

**MATHEMATICS 129, SPRING 2009
NUMBER FIELDS**

KATHERINE E. STANGE

CONTENTS

1. Concerning These Notes	2
2. Introduction (First Day)	2
3. Algebraic Numbers and Integers	5
4. Linear Algebra for Number Theory	10
5. Review of Field Theory; Traces/Norms	10
6. Units: Some Notes Missing Here	16
7. Diophantine Approximation	16
8. The Trace Pairing	18
9. Linear Algebra and Discriminants	21
10. The Ring of Integers Inside the Number Field	26
11. Some Computational Aspects of Discriminants	28
12. Cyclotomic Fields	33
13. Noetherian Modules and Noetherian Rings	36
14. Ideals	39
15. Dedekind Domains	40
16. Ideals in Dedekind Domains	42
17. Norms of Ideals	47
18. Geometry of Numbers	49
19. Geometry of Canonical Embedding; Class Groups	51
20. Hermite's Theorem on Discriminants	55
21. Dirichlet's Unit Theorem	57
22. Rings of Fractions / Localisation	61
23. Splitting of Primes	65
24. Splitting in Quadratic Fields	66
25. Splitting of Primes – the Main Theorems	69
26. The Discriminant and Ramification	73
27. Quadratic Reciprocity	78
28. An example Class Number Formula	81
29. Galois extensions	83
30. Relative Norms of Ideals	86

Date: Last revised: May 12, 2009.

31.	The Different	88
32.	Galois extensions, decomposition, inertia	91
33.	Finite Fields	93
34.	Decomposition in Number Fields	94
35.	p-adic numbers	98
36.	Valuations, Absolute Values	100
37.	INSERT HERE AMEYA and FRANCOIS's NOTES ON VALUATIONS FROM THEIR FATEFUL MONDAY!	103
38.	Baby algebraic geometry: affine and projective space	103
39.	Introduction to elliptic curves	106
40.	Curves and Rings of Integers: Introduction	106

1. CONCERNING THESE NOTES

These are notes I've TeX'd as part of preparing lectures for Mathematics 129, Spring 2009, but they are, frankly, full of misprints and outright errors, since they represent a first and single draft only. Please let me know of any errors you find and I'll correct them immediately. Suggestions are also welcome.

These notes closely follow the course textbook, Samuel's *Algebraic Theory of Numbers*, and many of the proofs are simply lifted wholesale from Samuel. The notes add more examples, results and surrounding background to Samuel's spare and elegant narrative.

2. INTRODUCTION (FIRST DAY)

Number theory could be described as having its origins in the study of the interaction between the multiplicative and additive structures of \mathbb{Z} . Each of these structures is fairly simple in its own right, but as soon as they are to be compared, a host of easily stated but incredibly difficult questions arises.

For example the non-zero elements of \mathbb{Z} form a monoid with infinitely many generators: the primes, among which there are no relations, and -1 , of order two. There is unique factorisation, meaning that any element of \mathbb{Z} decomposes into a product of these generators in a manner which is unique up to reordering. But how are these all-important prime numbers distributed with respect to the linear ordering on \mathbb{Z} imposed by the additive structure? Specific questions include the study of the growth of the function

$$\pi(X) = \#\{p < X : p \text{ prime}\}.$$

Asymptotically, we know $\pi(X)$ grows like $x/\ln x$, but bounding the error term with ever-growing accuracy is one of the central questions of number theory. Another famous open question is the Twin Primes Conjecture, which states that there exist infinitely many primes p such that $p + 2$ is also prime. Tao and Green showed in 2005 that there are infinitely many 3-term progressions of Chen primes (primes such that $p + 2$ is either prime or a product of two distinct primes). These sorts of questions lead naturally to complex analytic methods and the study of Analytic Number Theory.

Another fundamental question is the question of integer or rational solutions to polynomial equations, which in this context are called Diophantine equations. For example, the equation

$$y^2 = x^3 + ax + b$$

where a and b are integer or rational coefficients, is called an *elliptic curve*. The rational solutions to this equation form a finitely generated abelian group under an operation defined by geometric construction (the *chord and tangent method*). One of the most famous open questions is whether arbitrarily large ranks occur.

Probably the most famous Diophantine equation is Fermat's Last Theorem:

$$x^n + y^n = z^n \text{ for } x, z, y, n \in \mathbb{Z}, n > 0 \implies n \leq 2 \text{ or } xyz = 0.$$

This was finally proven only in 1994 by Wiles and Taylor, and required a great deal of abstract and powerful theory, including the study of elliptic curves.

The study of Diophantine equations leads naturally to the subject of Algebraic Number Theory, our topic for this course. As an example, consider the Pythagorean triples, the solutions to

$$x^2 + y^2 = z^2.$$

Over the complex numbers, the equation factors as

$$(x + iy)(x - iy) = z^2.$$

This is fortunate, since it rewrites the question as being one principally of multiplication. In fact, to obtain this factorisation, it suffices to consider the equation over the field $\mathbb{Q}(i)$. We can rewrite the question as follows: find $\alpha, \beta \in \mathbb{Z}[i]$ such that $\alpha\bar{\alpha} = \beta^2$ and $\beta = \bar{\beta}$. Our hope is that the multiplicative structure of $\mathbb{Z}[i]$, the so-called *Gaussian integers* will be as tractable as that of \mathbb{Z} .

Warning: In Math 129, *ring* means commutative ring with identity.

Definition 2.1. Let R be a ring.

A unit in R is an element u such that there exists some v for which $uv = 1$.

A prime in R is a nonzero nonunit p such that if $p \mid ab$ then $p \mid a$ or $p \mid b$. (We say that $x \mid y \iff \exists c : xy = c$.)

An irreducible in R is a nonzero nonunit p such that if $p = ab$ then a is a unit or b is a unit.

We say that R is a unique factorisation domain if R is an integral domain and every nonzero $\alpha \in R$ has an expression as a product of irreducibles which is unique up to reordering and multiplication by units.

We also call any nonzero nonunit which is not irreducible reducible, and we say that two elements related by a factor of a unit are associates.

The notions of *prime* and *irreducible* coincide in \mathbb{Z} but not in arbitrary rings. Fortunately, the Gaussian integers $\mathbb{Z}[i]$ form a unique factorisation domain in which *prime* is equivalent to *irreducible*. The units of a ring always form a group and for $\mathbb{Z}[i]$ this group consists of $\pm 1, \pm i$. These statements are verified in the first homework.

Returning to the classification of Pythagorean triples, we may consider only those x , y and z that do not share a factor, since these ‘primitive’ solutions will generate all others. Since modulo 4 the only squares are 0 and 1, we can conclude that either z is odd and exactly one of x and y is odd (since at least one of x , y or z must be odd by assumption).

We will now show that $x + iy$ is a square times a unit.

First, suppose that π is a prime (=irreducible) in $\mathbb{Z}[i]$ dividing both $x + iy$ and $x - iy$. Then π must also divide their sum $2x$ and product z^2 in $\mathbb{Z}[i]$. Thanks to unique factorisation, we may conclude that π divides z . But $\gcd(2x, z) = 1$ in \mathbb{Z} , by the coprimality assumptions on x , y and z . Hence there exist $a, b \in \mathbb{Z}$ such that $2ax + bz = 1$. But π must divide this linear combination of $2x$ and z , proving that π is a unit, a contradiction. Hence, $x + iy$ and $x - iy$ share no prime factors in $\mathbb{Z}[i]$.

So assume that $\pi \mid x + iy$ and $\pi \nmid x - iy$. Then $\pi \mid z^2$, and by unique factorisation π appears to even power in the factorisation of $z^2 = (x + iy)(x - iy)$. Hence it appears to even power in $x + iy$, and we have shown that $x + iy$ is a square times a unit.

So $x + iy = u\gamma^2$ where $\gamma = m + ni$ and $u \in \{\pm 1, \pm i\}$. Squaring γ and considering the options, we obtain

Theorem 2.2. *The solutions to $x^2 + y^2 = z^2$ in \mathbb{Z} are exactly those where (x, y, z) or (y, x, z) is of the form*

$$(\pm d(m^2 - n^2), \pm 2dmn, \pm d(m^2 + n^2))$$

with $\gcd(m, n) = 1$ and $2 \mid mn$, $d \in \mathbb{Z}$.

Thus, the study of $x^2 + y^2 = z^2$ leads naturally $\mathbb{Q}[i]$ and $\mathbb{Z}[i]$ and its factorisation properties. Studying $x^n + y^n = z^n$ for larger n leads to other *number fields* (field extensions of \mathbb{Q} of finite degree) and their *rings of integers* (subrings consisting of roots of monic polies in $\mathbb{Z}[x]$). These are the objects of study of algebraic number theory. When unique factorisation fails, as it often does, studying these rings becomes very difficult.

Other possible definitions for Algebraic Number Theory are: the study of number fields; the study of the Galois group of $\overline{\mathbb{Q}}$ over \mathbb{Q} ; the study of algebraic integers. It could also be defined as the use of algebraic methods to answer questions about integers, or the study of generalisations of \mathbb{Z} and its properties, in particular factorisation. And much more besides.

Suppose that K is a number field and \mathcal{O}_K its ring of integers. Then there is an exact sequence

$$1 \rightarrow \mathcal{O}_K^* \rightarrow K^* \rightarrow I \rightarrow C(\mathcal{O}_K) \rightarrow 1$$

where R^* are the units of a ring R , I is the collection of *fractional ideals*, and $C(\mathcal{O}_K)$, the *class group* is what the sequence defines it to be: the fractional ideals modulo the principal ideals. The study of the two outer groups measures the failure of unique factorisation. Our main theorems will address the structure of these groups. The structure is difficult in general: as an example open question, it is not known whether real quadratic fields have trivial class group infinitely often, even though computations indicate it should happen some three quarters of the time.

We will study the factorisation of ideals, the splitting of ideals in extensions, and further topics to be decided as the course advances.

3. ALGEBRAIC NUMBERS AND INTEGERS

Definition 3.1. *If $A \subset R$ are rings, then $\beta \in R$ is integral over A if*

$$\beta^n + a_{n-1}\beta^{n-1} + \dots + a_0 = 0$$

for some $n \geq 1$, $a_i \in A$.

If A is a field, we say β is algebraic over A . If $A = \mathbb{Q}$, we say β is an algebraic number. If $A = \mathbb{Z}$, we say β is an algebraic integer.

Rational numbers q are algebraic numbers: $x - q = 0$. If $q \in \mathbb{Z}$, it is an algebraic integer. Other algebraic numbers are $\sqrt{2}$ (since $x^2 - 2 = 0$) and $\sqrt{\sqrt{3} + 7}$ (since $(x^2 - 7)^2 - 3 = 0$); these are also algebraic integers. Numbers such as

$$\sqrt[7]{8} - \frac{\sqrt[3]{5} + \sqrt[9]{3 + 2\sqrt[4]{8 + \sqrt[3]{2}}}}{\sqrt[8]{21} + 1}$$

are also algebraic numbers: we will show that the algebraic numbers form a field (Proposition 15.3) and the algebraic integers form a ring (Corollary 3.5), and that integrality is transitive in extensions (Proposition 3.11).

A more interesting example of an algebraic integer is

$$\frac{1 + \sqrt{5}}{2}$$

which has denominator but satisfies $x^2 - x - 1 = 0$. By contrast,

$$\frac{1 + \sqrt{3}}{2}$$

is not an algebraic integer. Its minimal polynomial is $x^2 - x - \frac{1}{2}$ and its non-integrality follows from the next proposition

Proposition 3.2. *The minimal polynomial of an algebraic integer α is in $\mathbb{Z}[x]$.*

Proof. Since α is an algebraic integer, it is the root of some $h(x) \in \mathbb{Z}[x]$ which is monic. Let $f(x) \in \mathbb{Q}[x]$ be its minimal polynomial, which is also monic. The minimal polynomial divides every other polynomial of which α is a root (since α is a root of the greatest common divisor of the minimal polynomial and the other polynomial, that gcd cannot have degree less than the minimal polynomial). So $h(x) = f(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. Choose some $a, b \in \mathbb{Z}$ such that $af(x), bg(x)$ are in $\mathbb{Z}[x]$ and have content one. (This is only possible since they are monic.) Then $abh(x) = af(x)bg(x)$ has content one by Gauss' lemma. But $h(x) \in \mathbb{Z}[x]$ is monic, so $ab = 1$ and $f \in \mathbb{Z}[x]$. \square

Example 3.3. *Let us find the algebraic integers in $\mathbb{Q}[i]$. Consider $\gamma = a + bi$. It satisfies the minimal polynomial $0 = (\gamma - a)^2 - b^2 = \gamma^2 - 2\gamma + a^2 + b^2$. So γ is algebraic if and only if $2a, a^2 + b^2 \in \mathbb{Z}$. From this we conclude that $a, b \in \frac{1}{2}\mathbb{Z}$, so suppose that $a = a'/2, b = b'/2$.*

Then

$$\begin{aligned} \gamma \text{ algebraic} &\iff a'^2 + b'^2 \equiv 0 \pmod{4} \\ &\iff a'^2 \equiv -b'^2 \pmod{4} \\ &\iff a'^2 \equiv b'^2 \equiv 0 \pmod{4} \end{aligned}$$

So in fact γ is algebraic if and only if $a, b \in \mathbb{Z}$. Thus the algebraic integers in $\mathbb{Q}[i]$ form the ring $\mathbb{Z}[i]$.

You will extend this analysis to all quadratic fields in your homework.

