

Proof of the theorem. Let I be any fractional ideal. There is an $n \in \mathbb{N}$ such that $nI \subset \mathfrak{o}$. In other words $(n)I$ is an ideal. This shows that every ideal class contains an ideal.

Now let J be an ideal in the class of I^{-1}. By the lemma there is a non-zero $x \in J$ with $N(x) \leq cN(J)$. Since $x \in J$ it follows that $J|(x)$. I.e. $(x) = JJ'$ for some ideal J'. Since JJ' is a principal ideal, J' is in the same class as I. We have

$$cN(J) \geq |N(x)| = N((x)) = N(J)N(J').$$

Therefore $N(J') \leq c$.

We've shown that every ideal class contains an ideal with norm $\leq c$. As there are only finitely many ideals with any given norm, it follows that there are only finitely many ideal classes. □

4.8 The Minkowski constant

In fact, the proof that Cl_k is finite shows that every ideal class contains an ideal with norm $\leq c$. Therefore, to calculate the class group, we simply find all the ideals with norm $\leq c$ and determine which of these are in the same class as each other. To do this we will need to know what the constant c is (this is known as the Minkowski constant).

Recall that we have field embeddings $\sigma_1, \ldots, \sigma_d : k \hookrightarrow \mathbb{C}$. We shall call one of these embeddings *real* if $\sigma_i(k) \subseteq \mathbb{R}$. Otherwise we shall call the embedding *complex*. If σ_i is a complex embedding then its complex conjugate $\bar{\sigma}_i$ is another complex embedding, so the complex embeddings come in pairs.

Let r be the number or real embeddings and s the number of pairs of complex embeddings. Thus $d = r + 2s$.

Note that if $k = \mathbb{Q}(\alpha)$ then σ_i is real if and only if $\sigma_i(\alpha) \in \mathbb{R}$. Hence r is the number of real roots of the minimal polynomial of α, and s is the number of complex conjugate pairs of roots, which are not real.

With this notation, the constant c in the key lemma is given by

$$c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|},$$

where Δ is the discriminant of an integral basis.

We can now use this to calculate a few class groups.

172 Example $k = \mathbb{Q}(i)$ has trivial class group.

173 Example $k = \mathbb{Q}(\sqrt{6})$ has trivial class group.

Lecture 22

4.9 Geometry of numbers and Minkowski's Lemma

Let $V = \mathbb{R}^d$ and let $\mathcal{B}$ be a basis for V (over $\mathbb{R}$). We define the *lattice* spanned by $\mathcal{B}$ to be

$$L = \mathrm{span}_{\mathbb{Z}}\mathcal{B}.$$

We also define the *fundamental cell* of $\mathcal{B}$ by

$$\mathcal{P} = \left\{ \sum x_i b_i : 0 \leq x_i < 1 \right\}.$$

Note that

$$\mathrm{vol}(\mathcal{P}) = |\det(b_1 \ \ldots b_d)|.$$

Note that V is the disjoint union of the translations of $\mathcal{P}$ by lattice points:

$$V = \bigcup_{l \in L} \mathcal{P} + l.$$

In other words $\mathcal{P}$ is a set of representatives for the cosets of L is V, i.e. every vector may be written uniquely in the form $v = l + p$ with $l \in L$ and $p \in \mathcal{P}$. We define a function $\mathrm{pr} : V \to \mathcal{P}$ by $\mathrm{pr}(v) = p$.

174 Lemma *Let $U \subset V$ be a subset with a volume, and suppose that $\mathrm{vol}(U) > \mathrm{vol}(\mathcal{P})$. Then there are two points $v, w \in U$ with $v \neq w$ and $v - w \in L$.*

Actually, to make the proof rigorous, we need to know exactly what we mean by "volume". This would involve going into measure theory, which is not part of the course. Instead we'll just give a sketch proof.

Proof. Suppose that two such points do not exist, so the restriction of pr to U is injective. The set U may be written as a disjoint union:

$$U = \bigcup_{l \in L} U_l,$$

where $U_l = U \cap (\mathcal{P} + l)$. Clearly on the sets U_l, the map pr is given by $\mathrm{pr}(v) = v - l$. Hence $\mathrm{pr}(U_l) = U_l - l$. Since pr is injective on U, the sets $U_l - l$ are disjoint. It follows that

$$\mathrm{vol}(U) = \sum \mathrm{vol}(U_l) = \sum \mathrm{vol}(U_l - l) = \mathrm{vol}\left(\bigcup (U_l - l) \right) \leq \mathrm{vol}(\mathcal{P}).$$

□

175 Definition A subset $U \subset V$ is *convex* if for any two points $u, v \in U$ and any $\lambda \in [0, 1]$ the point $\lambda u + (1 - \lambda)v$ is also in U.