Theorem 3.4. *Let R be a ring with subring A and suppose $\alpha \in R$. The following are equivalent:*

- (1) α is algebraic over A .
- (2) $A[\alpha]$ is a finitely generated A -module.
- (3) There exists a subring $B \subset R$ such that
 - (a) $A \subset B$
 - (b) $\alpha \in B$
 - (c) B is a finitely generated A -module

Proof. 1 \implies 2: Let α satisfy a monic irreducible f of degree n over A . Let $M = A + A\alpha + \cdots + A\alpha^{n-1}$. Then $\alpha^n = -f(\alpha) + \alpha^n \in M$ and similarly $\alpha^{n+j} \in M$ for all $j \geq 0$. So $M = A[\alpha]$ is finitely generated as an A -module.

2 \implies 3: Immediate.

3 \implies 1: $B = Ay_1 + \cdots + Ay_n$ for some y_i . Then $\alpha y_i \in B$ so it has the form

$$\alpha y_i = \sum_{j=1}^n a_{ij} y_j$$

i. e. for each i ,

$$\sum_{j=1}^n (\alpha \delta_{ij} - a_{ij}) y_j = 0.$$

Let $M = (\alpha \delta_{ij} - a_{ij})$. Then $M^{adj} M = \det(M)I$ where adj denotes adjugate. Since $M(y_i) = (0)$, then $\det(M)y_i = 0$ for all y_i and so $\det(M)B = 0$. In particular, $\det(M) \cdot 1 = 0$ which implies $\det(M) = 0$. But $\det(M)$ is a monic polynomial of degree n in α , with coefficients in A . □

As in this proof, it will often be profitable to see a ring extension as a module over the base ring whose elements act as module homomorphisms by multiplication.

Corollary 3.5. *Let $A \subset R$ be rings. The elements of R integral over A form a ring.*

We will call this ring the *integral closure of A in R* .

Proof. If $a, b \in R$ are integral over A then $A[a]$ and $A[b]$ are finitely generated. Let a_i and b_i be finite sets spanning these two modules respectively. Then $A[a, b]$ is spanned by $a_i b_j$. Since ab and $a + b$ are contained in this finitely generated A -module inside R , they are integral over A . \square

Definition 3.6. *The integral closure of \mathbb{Z} in a finite extension K of \mathbb{Q} is called the ring of integers of K , denoted \mathcal{O}_K .*

Example 3.7.

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}, \quad \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z} + i\mathbb{Z}, \quad \mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z} + \left(\frac{1 + \sqrt{5}}{2}\right)\mathbb{Z}.$$

Definition 3.8. *The integral closure of A in its field of fractions is simply called the integral closure.*

A ring is integrally closed if it is an integral domain and it is its own integral closure.

A ring B is integral over a subring A if all elements of B are integral over A .

Example 3.9. *We will show that $\alpha = \sqrt{2} + i$ is algebraic by finding a monic polynomial of \mathbb{Z} coefficients which has this root. Consider the ring $A[\sqrt{2}, i] = A + \sqrt{2}A + iA + \sqrt{2}iA$. Multiplication by $(\sqrt{2} + i)$ has, with respect to this basis, the matrix*

$$\begin{pmatrix} 0 & 2 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

The characteristic polynomial of this matrix is $x^4 - 2x^2 + 9$. Exactly as in the proof of Theorem 3.4, α must satisfy this equation. Therefore it is integral. In fact, this is its minimal polynomial. (To see this last remark, it suffices to see that α is degree 4 over \mathbb{Q} . Since $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}, i)$ which degree four and Klein 4 Galois group, the only possibilities for $\mathbb{Q}(\alpha)$ are $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(i)$. Since the three latter fields intersect pairwise in \mathbb{Q} , it must be the larger field.)

Theorem 3.10. *Let d be a squarefree integer. Then*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z} + \sqrt{d}\mathbb{Z} & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z} + \left(\frac{1 + \sqrt{d}}{2}\right)\mathbb{Z} & d \equiv 1 \pmod{4} \end{cases}$$

Proof. Exercise in homework. \square

Proposition 3.11. *Let $A \subset B \subset C$ be rings. If C is integral over B and B is integral over A , then C is integral over A .*

Proof. Let $\alpha \in C$. Then for some $b_i \in B$, we have an equation of integrality:

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0.$$

Let $B' = A[b_0, \dots, b_{n-1}]$. Then α is integral over B' . So $B'[\alpha]$ is a finitely generated B' -module. But B' is a finitely generated A -module. So $B'[\alpha] = A[b_0, \dots, b_{n-1}, \alpha]$ is a finitely generated A -module containing α and so α is integral over A . \square

Proposition 3.12. *Let α be an algebraic number. Then there exists $d \in \mathbb{Z}$ such that $d\alpha$ is an algebraic integer.*

Proof. For some monic $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$, we have $f(\alpha) = 0$. So there exists some $d \in \mathbb{Z}$ such that $df(x) \in \mathbb{Z}[x]$ (a common denominator to all coefficients a_i). Then

$$\begin{aligned} 0 &= d^n f(\alpha) \\ &= d^n \alpha^n + d^n a_{n-1} \alpha^{n-1} + \cdots + d^n a_0 \\ &= (d\alpha)^n + da_{n-1}(d\alpha)^{n-1} + \cdots + d^{n-1}a_1(d\alpha) + d^n a_0 \end{aligned}$$

which is an equation of integrality for $d\alpha$ since each coefficient is in \mathbb{Z} . \square

We have several important corollaries.

Corollary 3.13. *Let K be a number field. The field of fractions of \mathcal{O}_K is K .*

Proof. Let L be the field of fractions of \mathcal{O}_K . Then L is the smallest field containing \mathcal{O}_K . So $L \subset K$. If $[K : L] > 1$, then there exists some $\alpha \in K \setminus L$ which is algebraic over \mathbb{Q} . So there exists a $d \in \mathbb{Z}$ so that $d\alpha \in K \setminus L$ is integral over \mathbb{Q} . So $d\alpha \in \mathcal{O}_K$ but $d\alpha \notin L$, a contradiction. \square

Corollary 3.14. $\mathbb{Q}\mathcal{O}_K = K$

Proof. Let $\alpha \in K$. Then $d\alpha \in \mathcal{O}_K$ for some $d \in \mathbb{Z}$, so $\alpha = \frac{1}{d}d\alpha$. So $K \subset \mathbb{Q}\mathcal{O}_K$. Conversely, any $\frac{a}{b}\alpha$ where $\alpha \in \mathcal{O}_K$ and $a, b \in \mathbb{Z}$, is in the field of fractions of \mathcal{O}_K which is contained in K . \square

Corollary 3.15. \mathcal{O}_K is integrally closed.

Proof. Suppose not. Then there is some $\alpha \in K$ such that α is integral over \mathcal{O}_K . Since \mathcal{O}_K is integral over \mathbb{Z} , then α is integral over \mathbb{Z} . Then $\alpha \in \mathcal{O}_K$ by definition. \square

4. LINEAR ALGEBRA FOR NUMBER THEORY

Suppose that A is a ring and B is a free A -module of rank n . Let $u : B \rightarrow B$ be an endomorphism of A -modules. This situation is a generalisation of the case where A is a field, B a vector space over that field, and u a linear transformation. We wish to generalise some of the linear algebra of vector spaces to modules.

Suppose that $\{e_i\}_{i=1}^n$ is a basis for B over A (the fact that B is a free A -module of rank n guarantees the existence of such a basis). Then u has a matrix with respect to this basis, i.e. $M = (a_{ij})$, where each entry $a_{ij} \in A$. We define the following:

$$\text{trace: } \text{Tr}(u) = \sum_{i=1}^n a_{ii}$$

$$\text{determinant: } \det(u) = \det(a_{ij})$$

$$\text{characteristic polynomial: } \det(X \cdot I - u) = \det(X\delta_{ij} - a_{ij})$$

These things are all independent of basis.

If B is a ring also, and $\alpha \in B$, then $m_\alpha : B \rightarrow B$ taking $y \mapsto \alpha y$ is an endomorphism of B as an A -module. In this case we say

$$\text{trace: } \text{Tr}(\alpha) = \text{Tr}_{B/A}(\alpha) = \text{Tr}(m_\alpha)$$

$$\text{norm: } N(\alpha) = N_{B/A}(\alpha) = \det(m_\alpha)$$

$$\text{characteric polynomial: } c_\alpha(X) = c_{B/A, \alpha}(X) = \det(X \cdot I_B - m_\alpha)$$

Proposition 4.1. *The following properties hold, where $x, x' \in B, a \in A$:*

- (1) $\text{Tr}(x + x') = \text{Tr}(x) + \text{Tr}(x')$
- (2) $\text{Tr}(ax) = a\text{Tr}(x)$
- (3) $\text{Tr}(a) = na$
- (4) $N(xx') = N(x)N(x')$
- (5) $N(a) = a^n$
- (6) $N(ax) = a^n N(x)$

Proof. Exercise in homework. □

Note that the constant term of $c_\alpha(X)$ is $(-1)^{\deg c_\alpha} N(\alpha)$ and the coefficient of $x^{\deg c_\alpha - 1}$ is $-\text{Tr}(\alpha)$.

5. REVIEW OF FIELD THEORY; TRACES/NORMS

If L/K is a finite separable extension of degree d , then there are exactly d distinct embeddings of L into \overline{K} fixing the elements of K . Recall that any field which has characteristic zero or is finite is separable. A homework question asks you to work out a famous example of

a non-separable extension. In this class, all fields will be separable until further notice.

The embeddings of L into \overline{K} can be labelled $\sigma_i : L \rightarrow \overline{K}$ for $i = 1, \dots, d$. Furthermore, if $L = K(\alpha)$, then $\{\alpha^{\sigma_i}\}_{i=1}^d$ are exactly the roots of the minimal polynomial of α over K , called the *conjugates* of α (note that a^σ is notation for $\sigma(a)$). If, more generally, $[L : K(\alpha)] = m$, and $[K(\alpha) : K] = n$ (so in particular $nm = d$), then the set of all α^{σ_i} runs over each of the n conjugates of α m times each.

The trace and norm of an element can be expressed in terms of its conjugates.

Theorem 5.1. *Let L/K be a separable field extension of degree d . Let $\sigma_1, \dots, \sigma_d$ be the embeddings of L into \overline{K} . Let $\alpha \in L$. Then*

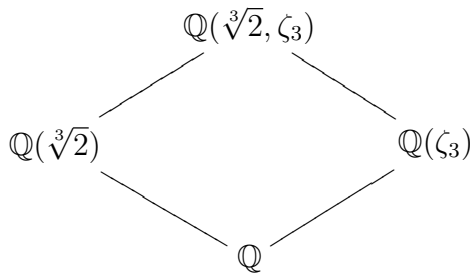
$$\text{Tr}_{L/K}(\alpha) = \sum_{i=1}^d \alpha^{\sigma_i}, \quad N_{L/K}(\alpha) = \prod_{i=1}^d \alpha^{\sigma_i}.$$

Furthermore,

$$c_{L/K,\alpha}(X) = (m_{K,\alpha}(X))^{[L:K(\alpha)]}.$$

Before proving the theorem, consider an extended example.

Example 5.2. *Let $\zeta_3 = \frac{1+\sqrt{-3}}{2}$ be a primitive cube root of unity. Then the other primitive cube root of unity is $\zeta_3^2 = \frac{1-\sqrt{-3}}{2}$. These are the roots of the polynomial $x^2 + x + 1$ irreducible over \mathbb{Q} . Let $\sqrt[3]{2}$ denote the real cube root of 2. Consider the field extensions:*



Note that $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. The embeddings of $\mathbb{Q}(\sqrt[3]{2})$ into $\overline{\mathbb{Q}}$ (we may as well assume $\overline{\mathbb{Q}} \subset \mathbb{C}$) are

$$\sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3, \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2.$$

(We need only specify where $\sqrt[3]{2}$ goes to determine the embedding, since it fixes \mathbb{Q} .) The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ which has as its roots $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$. These are the conjugates of $\sqrt[3]{2}$ in the extension.

We can determine the trace and norm of $\sqrt[3]{2}$ directly by considering it as an endomorphism of the vector space $\mathbb{Q}(\sqrt[3]{2})$ over \mathbb{Q} . That is, suppose we take the basis $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ of $\mathbb{Q}(\sqrt[3]{2})$ over \mathbb{Q} . Then $m_{\sqrt[3]{2}}$ has matrix

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Thus the trace is $\text{Tr}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2}) = 0$, and the determinant gives $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2}) = 2$. We also have

$$c_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}, \sqrt[3]{2}}(X) = \det \begin{pmatrix} X & 0 & -2 \\ -1 & X & 0 \\ 0 & -1 & X \end{pmatrix} = X^3 - 2.$$

We can do the same calculation from the conjugates, thus

$$\begin{aligned} \text{Tr}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2}) &= \sqrt[3]{2} + \sqrt[3]{2}\zeta_3 + \sqrt[3]{2}\zeta_3^2 \\ &= \sqrt[3]{2}(1 + \zeta_3 + \zeta_3^2) \\ &= \sqrt[3]{2} \cdot 0 = 0, \end{aligned}$$

and

$$\begin{aligned} N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot \sqrt[3]{2}\zeta_3 \cdot \sqrt[3]{2}\zeta_3^2 \\ &= \sqrt[3]{2}^3 (\zeta_3^3) \\ &= 2 \cdot 1 = 2, \end{aligned}$$

and finally,

$$\begin{aligned} c_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}, \sqrt[3]{2}}(X) &= (X - \sqrt[3]{2})(X - \sqrt[3]{2}\zeta_3)(X - \sqrt[3]{2}\zeta_3^2) \\ &= (X - \sqrt[3]{2})(X^2 - \sqrt[3]{2}(\zeta_3 + \zeta_3^2)X + \sqrt[3]{2}^2) \\ &= X^3 - 2. \end{aligned}$$

We have verified the theorem in a special case.

Now consider instead the extension of $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ over \mathbb{Q} . The extension K is degree 6 over \mathbb{Q} and can be thought of as a tower of extensions

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \\ \left| \begin{array}{c} 2 \\ 3 \end{array} \right. \\ \mathbb{Q}(\sqrt[3]{2}) \\ \left| \begin{array}{c} 3 \end{array} \right. \\ \mathbb{Q} \end{array}$$

It becomes apparent that a basis for K over \mathbb{Q} is given by

$$1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta_3, \zeta_3 \sqrt[3]{2}, \zeta_3 \sqrt[3]{2}^2.$$

Thus we can write the matrix M for the endomorphism $m_{\sqrt[3]{2}}$ in terms of this basis. It is

$$\begin{pmatrix} 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

since, for example, $\sqrt[3]{2}(\zeta_3 \sqrt[3]{2}^2) = 2\zeta_3$. From this we find that

$$\text{Tr}(\sqrt[3]{2}) = \text{Tr}(M) = 0, \quad N(\sqrt[3]{2}) = \det(M) = 4,$$

and the characteristic polynomial of $\sqrt[3]{2}$ is

$$\det(X \cdot I - M) = (X^3 - X)^2.$$

Again, we can do these same calculations using conjugates. We need to know the embeddings of K into \mathbb{C} . These are given by all possible choices for the images of $\sqrt[3]{2}$ and ζ_3 (these are independent since the fields these two elements generate intersect only in \mathbb{Q}). Thus, there are three choices for the image of $\sqrt[3]{2}$:

$$\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$$

and there are two choices for the image of ζ_3 :

$$\zeta_3, \zeta_3^2.$$

This gives six total embeddings.

The conjugates of $\sqrt[3]{2}$ in this extension are therefore

$$\sqrt[3]{2}, \sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2, \sqrt[3]{2}\zeta_3^2.$$

Each of the three conjugates of $\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$ over \mathbb{Q} are repeated twice because for each choice of image of $\sqrt[3]{2}$, there are two embeddings.

Now what remains is just a calculation: We can do the same calculation from the conjugates, thus

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}) &= 2(\sqrt[3]{2} + \sqrt[3]{2}\zeta_3 + \sqrt[3]{2}\zeta_3^2) \\ &= 2 \cdot 0 = 0 \end{aligned}$$

and

$$\begin{aligned} N_{K/\mathbb{Q}}(\sqrt[3]{2}) &= (\sqrt[3]{2} \cdot \sqrt[3]{2}\zeta_3 \cdot \sqrt[3]{2}\zeta_3^2)^2 \\ &= \sqrt[3]{2}^6 (\zeta_3^6) \\ &= 2^2 \cdot 1 = 4, \end{aligned}$$

and finally,

$$\begin{aligned} c_{K/\mathbb{Q}, \sqrt[3]{2}}(X) &= (X - \sqrt[3]{2})^2 (X - \sqrt[3]{2}\zeta_3)^2 (X - \sqrt[3]{2}\zeta_3^2)^2 \\ &= (X - \sqrt[3]{2})^2 (X^2 - \sqrt[3]{2}(\zeta_3 + \zeta_3^2)X + \sqrt[3]{2}^2)^2 \\ &= (X^3 - 2)^2 \\ &= (m_{\mathbb{Q}, \sqrt[3]{2}}(\sqrt[3]{2}))^2. \end{aligned}$$

And again we have verified the theorem. Note that the 2's that show up here (the trace is twice what we calculated for the the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, the norm the square) is the degree $[K : \mathbb{Q}(\sqrt[3]{2})]$.

Proof. Proof of the Theorem 5.1. Suppose first that $L = \mathbb{Q}(\alpha)$. In this case, $L \cong K[X]/m_{K,\alpha}(X)$ and L/K is a vector space of dimension d with basis $1, x, \dots, x^{d-1}$. Let $m_{K/\alpha}(X) = X^d + a_{d-1}X^{d-1} + \dots + a_0$. Then m_α has matrix

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & & & -a_2 \\ & \ddots & \ddots & & \vdots \\ & & 0 & 1 & -a_{d-1} \end{pmatrix}$$

So,

$$\begin{aligned} c_{L/K,\alpha}(X) &= \det(X \cdot I_d - M) \\ &= \det \begin{pmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & & & a_2 \\ & \ddots & \ddots & & \vdots \\ & & 0 & -1 & X + a_{d-1} \end{pmatrix} \\ &= m_{K,\alpha}(X) \end{aligned}$$

The trace and norm statements follow from this statement.

Now we must consider the case where we have a tower

$$\begin{array}{c} L \\ | \\ m \\ K(\alpha) \\ | \\ n \\ K \end{array}$$

Where the upper extension has basis z_1, \dots, z_m and the lower extension has basis $1, \dots, x^{n-1}$. Then a basis for the extension L/K is $x^{j-1}z_i$ where $i = 1, \dots, m$ and $j = 1, \dots, n$. Then m_α has a block diagonal matrix

$$M' = \begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix}$$

where M is the matrix from the first part of the proof for $K(\alpha)/K$ (each block corresponds to basis elements $x^{j-1}z_i$ for fixed i). Thus,

$$c_{L/K,\alpha}(X) = \det(X \cdot I_d - M') = \det(X \cdot X_n - M)^m = m_{K,\alpha}(X)^m.$$

As before, the trace and norm statements follow from this, since the roots of the minimal polynomial are the conjugates for the extension $K(\alpha)$. \square

Corollary 5.3. *Let L/K be an extension of number fields and suppose $\alpha \in L$ is integral over \mathcal{O}_K . Then the coefficients of $c_{L/K,\alpha}(X)$ are in \mathcal{O}_K . In particular, $Tr_{L/K}(\alpha), N_{L/K}(\alpha) \in \mathcal{O}_K$.*

Proof. Let $h(\alpha) = 0$ where $h(x) \in \mathcal{O}_K[x]$. Then $h(\alpha^{\sigma_i}) = (h(\alpha))^{\sigma_i} = 0^{\sigma_i} = 0$. So all the conjugates of α are integral over \mathcal{O}_K and so the coefficients of $c_{L/K,\alpha}(X)$ are integral over \mathcal{O}_K , but they are also in K , from which the result follows. \square

Recall that we proved this for $K = \mathbb{Q}$ using Gauss' lemma; Gauss' lemma was not strong enough to generalise to arbitrary extensions of number fields.

Proposition 5.4. *Suppose we have a tower of number fields $K \subset L \subset M$. Suppose that $a \in M$. Then we have*

$$\begin{aligned} Tr_{M/K}(a) &= Tr_{L/K}(Tr_{M/L}(a)), \\ N_{M/K}(a) &= N_{L/K}(N_{M/L}(a)). \end{aligned}$$

Proof. Suppose the embeddings of L into \overline{K} fixing K are σ_i for $i = 1, \dots, n$. Suppose the embeddings of M into \overline{L} fixing L are τ_j for $j = 1, \dots, m$. For each σ_i , choose an embedding $\overline{\sigma}_i$ of \overline{L} into \overline{K} which extends σ_i . My claim is that $\overline{\sigma}_i \circ \tau_j$ are all distinct embeddings of M into \overline{K} fixing K . Clearly they fix K . To see that they are distinct, suppose $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i'} \circ \tau_{j'}$. Then they are equal when restricted to L , where they are just σ_i and $\sigma_{i'}$; thus $\sigma_i = \sigma_{i'}$. Therefore, $\overline{\sigma}_i \circ \tau_j - \overline{\sigma}_{i'} \circ \tau_{j'} = \overline{\sigma}_i \circ (\tau_j - \tau_{j'}) = 0$. Since $\overline{\sigma}_i$ is an embedding (in particular injective), it must be that $\tau_j = \tau_{j'}$.

Now, there are exactly nm such embeddings and that is the degree of M over K , so these are the complete set of embeddings of M into \overline{K} . Now it remains to compute

$$\text{Tr}_{M/K}(a) = \sum_{i,j} a^{\overline{\sigma}_i \circ \tau_j}$$

while

$$\text{Tr}_{L/K}(\text{Tr}_{M/L}(a)) = \sum_i \left(\sum_j a^{\tau_j} \right)^{\sigma_i} = \sum_{i,j} a^{\overline{\sigma}_i \circ \tau_j}.$$

The norm calculation is very similar. □

6. UNITS: SOME NOTES MISSING HERE

Theorem 6.1. *Let L/K be an extension of number fields. ...*

not yet tex'd lots...

7. DIOPHANTINE APPROXIMATION

The following is a result of Liouville in 1844.

Theorem 7.1. *Let α be an algebraic number of degree $d \geq 2$. Then there exists a constant $c = c(\alpha) > 0$ such that*

$$\left| \frac{p}{q} - \alpha \right| > \frac{c}{q^d}$$

for all $p, q \in \mathbb{Z}$.

Proof. Since the theorem is trivial otherwise, we may assume that α is real. Let $P(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α , having degree d . Then, the Mean Value Theorem applies to P and there exists some z lying between α and $\frac{p}{q}$ such that

$$P(\alpha) - P\left(\frac{p}{q}\right) = \left(\alpha - \frac{p}{q}\right) P'(z).$$

Now, since $q^d P\left(\frac{p}{q}\right)$ is an integer, and P has no rational roots,

$$\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}.$$

Now, the stated inequality holds trivially unless

$$\left|\frac{p}{q} - \alpha\right| < 1.$$

So $|z| < |\alpha| + 1$. Thus, $P'(z)$ is bounded depending on α , i.e.

$$|P'(z)| < K$$

for some $K = K(\alpha)$. Thus

$$\left|\frac{p}{q} - \alpha\right| = \frac{\left|P\left(\frac{p}{q}\right)\right|}{|P'(z)|} > \frac{1}{Kq^d}.$$

□

The steps of the proof are roughly as follows: choose a polynomial which vanishes at α ; bound its value at $\frac{p}{q}$ away from zero (using the discreteness of integers); bound its value at $\frac{p}{q}$ close to zero (using analysis or geometry); derive a contradiction from the two inequalities for p, q not satisfying the theorem.

Liouville's result can be restated as follows:

If α is algebraic of degree d , then $\left|\frac{p}{q} - \alpha\right| < \frac{q}{q^m}$ has only finitely many solutions.

where $m > d$. In 1908, Thue improved this to $m > d/2 + 1$; Siegel in 1921 to $m > 2\sqrt{d}$; Dyson in 1947 to $m > \sqrt{2d}$, and Roth to $m > 2$ in his Fields Medal winning work of 1955. Each of these proofs is roughly of the same plan as Liouville's, presented here, but much more difficult, having more variables and dimensions and requiring tools from arithmetic geometry. For more about these proofs, see Hindry and Silverman, [?].

The 'best' rational approximants (as measured with respect to their own denominators) to a number are governed by the coefficients in the continued fraction expansion of the number (bounded coefficients means poor approximation). As such, a cardinality argument demonstrates that a converse to Liouville's theorem cannot hold. For more about continued fractions and their relationship to this study of *Dio-phantine Approximation*, see [?].

8. THE TRACE PAIRING

Let $A \subset B$ be rings, where B is a free A -module of rank n . Then we may define a bilinear pairing

$$B \times B \rightarrow A$$

given by

$$(x, y) \mapsto \text{Tr}_{B/A}(xy),$$

called the trace pairing. (Check that this is bilinear.)

As an example of such a pairing, consider the cyclotomic extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ where p is a prime and ζ_p a primitive p -th root of unity. Since ζ_p satisfies

$$1 + \zeta_p + \zeta_p^2 + \dots + \zeta_p^{p-1},$$

a basis for this extension is

$$1, \quad \zeta_p, \quad \dots, \quad \zeta_p^{p-2}.$$

Thus, to compute the trace pairing, we must compute

$$\text{Tr}(\zeta_p^n) = \begin{cases} -1 & \gcd(n, p) = 1 \\ p-1 & \gcd(n, p) = p \end{cases}$$

(Do it as an exercise.) Thus, with respect to the basis chosen, the trace pairing can be expressed as the matrix

$$(\text{Tr}(\zeta_p^{i+j})) =$$

Now, under the rule that any interesting matrix has an interesting determinant, let's compute the determinant.

$$\begin{aligned} \det(\text{Tr}(\zeta_p^{i+j})) &= \det \begin{pmatrix} p & -1 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & p & \cdots & 0 \end{pmatrix} \\ &= p \cdot \det \begin{pmatrix} -1 & 0 & \cdots & 0 \\ -1 & 0 & \cdots & p \\ \vdots & \vdots & \ddots & \vdots \\ -1 & p & \cdots & 0 \end{pmatrix} \\ &= -p \cdot \det \begin{pmatrix} 0 & \cdots & p \\ \vdots & \ddots & \vdots \\ p & \cdots & 0 \end{pmatrix} \\ &= -p(-1)^{\frac{p-3}{2}} \cdot \det \begin{pmatrix} p & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & p \end{pmatrix} \\ &= (-1)^{\frac{p-1}{2}} p^{p-2}. \end{aligned}$$

In general, the *discriminant* of a bilinear pairing is the determinant of its matrix, which is defined up to squares of units, since if the pairing has matrix A with respect to one basis and A' with respect to a second, then

$$A' = B^t AB$$

where B is the appropriate change of basis matrix between the two bases. Thus,

$$\det(A') = \det(B)^2 \det(A).$$

where $\det(B)$ must be a unit.

A pairing is called *degenerate* if there exists some x which pairs with everything else trivially, i.e. $\langle x, y \rangle = 0$ for all y . One can show (do it) that a pairing is degenerate if and only if its discriminant is zero.

Exercise: Show that if B is a field, the trace pairing is nondegenerate.