176 Definition A subset $U \subset V$ is *symmetric* if for any point $u \in U$ we also have $-u \in U$.

177 Minkowski's Lemma *Let $U \subseteq V$ be convex and symmetric and suppose $\mathrm{vol}(U) > 2^d \mathrm{vol}(\mathcal{P})$. Then there is a non-zero point of L in U.*

Proof. We have $\mathrm{vol}(U) > \mathrm{vol}(2\mathcal{P})$ so by the previous lemma there are two distinct points $v, w \in U$ such that $v - w \in 2L$. Since U is symmetric, we have $-w \in U$. Since U is convex we have $(v - w)/2 \in U$. On the other hand $(v - w)/2$ is a non-zero point of L. □

Lecture 23

4.10 The Minkowski Space

The idea is to use Minkowski's Lemma to prove the key lemma. The ideal will be a lattice in a real vector space k_∞ and all points in the set U will have small norm.

Recall that we have field embeddings $\sigma_1, \ldots, \sigma_d$. We shall reorder these so that $\sigma_1, \ldots, \sigma_r$ are real and $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ are complex, with $\sigma_{r+s+i} = \bar{\sigma}_{r+i}$. We define the d-dimensional real vector space k_∞ by

$$k_\infty = \mathbb{R}^r \oplus \mathbb{C}^s.$$

There is an embedding $\underline{\sigma} : k \to k_\infty$ defined by

$$\underline{\sigma}(x) = \begin{pmatrix} \sigma_1(x) \\ \vdots \\ \sigma_{r+s}(x) \end{pmatrix}.$$

Since each field embedding is injective, $\underline{\sigma}$ is also injective.

178 Messy Lemma *If $\mathcal{B}$ is a basis of k over $\mathbb{Q}$ then $\underline{\sigma}(\mathcal{B})$ is a basis for k_∞ over $\mathbb{R}$; furthermore the fundamental cell has volume*

$$\mathrm{vol}(\mathcal{P}) = 2^{-s}\sqrt{|\Delta\mathcal{B}|}.$$

Proof. It is sufficient to show that the volume of $\mathcal{P}$ is given by the formula, since if $\underline{\sigma}\mathcal{B}$ were not a basis, then this volume would be zero. The volume is given by:

$$\mathrm{vol}(\mathcal{P}) = \left| \det \begin{pmatrix} \sigma_1(b_1) & \ldots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \ldots & \sigma_r(b_d) \\ \Re\sigma_{r+1}(b_1) & \ldots & \Re\sigma_{r+1}(b_d) \\ \Im\sigma_{r+1}(b_1) & \ldots & \Im\sigma_{r+1}(b_d) \\ \vdots & & \vdots \\ \Re\sigma_{r+s}(b_1) & \ldots & \Re\sigma_{r+s}(b_d) \\ \Im\sigma_{r+s}(b_1) & \ldots & \Im\sigma_{r+s}(b_d) \end{pmatrix} \right|.$$

Adding $i\times\mathrm{row}(r+2a)$ to $\mathrm{row}(r+2a-1)$ for $a = 1, \ldots s$ we obtain:

$$\mathrm{vol}(\mathcal{P}) = \left| \det \begin{pmatrix} \sigma_1(b_1) & \ldots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \ldots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \ldots & \sigma_{r+1}(b_d) \\ \Im\sigma_{r+1}(b_1) & \ldots & \Im\sigma_{r+1}(b_d) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \ldots & \sigma_{r+s}(b_d) \\ \Im\sigma_{r+s}(b_1) & \ldots & \Im\sigma_{r+s}(b_d) \end{pmatrix} \right|.$$

Multiplying rows $r+2a$ by -2 we obtain:

$$\mathrm{vol}(\mathcal{P}) = 2^{-s}\left|\det\begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \dots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \dots & \sigma_{r+1}(b_d) \\ -2\Im\sigma_{r+1}(b_1) & \dots & -2\Im\sigma_{r+1}(b_d) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \dots & \sigma_{r+s}(b_d) \\ -2\Im\sigma_{r+s}(b_1) & \dots & -2\Im\sigma_{r+s}(b_d) \end{pmatrix}\right|.$$