Definition 8.1. If $x_1, \dots, x_n \in B$, the discriminant of the set is

$$\text{disc}(x_1, \dots, x_n) = \det(\text{Tr}_{B/A}(x_i x_j)).$$

If x_1, \dots, x_n form a basis for B over A , we call the class of $\text{disc}(x_1, \dots, x_n)$ up to squares of units the discriminant of B over A .

Now, for a field B , these classes tend to be rather large: there are only two classes modulo squares of units in \mathbb{Q} (zero is disregarded), four in $\mathbb{Q}(\sqrt{2})$ and one in \mathbb{C} for example. So we will concern ourselves with the case of $\mathcal{O}_L/\mathcal{O}_K$.

We have not shown this yet, but it is true that, $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ and so $1, \zeta_p, \dots, \zeta_p^{p-2}$ form a basis for the ring of integers of $\mathbb{Q}(\zeta_p)$. Our example above then shows that

$$\text{disc}(\mathcal{O}_{\mathbb{Q}(\zeta_p)}/\mathbb{Z}) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Since the only square of a unit in \mathbb{Z} is 1, the discriminant of any ring of integers over \mathbb{Z} is actually an integer.

By what should probably be considered abuse of language, we set the following convention.

Definition 8.2. For a number field K , the discriminant of the field K is

$$\text{disc}(K) = \text{disc}(\mathcal{O}_K/\mathbb{Z}).$$

Samuel sets the following definition.

Definition 8.3. The ideal in A generated by $\text{disc}(x_1, \dots, x_n)$ for any basis x_1, \dots, x_n is denoted $\mathcal{D}_{B/A}$.

Proposition 8.4. A set $x_1, \dots, x_n \in B$ is a basis over A if and only if

$$(\text{disc}(x_1, \dots, x_n)) = \mathcal{D}_{B/A}.$$

Proof. One direction has already been established.

Suppose x_1, \dots, x_n is a basis for B over A and y_1, \dots, y_n is a collection of elements in B . Then let $d' = \text{disc}(x_1, \dots, x_n)$ and let $d = \text{disc}(y_1, \dots, y_n)$.

Suppose now that $\mathcal{D}_{B/A} = (d') = (d)$. Then $d' = bd$ for a unit b . But since the x_i form a basis,

$$y_i = \sum_j a_{ij} x_j$$

for each i , and so $d = \det(a_{ij})^2 d'$.

Combining the equations, $d(1 - b \det(a_{ij})^2) = 0$ and since d is not a zero-divisor, then $\det(a_{ij})$ is a unit, and the y_i form a basis. \square

As usual, we must update the running example of quadratic fields. Let d be a squarefree and nonzero integer. Then

$$\text{disc}(1, \sqrt{d}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

If d is 1 modulo 4, then we should instead consider

$$\text{disc} \left(1, \frac{1 + \sqrt{d}}{2} \right) = \det \begin{pmatrix} 2 & 1 \\ 1 & 2\frac{d+1}{2} \end{pmatrix} = d.$$

Thus,

$$\text{disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} 4d & d \equiv 2, 3 \pmod{4} \\ d & d \equiv 1 \pmod{4} \end{cases}$$

9. LINEAR ALGEBRA AND DISCRIMINANTS

We begin with the following observation. Suppose that L/K is a separable field extension of degree n with embeddings $\sigma_1, \dots, \sigma_n$ and basis x_1, \dots, x_n . Then

$$\begin{aligned} \text{disc}(x_1, \dots, x_n) &= \det(\text{Tr}(x_i x_j)) \\ &= \det \left(\sum_k \sigma_k(x_i x_j) \right) \\ &= \det \left(\sum_k \sigma_k(x_i) \sigma_k(x_j) \right) \\ &= \det(\sigma_k(x_i)) \det(\sigma_k(x_j)) \\ &= \det(\sigma_i(x_j))^2 \end{aligned}$$

Now, the calculation is easy enough, but I think this should bring to mind some questions. In general, whenever one writes down a matrix, there is a linear transformation to which it is associated, and it can be fruitful to see things from the viewpoint of linear algebra. In our case, the matrix $(\sigma_i(x_j))$ seems to be the mysterious one. In this section we will answer the question “what is this map?”

To begin, let’s consider a specific case. Suppose that $B = \mathbb{Q}(\sqrt{2})$ and $A = \mathbb{Q}$. Then $1, \sqrt{2}$ will serve as a basis for $\mathbb{Q}(\sqrt{2})$ considered as a vector space over \mathbb{Q} .

With respect to this basis, multiplication by $\sqrt{2}$ has matrix

$$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

This matrix has eigenvalues $\sqrt{2}$ and $-\sqrt{2}$ (the roots of the minimal polynomial for $\sqrt{2}$), so it is not diagonalisable over \mathbb{Q} . The idea is to extend scalars so that this matrix becomes diagonalisable. That is, just allow the scalars to live in a larger field, in this case $\mathbb{Q}(\sqrt{2})$ or \mathbb{C} would do fine. Then, in this new extended vector space, the matrix

diagonalises as

$$\begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$$

The change of basis that accomplishes this diagonalisation has matrix

$$\begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}$$

which is the matrix $(\sigma_i(x_j))$ we have been wondering about.

Now, you'll immediately notice that there's some confusion inherent in this situation: we are using basis $1, \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$. That is, we have a vector $\sqrt{2}$ and a scalar $\sqrt{2}$ and we need to keep them straight: we need to setup the correct formalism before all hell breaks loose.

What we need is some commutative algebra.

9.1. Tensor Products. The description of tensor products I give here follows Atiyah-Macdonald [?] in Chapter 2 (pp.24-28).

Suppose that M and N are A -modules. The tensor product, denoted $M \otimes_A N$ is an A module which comes with a map $g : M \times N \rightarrow M \otimes_A N$ and is characterised by the following universal property:

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & P \\ \downarrow g & \nearrow f' & \\ M \otimes_A N & & \end{array}$$

For all A -bilinear maps f from $M \times N$ to another A -module P , there exists a unique A -bilinear map $f' : M \otimes_A N \rightarrow P$ such that the diagram commutes. It follows that the module $M \otimes_A N$ is unique up to unique isomorphism. (Check this by using the universal property twice.)

The idea is to construct a module $M \otimes_A N$ which is the *bilinear* combination of M and N : every bilinear map from $M \times N$ will factor through it. As I give the construction, compare the abelianisation of a group, for example.

Let $C = A^{M \times N}$ be the free A -module on the symbols (m, n) where $m \in M$ and $n \in N$. Let D be the submodule generated by

$$\begin{aligned} &(x + x', y) - (x, y) - (x', y), \\ &(x, y + y') - (x, y) - (x, y'), \\ &(ax, y) - a(x, y), \\ &(x, ay) - a(x, y). \end{aligned}$$

Let $M \otimes_A N = C/D$ where we now denote the class of (m, n) by $m \otimes n$. The map $g : M \times N \rightarrow M \otimes_A N$ is simply the quotient map $g(m, n) = m \otimes n$.

In the case that M and N are free A -modules of rank m and n with bases e_1, \dots, e_m and f_1, \dots, f_n respectively, the module $M \otimes_A N$ is a free A -module of rank mn with basis

$$\{e_i \otimes f_j\}_{1 \leq i \leq m, 1 \leq j \leq n}.$$

A little practice with the calculations is in order:

$$g\left(\sum_i a_i e_i, \sum_j b_j f_j\right) = \left(\sum_i a_i e_i\right) \otimes \left(\sum_j b_j f_j\right) = \sum_{i,j} a_i b_j (e_i \otimes f_j)$$

We also have such things as

$$0 \otimes a = 0(1 \otimes a) = 0 = 0(b \otimes 1) = b \otimes 0.$$

Now, our purpose in introducing tensor products is to have an appropriate notation for *extension of scalars* discussed informally in the last section.

If M is an A -module, and $A \subset B$ are rings (so in particular B is an A module), then the A -module $B \otimes_A M$ is also a B -module under the B -action $b'(b \otimes m) = b'b \otimes m$ for $b, b' \in B, m \in M$.

For example, suppose $V = \mathbb{Q}^2$ is a \mathbb{Q} vector space with standard basis e_1, e_2 . Also we have seen that $\mathbb{Q}(i)$ has basis $1, i$ as a \mathbb{Q} vector space. The tensor product $\mathbb{Q}(i) \otimes_{\mathbb{Q}} V$ is of dimension 4 and has basis $1 \otimes e_1, 1 \otimes e_2, i \otimes e_1, i \otimes e_2$ as a \mathbb{Q} vector space. But it is also a $\mathbb{Q}(i)$ vector space of dimension 2, with basis $1 \otimes e_1$ and $1 \otimes e_2$. For example, $i \otimes e_i = i(1 \otimes e_i)$ is a scalar multiple of $1 \otimes e_i$ under the $\mathbb{Q}(i)$ vector space structure.

In general, if $K \subset L$ are fields and $V \cong K^n$, then $L \otimes_K V \cong L^n$. In fact, if a basis for V over K is e_1, \dots, e_n , then a basis for $L \otimes_K V$ over L is $1 \otimes e_1, \dots, 1 \otimes e_n$.

Finally, let's consider the example we were working with informally. Consider $B = \mathbb{Q}(\sqrt{2})$ as a \mathbb{Q} vector space with basis $1, \sqrt{2}$. Extend scalars to $B \otimes_{\mathbb{Q}} B$. The tensor product is a \mathbb{Q} vector space with basis $1 \otimes 1, 1 \otimes \sqrt{2}, \sqrt{2} \otimes 1, \sqrt{2} \otimes \sqrt{2}$. But as a B vector space it is two-dimensional with basis $1 \otimes 1, 1 \otimes \sqrt{2}$. For example, $\sqrt{2} \otimes \sqrt{2} = \sqrt{2}(1 \otimes \sqrt{2})$.

Multiplication by $\sqrt{2}$ in the right factor is a linear transformation. It has matrix

$$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

in the vector space $\mathbb{Q}(\sqrt{2})$ over \mathbb{Q} or in the vector space $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$.

Define $\phi : B \otimes_{\mathbb{Q}} B \rightarrow B^2$ by

$$\phi(a \otimes b) = a(\sigma_1(b), \sigma_2(b))$$

(where as usual the σ 's are the embeddings over \mathbb{Q}). Alternatively, we could extend to $\overline{\mathbb{Q}}$, obtaining

$$\phi : \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \rightarrow \overline{\mathbb{Q}}^2.$$

The matrix of ϕ in either case is

$$\begin{pmatrix} 1 & \sqrt{2} \\ 1 & \sqrt{2} \end{pmatrix}.$$

And so multiplication by $\sqrt{2}$ in the image becomes

$$\begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$$

In this example, both factors of the tensor product are rings. If M and N are rings as well as A -modules, then $M \otimes_A N$ is also a ring with operation

$$(m \otimes n)(m' \otimes n') = mm' \otimes nn'.$$

Thus, in this case, scalar multiplication defined for extension of scalars is just a special case of the ring multiplication:

$$(b' \otimes 1)(b \otimes m) = bb' \otimes m.$$

In the last example ($B \otimes_{\mathbb{Q}} B$), it is important to distinguish scalar multiplication which looks like

$$a(b \otimes c) = ab \otimes c$$

from the multiplication in the right-hand factor of B , which is a ring, carried up to the scalar extension. For example, multiplication of a times c in B looks like

$$(1 \otimes a)(1 \otimes c) = 1 \otimes ac$$

in the scalar extension. These are the two ways of “multiplying by $\sqrt{2}$ ” which I claimed are confusing in the informal example preceding this section. Now they have different notations.

Now we will describe this in general. Suppose that L/K is a separable extension of degree n with embeddings σ_i , $i = 1, \dots, n$. Define

$$\phi : \overline{K} \otimes_K L \rightarrow \overline{K}^n$$

by

$$\phi(k \otimes l) = k(\sigma_1(l), \dots, \sigma_n(l))$$

The map ϕ travels between two objects which are \overline{K} vector spaces of dimension n and also rings. (Both have the appropriate notion of coordinatewise multiplication.) We wish to show that ϕ is an isomorphism. For this we need...

Proposition 9.1. *The embeddings $\sigma_1, \dots, \sigma_n$ of a separable field extension L/K of degree n are linearly independent.*

Proof. Suppose not. Then

$$\sum_{i=1}^n u_i \sigma_i(l) = 0, \quad \forall l \in L$$

where the u_i are not all 0. We can choose such a relation so that the number of non-zero u_i 's is minimal, say $q \geq 2$. Thus renumbering

$$\sum_{i=1}^q u_i \sigma_i(l) = 0, \quad \forall l \in L.$$

Let l_1, l_2 be elements of L . Then

$$\sum_i u_i \sigma_i(l_1) \sigma_i(l_2) = \sum_i u_i \sigma_i(l_1 l_2) = 0$$

and

$$\sum_i u_i \sigma_1(l_1) \sigma_i(l_2) = \sigma_1(l_1) \sum_i u_i \sigma_i(l_2) = 0$$

Thus,

$$\sum_{i=1}^q u_i (\sigma_1(l_1) - \sigma_i(l_1)) \sigma_i(l_2) = 0$$

But this is a relation of fewer nonzero coefficients in terms of l_2 , so

$$u_i (\sigma_1(l_1) - \sigma_i(l_1)) = 0$$

for all l_1 . Since u_i is nonzero, it is not a zero divisor and $\sigma_1 = \sigma_i$ for all l , a contradiction. \square

In other words, we have shown that the matrix $(\sigma_j(e_i))$, where e_i form a basis for L/K , has trivial kernel. The matrix for ϕ , in terms of the basis $1 \otimes e_i$ for $\overline{K} \otimes_K L$ over \overline{K} , is $(\sigma_i(e_j))$. Hence, the previous proposition shows

Proposition 9.2. *The map ϕ is an isomorphism, both for \overline{K} vector spaces and rings.*

Exercise: show that this is equivalent to ϕ being an isomorphism of \overline{K} algebras.

Multiplication by $\alpha \in L$ is taken to a multiplication by $\phi(1 \otimes \alpha)$ (notationally, $\phi \circ m_{1 \otimes \alpha} \circ \phi^{-1} = m_{\phi(1 \otimes \alpha)}$), which has matrix

$$\begin{pmatrix} \sigma_1(\alpha) & 0 & \cdots & 0 \\ 0 & \sigma_2(\alpha) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(\alpha) \end{pmatrix}.$$

The trace of this matrix is still $Tr_{L/K}(\alpha)$ of course, from which the conjugate formula for trace is immediate (and norm similarly).

In \overline{K}^n , the standard basis is e_i . Multiplication m_{e_i} has trace 1, and the trace pairing in terms of this standard basis has matrix exactly I_n , i.e. it has become the standard inner product pairing. But this means

$$\det(Tr_{L/K}(w_i w_j)) = \det(\sigma_i(w_j))^2 \det(I)$$

which is exactly the discriminant formula we began this section by asking about.

10. THE RING OF INTEGERS INSIDE THE NUMBER FIELD

Suppose that $K \subset L$ is a separable field extension. Then the trace pairing gives a K -linear map

$$L \rightarrow \text{Hom}_K(L, K)$$

which takes $x \in L$ to the map $s_x : y \mapsto Tr_{L/K}(xy)$.

Since the trace pairing is non-degenerate, this is injective. Since L and $\text{Hom}_K(L, K)$ are n -dimensional, this implies it is an isomorphism.

A reminder: the *dual basis* of a basis w_1, \dots, w_n of L over K is the basis

$$\{w_i^\vee : L \rightarrow K\}$$

where

$$w_i^\vee(w_j) = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}.$$

Since the map $L \rightarrow \text{Hom}(L, K)$ is surjective, there exist $z_1, \dots, z_n \in L$ such that $s_{z_i} = w_i^\vee$, i.e. $Tr_{L/K}(w_i z_j) = \delta_{ij}$. Through the identification of z with s_z , we'll call z_1, \dots, z_n the dual basis also.

Theorem 10.1. *Let A be an integrally closed ring, K its field of fractions of characteristic zero, L/K an extension of degree n , and A' the integral closure of A in L . Then A' is an A -submodule of a free A -module of rank n .*

Proof. Let x_1, \dots, x_n be a basis of L/K . By multiplying by some elements of K , the x_i can be taken to be integral over A . (We've seen the argument for this before: we have $a_n x^n + \dots + a_0 = 0$ and multiplying by a_n^{n-1} we get an integral relation for $a_n x$.)

Let $y_1, \dots, y_n \in L$ be a dual basis to x_1, \dots, x_n with respect to the trace pairing.

Now consider $z \in A'$. Then $x_i z \in A'$ also, so $Tr_{L/K}(x_i z) \in A$.

But $z = \sum_{j=1}^n b_j y_j$ for $b_j \in K$, so

$$Tr_{L/K}(x_i z) = Tr \left(x_i \sum b_j y_j \right) = \sum b_j Tr(x_i y_j) = b_i.$$

Hence $b_i \in A$, so $z \in Ay_1 + \dots + Ay_n$, a free A -module of rank n . \square

Corollary 10.2. *If A is a PID, then A' as above is a free A -module of rank n .*

Proof. We use the fact that any submodule of a free module is free for modules over a PID. (For this, see Samuel §1.5, Thm 1, p. 21, or Artin Chapter 12, especially §6. It is a generalisation of the Smith Normal Form you studied on your first homework (there $A = \mathbb{Z}$ is the PID).)

The rank of a free submodule of a free module (over a PID) is $\leq n$. But $y_1, \dots, y_n \in A$ is a basis for L/K , so the elements are independent, i.e. rank $\geq n$. So A' is of rank n . \square

In particular, we obtain the following.

Theorem 10.3. *Let K be a number field of degree n . Then \mathcal{O}_K is a lattice in K , i.e. $\mathbb{Q}\mathcal{O}_K = K$ and \mathcal{O}_K is a free \mathbb{Z} -module of rank n .*

Definition 10.4. *A basis for \mathcal{O}_K over \mathbb{Z} is called an integral basis.*

We have just seen that every number field of degree n has an integral basis of n elements. Note that all integral bases for a number field have the same discriminant.

Definition 10.5. *An order R in \mathcal{O}_K is a subring such that $[\mathcal{O}_K : R]$ is finite. (Where $[\mathcal{O}_K : R] = |\mathcal{O}_K/R|$ as abelian groups.)*

Example 10.6. (1) $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z} + \mathbb{Z} \left(\frac{1+\sqrt{5}}{2} \right)$ and $\mathbb{Z} + \mathbb{Z}\sqrt{5}$ is an order in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, but \mathbb{Z} is not an order, since the index is not finite. Also $\mathbb{Z}2 + \mathbb{Z}\sqrt{5}$ is not an order since for us rings contain 1.

(2) $\left\{ 1, \frac{1+\sqrt{5}}{2} \right\}$ is an integral basis for $\mathbb{Q}(\sqrt{5})$. But $\{1, \sqrt{5}\}$ is not, because the algebraic integer $\frac{1+\sqrt{5}}{2}$ cannot be expressed in terms of that basis with \mathbb{Z} coefficients.

Example 10.7. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^3 + \alpha - 1 = 0$. Consider the basis $1, \alpha, \alpha^2$. We can calculate the trace pairing if we know the trace of the powers of α . First we calculate

$$\begin{aligned}\alpha^3 &= -\alpha + 1 \\ \alpha^4 &= -\alpha^2 + \alpha \\ \alpha^5 &= \alpha^2 + \alpha - 1 \\ \alpha^6 &= \alpha^2 - 2\alpha + 1\end{aligned}$$

And then using these results

$$\begin{aligned}Tr(\alpha) &= 0 \\ Tr(\alpha^2) &= Tr \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} = -2 \\ Tr(\alpha^3) &= Tr \begin{pmatrix} -1 & 1 & 1 \\ 0 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix} = 3 \\ Tr(\alpha^4) &= Tr \begin{pmatrix} 0 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix} = 2\end{aligned}$$

Thus

$$\text{disc}(1, \alpha, \alpha^2) = \det \begin{pmatrix} 1 & 0 & -2 \\ 0 & -2 & 3 \\ -2 & 3 & 2 \end{pmatrix} = -31$$

Now since this result is squarefree, $1, \alpha, \alpha^2$ is an integral basis. For, if not, then $1, \alpha, \alpha^2$ can be expressed, with integer coefficients, in terms of an integral basis e_1, e_2, e_3 . That is, the coefficients form a matrix (a_{ij}) of integer non-unit determinant. And in that case $\text{disc}(1, \alpha, \alpha^2) = \det(a_{ij})^2 \text{disc}(e_1, e_2, e_3)$.

11. SOME COMPUTATIONAL ASPECTS OF DISCRIMINANTS

We begin with a very useful object:

Definition 11.1. *The resultant of polynomials*

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

$$g(x) = d \prod_{i=1}^m (x - \beta_i)$$

is

$$\text{Res}(f, g) = c^m d^n \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (\alpha_i - \beta_j).$$

Proposition 11.2. *Suppose that*

$$f = a_n x^n + \dots + a_0$$

$$g = b_m x^m + \dots + b_0$$

Then

$$\text{Res}(f, g) = \det \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & \dots & a_1 & a_0 & 0 & \dots & 0 \\ & & & \ddots & & & & \\ 0 & \dots & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ & & & & \ddots & & & & \\ 0 & 0 & \dots & 0 & 0 & b_m & b_{m-1} & \dots & b_0 \end{pmatrix}.$$

This $(m + n) \times (m + n)$ matrix is called the Sylvester matrix.

Proof. If $\text{gcd}(f, g) \neq 1$, then they share a root θ and $\text{Res}(f, g) = 0$. Then the Sylvester matrix has the vector $(\theta^{n+m}, \dots, \theta, 1)$ in its kernel, so it has zero determinant.

Thus we may assume $\text{gcd}(f, g) = 1$. Let $R = \text{Res}(f, g)$ and let D be the determinant of the Sylvester matrix.

Although it is not entirely necessary to the proof, it is informative to consider the map

$$\mathbb{Q}[x]/\langle g(x) \rangle \times \mathbb{Q}[x]/\langle f(x) \rangle \rightarrow \mathbb{Q}[x]/\langle f(x)g(x) \rangle$$

given by $(r(x), s(x)) \mapsto f(x)r(x) + g(x)s(x)$ has as its matrix the transpose of Sylvester's (convince yourself of this, using an appropriate ordering of the basis of powers of x). Since $\text{gcd}(f, g) = 1$, the map is a surjective ring homomorphism. By comparing dimensions as \mathbb{Q} -vector spaces, we see it is actually an isomorphism. Thus both R and D are non-zero.

Now, a series of facts about R and D :

- (1) $R, D \in \mathbb{Q}[a_m, b_m, \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m]$. For R , this is clear from the formula. For D , this occurs because the $a_i/a_n, b_i/b_m$ are symmetric functions in the roots α_i and β_i respectively.
- (2) As such, $R \mid D$. This is because R has no repeated linear factors, and whenever $R = 0$, then $D = 0$.
- (3) $R, D \in \mathbb{Q}[a_1, \dots, a_n, b_1, \dots, b_m]$. For D , this is clear. For R , this follows from the formula

$$R = (-1)^{mn} b_m^n \prod_{i=1}^m f(\beta_i) = a_n^m \prod_{i=1}^n g(\alpha_i).$$

For, consider the expression $\prod_{i=1}^m f(\beta_i)$: it is symmetric in the β_i 's, so it's a function of the symmetric functions on β_i , i.e. the b_i/b_m , and is of degree not more than n in these symmetric functions (the degree of f), with coefficients in a_i 's.

- (4) As such, R and D are homogeneous of degree m in the a_i 's and n in the b_i 's. For D this follows from the determinant formula. For R it follows from the previous point.
- (5) R and D have the form $a_n^m b_0^n + (\text{other monomials})$. For D , this follows from the formula for determinant ($a_n^m b_0^n$ is the product of the diagonal entries). For R , this is from point (3) above.

Taking all these together, we see that $R = D$ (since $R \mid D$ and they are both homogeneous of the same degree and the coefficient of at least one of their monomials agrees). \square

Proposition 11.3 (Vandermonde Determinant).

$$\det \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Proof. Exercise. \square

Consequently,

$$\begin{aligned}
 \text{disc}(1, x, \dots, x^{n-1}) &= \det(\sigma_i(x^j))^2 \\
 &= \det(x_i^j)^2 && x_i \text{ conjugates of } x \\
 &= \left(\prod_{i < j} (x_j - x_i) \right)^2 && \text{Vandermonde} \\
 &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n \prod_{\substack{j=1 \\ i \neq j}}^n (x_i - x_j) \\
 &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(x_i) && f = m_{\mathbb{Q},x} \\
 &= \begin{cases} (-1)^{\frac{n(n-1)}{2}} \text{Res}(f, f') & \text{fmula of Res pf} \\ (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(x)) & f'(x_i) \text{ conj's } f'(x) \end{cases}
 \end{aligned}$$

These formulæ are very useful for computation.

Example 11.4. Let $K = \mathbb{Q}(\alpha)$, $f(\alpha) = \alpha^2 + a\alpha + b = 0$. Then $m_{2\alpha+a}$ has matrix

$$\begin{pmatrix} a & -2b \\ 2 & -a \end{pmatrix}$$

and so

$$\text{disc}(1, \alpha) = (-1)N_{K/\mathbb{Q}}(2\alpha + a) = -a^2 + 4b = a^2 - 4b.$$

Alternatively, we might calculate

$$\begin{aligned}
 \text{disc}(1, \alpha) &= (-1)R(f, f') \\
 &= -\det \begin{pmatrix} 1 & a & b \\ 2 & a & 0 \\ 0 & 2 & a \end{pmatrix} \\
 &= -[a^2 - 2(a^2 - 2b)] = a^2 - 4b.
 \end{aligned}$$

The quantity $a^2 - 4b$ is the ‘discriminant’ of a quadratic polynomial. Discriminants of polynomials can be defined generally (but we won’t). When f is monic and irreducible of degree n with root α , we have

$$\text{disc}(f) = \text{disc}(\alpha) = \text{disc}(1, \alpha, \dots, \alpha^{n-1}).$$

Definition 11.5. A field whose ring of integers has a basis of the form $1, \alpha, \dots, \alpha^n$ (a power basis) is called monogenic.

Example 11.6. *An example due to Dedekind. Let $K = \mathbb{Q}(\alpha)$, where α satisfies the irreducible polynomial $f(x) = x^3 + x^2 - 2x + 8 = 0$ (to see that this is irreducible, note that any rational solution must be an integer dividing 8 and so it has no linear factors). Note that $f'(x) = 3x^2 + 2x - 2$, and so we may calculate the discriminant by a resultant:*

$$\begin{aligned} \text{disc}(1, \alpha, \alpha^2) &= (-1)^{\frac{3(3-1)}{2}} R(f, f') \\ &= -\det \begin{pmatrix} 1 & 1 & -2 & 8 & 0 \\ 0 & 1 & 1 & -2 & 8 \\ 3 & 2 & -2 & 0 & 0 \\ 0 & 3 & 2 & -2 & 0 \\ 0 & 0 & 3 & 2 & -2 \end{pmatrix} \\ &= -4 \cdot 503 \end{aligned}$$

Since 503 is prime, the discriminant of K is either $-4 \cdot 503$ or -503 . In fact, $\beta = \frac{\alpha^2 + \alpha}{2}$ satisfies the equation

$$\beta^3 - 3\beta^2 - 10\beta - 8 = 0$$

So β is algebraic but not in the \mathbb{Z} -span of $1, \alpha, \alpha^2$. Hence $1, \alpha, \alpha^2$ is not an integral basis. Therefore

$$\text{disc}(K) = -503 = \text{disc}(1, \alpha, \beta).$$

However, perhaps there is another power basis $1, \gamma, \gamma^2$ for \mathcal{O}_K ?