Subtracting rows $r+2a-1$ from rows $r+2a$ we obtain:

$$\mathrm{vol}(\mathcal{P}) = 2^{-s}\left|\det\begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \dots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \dots & \sigma_{r+1}(b_d) \\ \bar{\sigma}_{r+1}(b_1) & \dots & \bar{\sigma}_{r+1}(b_d) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \dots & \sigma_{r+s}(b_d) \\ \bar{\sigma}_{r+s}(b_1) & \dots & \bar{\sigma}_{r+s}(b_d) \end{pmatrix}\right|.$$

Reordering the rows we have:

$$\mathrm{vol}(\mathcal{P}) = 2^{-s}\left|\det\begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_d(b_1) & \dots & \sigma_d(b_d) \end{pmatrix}\right| = 2^{-s}\sqrt{|\Delta(\mathcal{B})|}.$$

□

179 Key Lemma *Let I be a non-zero ideal of $\mathfrak{o}_k$. Then there is a non-zero element $x \in I$ such that*

$$|N(x)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|}N(I),$$

where Δ is the discriminant of an integral basis.

Proof. Let $\mathcal{B}$ be a basis such that

$$I = \mathrm{span}_{\mathbb{Z}}\mathcal{B}.$$

Note that $\underline{\sigma}(I)$ is a lattice in k_∞ with covolume $2^{-s}\sqrt{|\Delta\mathcal{B}|}$. Recall that $N(I) = \sqrt{\frac{\Delta\mathcal{B}}{\Delta}}$. Hence the covolume is

$$\mathrm{vol}(k_\infty/\underline{\sigma}(I)) = 2^{-s}\sqrt{|\Delta|}N(I).$$

For any $a > 0$ consider the following subset of k_∞:

$$U_a = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{r+s} \end{pmatrix} : |x_i| < a \right\}.$$

The set U_a is clearly symmetric and convex. Its volume is given by

$$\mathrm{vol}(U_a) = (2a)^r(\pi a^2)^s = 2^r\pi^s a^d.$$

On the other hand if $\underline{\sigma}(x) \in U_a$ then for every field embedding we have $|\sigma_i(x)| < a$, which implies

$$N(x) < a^d.$$

We can apply Minkowski's Lemma with $\sigma(I)$ and U_a as long as

$$2^r \pi^s a^d > 2^d 2^{-s} \sqrt{|\Delta|} N(I).$$

This reduces to

$$a^d > cN(I).$$

where $c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|}$. As longs as a satisfies this inequality, there is a non-zero element $x \in I$ such that $\underline{\sigma}(x) \in U_a$, and hence $N(x) < a^d$.

We've shown that for any $b > cN(I)$, there is a non-zero $x \in I$ with $|N(x)| < b$. Now suppose

$$N = \min\{|N(x)| : x \in I \setminus \{0\}\}.$$

The minimum is attained since $N(x)$ takes integer values. Clearly $N < b$ for all $b > cN(I)$ and hence $N \leq cN(I)$. □

This finishes the proof that the class group is finite, and proves also that every ideal class contains an ideal whose norm is $\leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|}$.

Lecture 24

4.11 Calculating class groups

imaginary quadratic fields

Lecture 25

real quadratic fields

Lecture 26

cubic fields

Lecture 27

4.12 Dirichlet's Unit Theorem

We define a logarithmic map

$$\underline{\mathrm{Log}} : k^\times \to \mathbb{R}^{r+s}, \qquad \underline{\mathrm{Log}}(x) = \begin{pmatrix} \log|\sigma_1(x)| \\ \vdots \\ \log|\sigma_{r+s}(x)| \end{pmatrix}.$$

Clearly we have for $x, y \in k$,

$$\underline{\mathrm{Log}}(xy) = \underline{\mathrm{Log}}(x) + \underline{\mathrm{Log}}(y).$$

180 Proposition $\ker \underline{\mathrm{Log}}$ *is the subgroup of roots of unity in* k*.*

Proof. Suppose $x \in \ker \underline{\mathrm{Log}}$. This implies that $|\sigma_i(x)| = 1$ for all field embeddings σ_i. □

Now define a subspace

$$(\mathbb{R}^{r+s})_0 = \left\{ (v_i) \in \mathbb{R}^{r+s} : \sum v_i = 0 \right\}.$$

181 Proposition $\underline{\mathrm{Log}}(\mathfrak{o}^\times)$ *is a lattice in the subspace* $(\mathbb{R}^{r+s})_0$*.*