Write $\gamma = a + b\alpha + c\beta$. Then $\gamma^2 = A + B\alpha + C\beta$ where

$$A = a^2 - 2c^2 - 8bc$$

$$B = -2c^2 + 2ab + 2bc - b^2$$

$$C = 2b^2 + 2ac + c^2$$

Then

$$\text{disc}(1, \gamma, \gamma^2) = \det \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A & B & C \end{pmatrix}^2 \text{disc}(1, \alpha, \beta)$$

We will now show that the determinant above is even, which means $1, \gamma, \gamma^2$ cannot be an integral basis. We calculate

$$\begin{aligned} \det &= bC - cB = 2b^3 + 2abc + c^2b + 2c^3 - 2abc - 2bc^2 + b^2c \\ &= 2b^3 + 2c^3 - bc^2 + b^2c \\ &\equiv b^2c - bc^2 \equiv bc(b - c) \equiv 0 \pmod{2}. \end{aligned}$$

12. CYCLOTOMIC FIELDS

Some basic facts about cyclotomic fields (this should be review?).

Let $n \geq 1$. Let $K = \mathbb{Q}(\zeta_n)$ where $\zeta_n = e^{2\pi i/n}$, that is to say, ζ_n is a primitive n -th root of unity. The term *primitive* here means that ζ_n has order *exactly* n , not just dividing n . The conjugates of ζ_n are all other primitive n -th roots of unity. These are exactly ζ_n^i where $\gcd(i, n) = 1$. There are $\phi(n)$ such conjugates, and the minimal polynomial for ζ_n has these as roots. It is

$$\Phi_n(x) = \prod_{\substack{j=1 \\ \gcd(j,n)=1}}^n (x - \zeta_n^j)$$

of degree $\phi(n)$. This is called the *n-th cyclotomic polynomial* and it is irreducible over \mathbb{Q} . We have the following useful facts:

$$\Phi_n(x) \mid (x^n - 1), \quad x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

The embeddings of K are

$$\sigma_j : \zeta_n \mapsto \zeta_n^j$$

for all j relatively prime to n . Since these all take K to itself fixing \mathbb{Q} , we see that in fact K is Galois over \mathbb{Q} . The order of the Galois group is the degree of the extension:

$$|\text{Gal}(K/\mathbb{Q})| = \phi(n)$$

And in fact, one can see that the Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. To see this, simply check that the map $\lambda : \text{Gal}(K/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ given by $\lambda(\sigma_j) = j + n\mathbb{Z}$ is a homomorphism and a bijection.

Proposition 12.1.

$$\text{disc}(\zeta_n) \mid n^{\phi(n)},$$

and for p an odd prime,

$$\text{disc}(\zeta_p) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Proof. We know that

$$x^n - 1 = \Phi_n(x)g(x)$$

for some $g(x) \in \mathbb{Q}[x]$. So

$$nx^{n-1} = \Phi'_n(x)g(x) + \Phi_n(x)g'(x)$$

Let $x = \zeta_n$, so we obtain

$$n\zeta_n^{n-1} = \Phi'_n(\zeta_n)g(\zeta_n)$$

Taking the norm, from $K = \mathbb{Q}(\zeta_n)$ down to \mathbb{Q} , we get

$$N_{K/\mathbb{Q}}(n)N_{K/\mathbb{Q}}(\zeta_n^{n-1}) = N_{K/\mathbb{Q}}(\Phi'_n(\zeta_n))N_{K/\mathbb{Q}}(g(\zeta_n))$$

Now, of these four norms in order: the first is n raised to the degree of the extension; the second is the norm of a unit, hence ± 1 ; the third is the discriminant of ζ_n up to sign and the fourth is an integer. Hence

$$n^{\phi(n)} = \pm \text{disc}(1, \zeta_n, \dots, \zeta_n^{\phi(n)-1})k$$

for some $k \in \mathbb{Q}$.

For the second statement (recall that we've already proven this, but here we use a different method), we have $\phi(p) = p-1$ and $g(x) = x-1$. Using the equations above, then, we have

$$p = \zeta_p \Phi'_p(\zeta_p)(\zeta_p - 1)$$

Now we will take the norm. Again there are four factors which we norm separately: the first is in \mathbb{Z} so it is raised to the degree of the extension; the second and fourth are well known by now; and the third is related to the discriminant by a formula from earlier today. So we get

$$p^{p-1} = (-1)(-1)^{\frac{(p-1)(p-2)}{2}} \text{disc}(\zeta_p)(-p)$$

and the required formula follows. \square

Proposition 12.2. *The ring of integers of $K = \mathbb{Q}(\zeta_p)$ for p prime is $\mathbb{Z}[\zeta_p]$.*

Proof. For $p = 2$, this is immediate, so we may assume that p is odd. Consider the element

$$x = a_0 + a_1\zeta_p + \dots + a_{p-2}\zeta_p^{p-2} \in \mathcal{O}_K.$$

Then

$$x(1 - \zeta_p) = a_0(1 - \zeta_p) + a_1(\zeta_p - \zeta_p^2) + \dots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}) \in \mathcal{O}_K.$$

Taking the trace from K down to \mathbb{Q} gives

$$\text{Tr}_{K/\mathbb{Q}}(x(1 - \zeta_p)) = a_0p + a_1(0) + \dots + a_{p-2}(0) = a_0p.$$

Now from homework, we know $\text{Tr}(x(1 - \zeta_p)) \in p\mathbb{Z}$. So $a_0p \in p\mathbb{Z}$ implies that $a_0 \in \mathbb{Z}$ (since it is rational and an algebraic integer). Now $\zeta_p^{-1} = \zeta_p^{p-1} \in \mathcal{O}_K$ and so

$$(x - a_0)\zeta_p^{-1} = a_1 + a_2\zeta_p + \dots + a_{p-2}\zeta_p^{p-3} \in \mathcal{O}_K.$$

Repeating the same argument above (taking the Trace) we obtain $a_1 \in \mathbb{Z}$. Repeating, we get $a_i \in \mathbb{Z}$ for all i . \square

A remark relating to the proof. Set the notation

$$e_i = \zeta_p^i, \quad f_i = 1 - \zeta_p^{-i}$$

for $i = 1, \dots, p - 1$. Then

$$\text{Tr}(e_i f_j) = \text{Tr}(\zeta_p^i - \zeta_p^{j-i}) = \begin{cases} -p & i = j \\ 0 & \text{otherwise} \end{cases}$$

So

$$\frac{1 - \zeta_p^{-i}}{p}$$

is a dual basis to ζ_p^i . Consequently, for all $\alpha \in \mathbb{Z}[\zeta_p]$,

$$\text{Tr} \left(\alpha \left(\frac{1 - \zeta_p^{-i}}{p} \right) \right) \in \mathbb{Z}.$$

In the proof, we actually use the fact that this holds for all $\alpha \in \mathcal{O}_K$ to find \mathcal{O}_K .

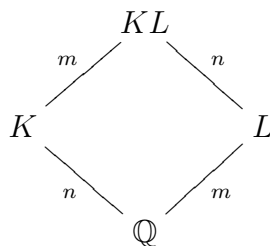
This motivates us to consider the *dual* of an order \mathcal{O} in a number field K , which is

$$\mathcal{O}^\vee = \{z \in K : \text{Tr}(\alpha z) \in \mathbb{Z} \forall \alpha \in \mathcal{O}\}.$$

In essence, the proof says that the dual of $\mathbb{Z}[\zeta_p]$ and \mathcal{O}_K are the same, so they themselves must be the same.

Theorem 12.3. *Let K and L be number fields of degree n and m respectively. Let KL have degree nm and let d be the greatest common divisor of $\text{disc}(K)$ and $\text{disc}(L)$. Then $\mathcal{O}_{KL} \subset \frac{1}{d} \mathcal{O}_K \mathcal{O}_L$.*

Proof. Here's the picture:



Let $\alpha_1, \dots, \alpha_n$ be an integral basis for K and β_1, \dots, β_m an integral basis for L . Then the $\alpha_i \beta_j$ form a basis for $\mathcal{O}_K \mathcal{O}_L$ (and KL). Why? Because the $\alpha_i \beta_j$ certainly span KL , and the dimension is correct, so they are independent. They also span $\mathcal{O}_K \mathcal{O}_L$ and must still be independent in this \mathbb{Z} -module, so they form a basis there also. (In particular, the rank of $\mathcal{O}_K \mathcal{O}_L$ is equal to the dimension of KL .)

Let $\gamma \in \mathcal{O}_{KL}$. Then

$$\gamma = \sum_{i,j} \frac{m_{ij}}{r} \alpha_i \beta_j$$

where $m_{ij}, r \in \mathbb{Z}$ and $\gcd(r, \gcd(m_{ij})) = 1$.

We wish to show that $r \mid d$. To do so, we show that $r \mid \text{disc}(K)$ and $r \mid \text{disc}(L)$.

Now let σ_i for $i = 1, \dots, n$ be the embeddings of K and extend these to $\bar{\sigma}_i$ embeddings of KL which restrict to the identity on L :

$$\bar{\sigma}_i|_L = id.$$

This is possible since the m embeddings of KL/K restrict to the m embeddings of L/\mathbb{Q} . Note that the m distinct extensions of one σ_i are distinct on KL but agree on K so they must be distinct on L . This means the correspondence is injective and hence bijective.

Now, using the map $\phi : \bar{\mathbb{Q}} \otimes_K KL \rightarrow \bar{\mathbb{Q}}^m$ given by $\phi(x) = (\sigma_i(x))$, we can write

$$\phi(\gamma) = (\sigma_i(\alpha_j))(x_i), \quad x_i = \sum_j \frac{m_{ij}}{r} \beta_j.$$

The coordinates of $\phi(\gamma)$ are algebraic integers, as are the entries in the matrix $(\sigma_i(\alpha_j))$. Thus the adjugate of the matrix has entries algebraic integers and so all the

$$\det(\sigma_i(\alpha_j))x_i$$

are algebraic integers, and therefore so are all the $\text{disc}(K)x_i$.

So we have

$$\text{disc}(K)x_i = \sum_j \frac{\text{disc}(K)m_{ij}}{r} \beta_j \in \mathcal{O}_L$$

which implies that all the coefficients of the β_j are rational integers. But since $\gcd(r, \gcd(m_{ij})) = 1$, this implies that $r \mid \text{disc}(K)$.

Symmetrically, $r \mid \text{disc}(L)$. So $r \mid d$. \square

13. NOETHERIAN MODULES AND NOETHERIAN RINGS

Definition 13.1. *Let R be a ring. An R -module M is Noetherian if every submodule of M is finitely generated.*

A ring R is Noetherian if it is a Noetherian R -module.

An R -module M satisfies the ascending chain condition if every sequence

$$M_1 \subset M_2 \subset \dots \subset M_n \subset \dots$$

of submodules is eventually constant (aka ‘stabilizes’ or ‘is stationary’) i.e. there exists $k \in \mathbb{Z}$ such that $M_i = M_j$ for all $i, j \geq k$.

Note that the R -submodules of a ring R a module over itself are exactly the ideals of R .

Theorem 13.2. *Let M be an R -module. The following are equivalent:*

- (1) M is Noetherian
- (2) M satisfies the ascending chain condition
- (3) Every nonempty set of submodules of M contains a maximal element (an element not strictly contained in another element of the set)

Proof. 1 \implies 2: Consider an ascending chain of submodules

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

Define $N = \cup_{i=1}^{\infty} M_i$. Then N is a submodule, so it is finitely generated by n_1, \dots, n_k . Each n_j is in some $M_{f(j)}$. Take $N = \max_{j=1, \dots, k} f(j)$. Then $n_i \in M_N$ for all $i = 1, \dots, k$. So $N \subset M_N$. Thus the chain stabilizes.

2 \implies 3: *Axiom of Choice Alert*¹ Assume that 3) fails. Let S be a nonempty set of submodules of M such that for all $N \in S$, there exists $N' \in S$ with $N' \supsetneq N$. Then choose any $N_1 \in S$ and choose $N_{i+1} \supsetneq N_i$ in S for each i . Then

$$N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \dots$$

so 2) fails.

3 \implies 1: Suppose that 1) fails. Let N be a submodule of M which is not finitely generated. Let S be the set of all finitely generated submodules of N . It contains (0) , so it is nonempty. If $L \in S$ then $L \neq N$ so there exists $a \in N, a \notin L$. Let $L' = L + aR \subset N$. This is a strictly larger element of S so 3) fails.

□

Examples of Noetherian rings are the integers (every ideal is finitely generated) and for the same reason any principal ideal domain.

Proposition 13.3. *Let A be a ring, M an A -module and $M' \subset M$ a submodule. Then M is Noetherian if and only if M' and M/M' are.*

¹The Axiom of Choice is used to make infinitely many choices of a member of a set. It is not needed for finitely many choices, nor is it needed if you can describe the function which determines the choice in general. But making arbitrary choices is... *suspicious*, shall we say. It leads to many interesting paradoxes, the most famous of which is the Banach-Tarski paradox wherein you can cut up one unit ball in \mathbb{R}^3 into finitely many pieces, translate and rotate those and end up with two identical disjoint unit balls.

(The picture in mind is the exact sequence

$$0 \rightarrow M' \rightarrow M \rightarrow M/M' \rightarrow 0.)$$

Proof. First, assume that M is Noetherian. Then the set of submodules of M' and the set of submodules of M contained in M' are both partially ordered sets, and as such are isomorphic (are in bijection preserving ordering). Similarly, the set of submodules of M/M' is in bijection with the set of submodules of M containing M' in such a way that order is preserved. For this latter case, the bijection in one direction is the quotient by M' and in the other is the map $N \mapsto N + M'$. So using either criterion 2 or 3 from the previous theorem, M' and M/M' are Noetherian.

Now, assume instead that M' and M/M' are Noetherian. Let

$$N_1 \subset N_2 \subset \dots$$

be an ascending chain of submodules of M . We wish to show that it stabilizes.

Consider the chain

$$N_0 \cap M' \subset N_1 \cap M' \subset \dots$$

in M' which must stabilize at some n_0 . Consider also the chain

$$(N_0 + M')/M' \subset (N_1 + M')/M' \subset \dots$$

in M/M' which must stabilize at some n_1 . Let $N = \sup(n_0, n_1)$.

Now suppose $n > N$. Then by definition $N_n \subset N_{n+1}$. Now we will show that $N_{n+1} \subset N_n$. Let $x \in N_{n+1}$. Now $(N_{n+1} + M')/M' = (N_n + M')/M'$ and so $N_{n+1} + M' = N_n + M'$. So there exists $y \in N_n$ and $z, z' \in M'$ such that

$$x + z = y + z'$$

which implies that $x - y = z' - z \in N_{n+1} \cap M' = N_n \cap M' \subset N_n$. Thus $x \in N_n$ and the chain N_i stabilizes. \square

Corollary 13.4. *Let A be a ring, and M_1, \dots, M_n Noetherian A -modules. Then $\prod_{i=1}^n M_i$ is Noetherian.*

Proof. Induct on n , using the exact sequence

$$0 \rightarrow M_1 \times \dots \times M_{n-1} \rightarrow M_1 \times \dots \times M_n \rightarrow M_n \rightarrow 0.$$

\square

Corollary 13.5. *Let A be a Noetherian ring. Let M be a finitely generated A -module. Then M is a Noetherian A -module.*

Proof. $M \cong A^n/N$ where n is the number of generators of M and the bottom is a submodule of A^n . By the previous corollary, since A^n is Noetherian, so is M . \square

Proposition 13.6. *Suppose that A is a Noetherian integrally closed ring with field of fractions K of characteristic zero. Let L/K be an extension of degree n , and let A' be the integral closure of A in L . Then A' is a finitely generated A -module and a Noetherian ring.*

Proof. From a previous theorem, A' is a submodule of a free A -module of rank n . By the last corollary and its theorem, the latter is Noetherian, so the former is finitely generated and a Noetherian A -module. We wish to show that it is a Noetherian A' -module. But the A' -submodules of A' are also A -submodules of A' : in fact, they form a sub-poset. So by the poset conditions for Noetherian-ness, A' is a Noetherian ring. \square

Corollary 13.7. *The ring of integers of a number field is Noetherian.*

Proof. In the foregoing, use $A = \mathbb{Z}$, $K = \mathbb{Q}$, let L be a number field and A' will be its ring of integers. We find that \mathcal{O}_L is a finitely generated \mathbb{Z} -module (this was already shown previously) and a Noetherian ring. \square

14. IDEALS

Some reminders of ideal properties.

An ideal is *prime* if the ring modulo the ideal is an integral domain. An ideal is *maximal* if the ring modulo the ideal is a field. Since fields are integral domains, all maximal ideals are prime. The converse doesn't hold: for example, (0) is prime in \mathbb{Z} but not maximal.

Suppose that $f : A \rightarrow B$ is a ring homomorphism. Then we can *extend* an ideal $I \subset A$ to obtain the ideal in B generated by the image of I . We can also *contract* an ideal $J \subset B$ to obtain the ideal $f^{-1}(J)$ in A . Contraction preserves primality since

$$A \rightarrow B \rightarrow B/J$$

is a ring homomorphism whose image is an integral domain, and having kernel $f^{-1}(J)$ in A and J in B .

Extension does not in general preserve primality. Of particular importance is the case where f is an injection (where contraction of an ideal J is just restriction $J \cap A$), so we will draw an example from there.

Consider $\mathbb{Z} \rightarrow \mathbb{Z}[i]$. Let (p) be a prime of \mathbb{Z} . Then the ideal $p\mathbb{Z}[i]$ may or may not be prime. In fact, if $p = x^2 + y^2$, where $x, y \in \mathbb{Z}$, then $p = (x + iy)(x - iy)$; however, neither $x + iy$ nor $x - iy$ is in $p\mathbb{Z}[i]$.

There is also a product of ideals: IJ is the ideal generated by all products ij of $i \in I, j \in J$ (i.e. consists of all finite sums of such

products). This operation is commutative and associative on ideals, and the ring A itself plays the role of identity element. Thus the ideals form a monoid. Recall from your homework that $IJ \subseteq I \cap J$ but it only equal when $I + J = A$.

If $P \subset A$ is a prime ideal, and P contains a product of of ideals $\prod_{i=1}^n A_i$, then P contains at least one of the A_i . For, otherwise, take $a_i \in A_i$ not in p and the product $\prod_{i=1}^n a_i$ could not therefore be in P .

Proposition 14.1. *If A is a Noetherian integral domain, and I is a nonzero ideal, then I contains a product of non-zero prime ideals.*

Proof. Let S be the set of non-zero ideals failing the conclusion of the theorem. Then, since A is Noetherian, S contains a maximal element I_0 . It cannot be itself prime. So we may choose $x_1, x_2 \in A \setminus I_0$ such that $x_1 x_2 \in I_0$. Then let $I_i = I_0 + Ax_i$ for $i = 1, 2$. The $I_i \notin S$ since they strictly contain I_0 . Thus, $I_i \supseteq \prod_j P_{i,j}$ where the $P_{i,j}$ are prime. But $I_0 \supseteq I_1 I_2 \supseteq \prod_{i,j} P_{i,j}$, a contradiction. \square

Definition 14.2. *Let A be an integral domain with field of fractions K . Then an A -submodule I of K is a fractional ideal if there exists some $d \neq 0$ such that $dI \subset A$.*

Example 14.3. (1) *Ordinary ideals are fractional ideals ($d = 1$).*

(2) *If A is Noetherian, then the fractional ideals are exactly the finitely generated A -submodules of K . For, on the one hand, $I \subset d^{-1}A \cong A$ and so I is finitely generated; on the other hand, if I is generated by x_i , $i = 1, \dots, n$, then one can always choose a $d \neq 0$ such that $dx_i \in A$.*

(3) *Suppose that $A = \mathbb{Z}$. Then we need only consider the finitely generated \mathbb{Z} modules of \mathbb{Q} . If I is generated by p_i/q_i for $i = 1, \dots, n$, then I is generated by g/l where $g = \gcd p_i$ and $l = \text{lcm } q_i$.*

Just as for ideals, we may define the product IJ . In fact, if I and J are fractional ideals witnessed by ‘denominators’ d and d' respectively, then $I \cap J$, $I + J$ and IJ are fractional ideals, where dd' suffices in each case.

The product of fractional ideals is again commutative, associative and A is the identity. Therefore it is a monoid containing the regular or ‘integral’ ideals as a submonoid.

The next question we turn to is: in what rings is this monoid actually a group?

15. DEDEKIND DOMAINS

Definition 15.1. *A Dedekind domain is a ring A such that*

- (1) A is an integral domain
- (2) A is integrally closed
- (3) A is Noetherian
- (4) every non-zero prime ideal in A is maximal

Theorem 15.2. *Every principal ideal domain is a Dedekind domain.*

Proof. Let A be a principal ideal domain. By definition, A is an integral domain, and since its ideals are finitely generated, it is Noetherian.

To show that every non-zero prime ideal is maximal, consider a prime (p) strictly contained in another ideal (m) . Then $m \mid p$ so there exists a k with $mk = p$. However, $m \notin (p)$ so $k \in (p)$, which means that $k = pu$ for some u . Hence $mk = pu = k$ and since cancellation holds in an integral domain, we obtain $mu = 1$. Thus $(m) = (1)$.

It remains to show that A is integrally closed. Let $x \in K$, the field of fractions of A . First we show a small lemma: for a principal ideal domain, we can write $x = a/b$ where $a, b \in A$ and are relatively prime (i.e. $(a) + (b) = (1)$). The proof of this is as follows. Define the A -ideal $(b) = \{y \in A : xy \in A\}$. Let $a = bx$. Now let $(g) = (a) + (b)$. I wish to claim that g is a unit. Let k be an element of A . If $ak = b x k$ is in (b) then kx is in A (cancellation since it's a domain), so by definition, $k \in (b)$. Let $k = b/g$. This is in A since $g \mid b$. But $ak = ab/g \in (b)$ since $g \mid a$. So by the argument above, $k \in (b)$. That is, $b/g \in (b)$. So $b \in (bg)$, i.e. g is a unit.

Thus, we may so express $x = a/b$. If x is integral over A , with equation

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$$

then we may substitute and multiply by b^n , obtaining

$$a^n + b(a_{n-1}a^{n-1} + \dots + a_0b^{n-1}) = 0$$

from which we deduce that $b \mid a^n$. But then $b \mid a$ (for $ax + by = 1$ for some x and y since a and b are relatively prime, so $a^n x + ba^{n-1}y = a^{n-1}$ is divisible by b , and we repeat until we find that a is divisible by b). But then $(b) = (a) + (b) = (1)$, so b is a unit and $x \in A$. □

Proposition 15.3. *Suppose that $A \subset B$ are integral domains and B is integral over A . Then B is a field if and only if A is a field.*

Proof. First, suppose that A is a field. Let $b \in B$ be non-zero. Then b is integral over A so $V = A[b]$ is a finite dimensional vector space over A . Multiplication by b is an A -linear transformation from V to itself. Since B is an integral domain, it is injective, hence surjective. To there exists some b' with $bb' = 1$.

Conversely, suppose that B is a field. Let $a \in A$ be non-zero. Then a^{-1} exists in B and we are required to show it is in A . But it is integral over A , so

$$a^{-n} + a_{n-1}a^{-n+1} + \dots + a_1a^{-1} + a_0 = 0$$

and so

$$a^{-1} = -(a_{n-1} + \dots + a_1a^{n-2} + a_0a^{n-1}) \in A.$$

□

Theorem 15.4. *Let A be a Dedekind domain with field of fractions K of characteristic zero. Let L be a field extension of finite degree over K and let A' be an integral closure of A in L . Then A' is a Dedekind domain.*

Proof. We already showed that A' is Noetherian previously. It is known to be an integrally closed integral domain. Let P be a non-zero prime of A' . Take $0 \neq x \in P$. Then x is integral over A , so we have

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$$

where $a_i \in A$, taken to have minimal degree among such equations of integral dependence. In particular, $a_0 \neq 0$. So $a_0 \in A'x \cap A \subset P \cap A$, which means that $P \cap A$ is non-zero. Since it is prime (restriction of a prime), it is maximal (A is a Dedekind domain), and so $A/(P \cap A)$ is a field. But $A/(P \cap A)$ is identified with a subring of A'/P , and this containment is an integral extension since A'/A is an integral extension. So A'/P is a field by the previous proposition. □

We have now shown

Theorem 15.5. *The ring of integers of a number field is a Dedekind domain.*

16. IDEALS IN DEDEKIND DOMAINS

Let's begin with an illustrative example. Consider the ring $\mathbb{Z}[\sqrt{10}]$ of integers of $\mathbb{Q}(\sqrt{10})$. In this ring,

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

The corresponding equation of norms of these elements is:

$$36 = 4 \cdot 9 = 6 \cdot 6.$$

We can observe that $a^2 - 10b^2 = 2$ and $a^2 - 10b^2 = 3$ have no solutions since 2 and 3 are not squares modulo 5. So there are no elements of norm 2 or 3 in the ring of integers. So there is no “further reduction” of this equation that will allow us to restore unique factorisation: $\mathbb{Z}[\sqrt{10}]$ is not a UFD.

However, we have the following equation of ideals:

$$(6) = (2, \sqrt{10})^2(3, 1 + \sqrt{10})(3, 1 - \sqrt{10}).$$

(To verify this involves checking a finite number of facts, such as these:

$$3 = 3 \cdot 3 - (4 + \sqrt{10})(4 - \sqrt{10}) \in (3, 1 + \sqrt{10})(3, 1 - \sqrt{10})$$

$$2 = \sqrt{10} \cdot \sqrt{10} - 2(2 \cdot 2) \in (2, \sqrt{10})^2.)$$

Each of the primes in the right-hand expression is prime. To see this, consider the quotient ring. For example,

$$\begin{aligned} \mathbb{Z}[\sqrt{10}]/(2, 1 + \sqrt{10}) &\cong \mathbb{Z}[x]/(2, x^2 - 10, x + 1) \\ &= (\mathbb{Z}/3\mathbb{Z})[x]/(x^2 - 1, x + 1) \\ &= (\mathbb{Z}/3\mathbb{Z})[x]/(x + 1) \\ &\cong \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

which is a field.

I claim that this expression as a product of prime ideals is unique (up to reordering). To see this, it is convenient to define the norm $N(I)$ of an ideal I to be the size $|A/I|$.

Then $N(6) = |\mathbb{Z}[\sqrt{10}]/(6)| = |(\mathbb{Z}/6\mathbb{Z})[x]/(x^2 - 4)| = 36$. Similarly, $N(2, \sqrt{10}) = 2$ and $N(3, 1 \pm \sqrt{10}) = 3$.

Now, if I and J are coprime ideals, then

$$R/IJ \cong R/I \times R/J$$

by the Chinese Remainder Theorem, so this norm is multiplicative on coprime ideals (actually we will see later it is multiplicative in general, but this requires more than CRT).

Now, prime ideals are maximal and hence coprime. Also $N(I) = 1$ if and only if $I = (1)$.

At this point we are almost convinced. The only remaining possibility is that there are prime ideals of Norm 4 and 9 whose product is (6)? After all, there do exist fields of these orders. If that were so, then

$$\mathbb{Z}[\sqrt{10}]/(6) \cong \mathbb{Z}[\sqrt{10}]/P_1 \times \mathbb{Z}[\sqrt{10}]/P_2 \cong \mathbb{F}_4 \times \mathbb{F}_9$$

But the left-hand ring has an element (2) of multiplicative order 5, which the right-hand ring does not. So this is not possible.

We will now show two main results: that the monoid of fractional ideals is a group, and that (fractional) ideals in Dedekind domains have unique factorisation into primes.

Theorem 16.1. *Let A be a Dedekind domain which is not a field. Then every maximal ideal of A is invertible in the monoid of fractional ideals of A .*

Proof. Let $M \subset A$ be a maximal ideal. Since A is not a field, we may assume $M \neq (0)$. Let K be the field of fractions of A . Define

$$M' = \{x \in K : xM \subset A\}.$$

This is an A -submodule of K and a fractional ideal (take as denominator any element of M). Our claim is that this is the inverse of M .

By definition, $M'M \subset A$. Also $A \subset M'$. Thus $M \subset M'M \subset A$ where M is maximal. We wish to show that $M'M = M$ is impossible, leaving $M'M = A$.

Suppose for a contradiction that $M'M = M$. We will show that $M' = A$ and $M' \neq A$.

Let $x \in M'$. Then $xM \subset M$ and in fact $x^n M \subset M$ for all positive integer n . Hence $A[x]$ is a fractional ideal of A (take any $d \in M$ as denominator). Since A is Noetherian, $A[x]$ is a finitely generated A -module and so x is integral over A . Since A is integrally closed, $x \in A$. So $M' \subset A \subset M'$, i.e. $M' = A$.

Take $0 \neq a \in M$. Then $(a) \supset \prod_{i=1}^n P_i$, P_i prime (since A is Noetherian). Suppose that n is minimal among the sizes of products of primes in (a) . Now

$$M \supset (a) \supset \prod P_i$$

so M contains some prime P_i (since M is maximal, it is prime). But primes are maximal (A is a Dedekind domain), so actually $M = P_i$. Let $B = \prod_{j \neq i} P_j$ be the product of the remaining $n - 1$ primes. Then $(a) \supset MB$, and $(a) \not\supset B$ since n was minimal. Let $b \in B$ such that $b \notin (a)$. Then $Mb \subset (a)$ so $M(ba^{-1}) \subset A$ (recall that a^{-1} exists in K). Hence $ba^{-1} \in M'$. But $ba^{-1} \notin A$ since $b \notin (a)$. So $A \neq M'$, a contradiction. \square

Let A be an integral domain with field of fractions K . We can use the principal ideal notation (and notion) for fractional ideals as well, i.e. $(a) = aA$ for $a \in K$. This is always a fractional ideal (even if A is not a Noetherian ring) since there exists some $r \in A$ such that $ar \in A$ and so r serves as a denominator for (a) . Furthermore, $(a)(b) = (ab)$, clearly. If $a \in A$, then $(a)^{-1}$ is (a^{-1}) , since $(a)(a^{-1}) = (1)$.

Let's find the inverse of $(2, \sqrt{10})$.

$$\begin{aligned}
 (2, \sqrt{10}) &= \{x \in \mathbb{Q}(\sqrt{10}) : x(2, \sqrt{10}) \subset \mathbb{Z}[\sqrt{10}]\} \\
 &= \{x \in \mathbb{Q}(\sqrt{10}) : 2x, \sqrt{10}x \in \mathbb{Z}[\sqrt{10}]\} \\
 &= \{x \in \mathbb{Q}(\sqrt{10}) : x \in \frac{1}{2}\mathbb{Z}[\sqrt{10}] \cap \frac{1}{\sqrt{10}}\mathbb{Z}[\sqrt{10}]\} \\
 &= \{x \in \mathbb{Q}(\sqrt{10}) : x = \frac{a}{2} + \frac{b}{2}\sqrt{10} = \frac{c}{\sqrt{10}} + \frac{d}{\sqrt{10}}\sqrt{10}, a, b, c, d \in \mathbb{Z}\} \\
 &= \mathbb{Z} + \frac{\sqrt{10}}{2}\mathbb{Z} \\
 &= (1, \frac{\sqrt{10}}{2})
 \end{aligned}$$

Importantly, $a\mathbb{Z} + b\mathbb{Z} \neq (a, b)$ in general but in this instance it is true.

Note also that $[\mathbb{Z} + \frac{\sqrt{10}}{2}\mathbb{Z} : \mathbb{Z}[\sqrt{10}]] = 2 = N(2, \sqrt{10})$.

Theorem 16.2. *Let A be a Dedekind domain, and let*

$$S = \{P \subset A : P \text{ non-zero prime ideal}\}.$$

Then for any non-zero fractional ideal B of A ,

$$B = \prod_{P \in S} P^{e_P}$$

where the $e_P \in \mathbb{Z}$ are almost always zero. This expression is unique and the monoid of fractional ideals is a group.

Proof. Let d be a denominator for B , i.e. $dB \subset A$. Then $B = dB \cdot (d)^{-1}$ is a quotient of integral ideals. So without loss of generality, we prove the factorisation statement for integral ideals B .

Let

$$T = \{I \subset A \text{ non-zero ideals which are not products of primes}\}.$$

Suppose that T is nonempty. Then it has a maximal element J . Note that $J \neq A$ since A is the empty product. So J is contained in some maximal element P which is prime.

$J \subset P \implies JP^{-1} \subset PP^{-1} = A$ so JP^{-1} is an integral ideal. Since $A \subset P^{-1}$, JP^{-1} is an integral ideal containing J . But the containment is strict, since the containment $A \subset P^{-1}$ is strict. That is, if $J = JP^{-1}$, then for any $x \in P^{-1}$, $xJ \subset J$, and in fact $x^n J \subset J$ in general, so $x \in A$.

Therefore $JP^{-1} \notin T$. So $JP^{-1} = \prod P_i$ and $J = P \prod P_i$, a contradiction.

For uniqueness, suppose that we have two different factorisations of a fractional ideal,

$$\prod P^{e_P} = \prod P^{f_P}$$

or in other words, $\prod P^{e_P - f_P} = A$ where $e_P \neq f_P$ at least once. In fact, not all exponents can be positive (or negative) since any product of proper integral ideals is proper. We can then rearrange the equation to obtain the two factorisations

$$\prod P_i = \prod Q_i$$

where factors may repeat in each product, but the primes which appear on the left are distinct from those appearing on the right. At least one of these is a non-empty product. Then this is a proper integral ideal, so it is contained in some maximal/prime ideal R . But a prime containing a product contains at least one of the factors, i.e. $R = P_i$ for some i and $R = Q_j$ for some j , contradicting the disjointness.

Now the statement of invertibility comes from factorisation: the inverse of $\prod P^{e_P}$ is $\prod (P^{-1})^{e_P}$. \square

Exercise: The formula

$$I^{-1} = \{x \in K : xI \subset A\}$$

was only shown to hold for I maximal. Show that the formula holds in general.

Definition 16.3. *Let K be a number field. The ideal class group of \mathcal{O}_K (or K) is the group*

$$C(\mathcal{O}_K) = \{\text{non-zero fractional ideals}\} / \{\text{non-zero principal ideals}\}.$$

The class group is the trivial group if and only if \mathcal{O}_K is a principal ideal domain.

In homework, we will show

Theorem 16.4. *A ring is a Dedekind domain and a unique factorisation domain if and only if the ring is a principal ideal domain.*

The class group measures the extent to which unique factorisation of elements fails. The famous exact sequence

$$1 \rightarrow \mathcal{O}_K^* \rightarrow K^* \rightarrow \{\text{frac idls}\} \rightarrow C(K) \rightarrow 1$$

indicates that the other part of the story is the unit group. The size of $C(K)$ is called the class number of K , often denoted h_K . Which quadratic fields $\mathbb{Q}(\sqrt{d})$ have class number 1? The list is finite for negative d :

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

While for positive d it appears that a good 3/4 or so have class number 1. However, it is not known that there are infinitely many.

Some useful language:

Definition 16.5. *The order of a fractional ideal I at a prime ideal P , denoted $\text{ord}_P(I)$ is the exponent to which P appears in the factorisation of I .*

Proposition 16.6. (1) $\text{ord}_P(IJ) = \text{ord}_P(I) + \text{ord}_P(J)$

(2) I is integral $\iff \text{ord}_P(I) \geq 0, \quad \forall P$

(3) $I \subset J \iff \text{ord}_P(I) \geq \text{ord}_P(J), \quad \forall P$

(4) $\text{ord}_P(I + J) = \min(\text{ord}_P(I), \text{ord}_P(J))$

(5) $\text{ord}_P(I \cap J) = \max(\text{ord}_P(I), \text{ord}_P(J))$

Theorem 16.7. *Any fractional ideal I in a Dedekind domain A is of the form $I = (a, b)$ for some $a, b \in K$, the field of fractions of A .*

In fact, as we will see in the proof, at least one of the generators can be chosen arbitrarily.

Proof. Since $I = dJ$ for some integral ideal J , and $d \in K$, it suffices to prove this for integral ideals.

Let $a \in I$. Then $(a) \subset I$. Then we have factorisations

$$I = \prod P_i^{n_i}, \quad (a) = \prod P_i^{m_i}.$$

where $m_i \geq n_i$. For only finitely many i do we have $m_i > 0$. For these i , choose $b_i \in P_i^{n_i} \setminus P_i^{n_i+1}$ and use the Chinese Remainder Theorem to find $b \in A$ such that

$$b \equiv b_i \pmod{P_i^{n_i+1}}.$$

Now $\text{ord}_{P_i}(b) = \text{ord}_{P_i}(b_i) = n_i = \text{ord}_{P_i}(I)$ for all i with $m_i > 0$. Otherwise, $\text{ord}_{P_i}(b) \geq 0 = \text{ord}_{P_i}(a)$. So

$$\min(\text{ord}_P(a), \text{ord}_P(b)) = \text{ord}_P(I)$$

for all prime P and so $I = (a) + (b) = (a, b)$. □

17. NORMS OF IDEALS

Let K be a number field.

Proposition 17.1. *Let $x \in \mathcal{O}_K$. Then $|N_{K/\mathbb{Q}}(x)| = |\mathcal{O}_K/x\mathcal{O}_K|$.*

Proof. The ring \mathcal{O}_K is a free \mathbb{Z} -module of rank $n = [K : \mathbb{Q}]$. Multiplication by x is a module homomorphism with image the \mathbb{Z} -submodule $x\mathcal{O}_K$. It is injective (since \mathcal{O}_K is an integral domain) so the image is also free of rank n . Thus, the index of the image in \mathcal{O}_K is the determinant of the homomorphism, which is the statement. □

Definition 17.2. Let $I \subset \mathcal{O}_K$ be an ideal. Its norm is defined to be the quantity

$$N(I) = |\mathcal{O}_K/I|.$$

Since there exists some ideal J with $IJ = (a)$ where $a \in \mathcal{O}_K$ (take $J = (a)I^{-1}$ where a is a denominator to I^{-1}), then $(a) \subset I$, and the sequence

$$\mathcal{O}_K/(a) \rightarrow \mathcal{O}_K/I \rightarrow 0$$

is exact, then $N(I)$ is finite since $N((a))$ is finite.

Proposition 17.3. The norm on ideals is multiplicative.

Proof. First we will show that $N(P^m) = N(P)^m$ for prime ideals P , $m \geq 1$. To do so, consider P^n/P^{n+1} , which is an \mathcal{O}_K module for any $n \geq 1$. But since $P(P^n/P^{n+1}) = 0$, it can also be considered an \mathcal{O}_K/P -module, and it has the same structure: sub- \mathcal{O}_K -modules and sub- \mathcal{O}_K/P -modules coincide. The sub- \mathcal{O}_K -modules of P^n/P^{n+1} are exactly the possible images of the sub \mathcal{O}_K -modules of P^n under quotient by P^{n+1} . These are in bijection with the ideals J of \mathcal{O}_K such that $P^n \supset J \supset P^{n+1}$, and this bijection is order preserving. In a Dedekind domain, we have ‘cancellation of ideals’ in equalities and inequalities (shown in your homework). Therefore, ideals J above are in bijection with proper ideals of \mathcal{O}_K properly containing P , of which there are none.

Thus, P^n/P^{n+1} has no proper vector subspaces, and so $P^n/P^{n+1} \cong \mathcal{O}_K/P$ as \mathcal{O}_K -modules. In particular, their cardinalities are equal. Thus

$$|\mathcal{O}_K/P^m| = |\mathcal{O}_K/P| |P/P^2| \cdots |P^{m-1}/P^m| = |\mathcal{O}_K/P|^m$$

as required.

The second ingredient is the Chinese Remainder Theorem, which tells us that

$$\mathcal{O}_K/IJ \cong \mathcal{O}_K/I \times \mathcal{O}_K/J$$

whenever I and J are coprime.

These two taken together with unique factorisation into primes tells us that the norm is multiplicative. \square

In consequence, if the norm of an ideal is prime, then the ideal is prime.

We can of course extend the norm to fractional ideals via the factorisation of ideals, and it will still be multiplicative, with values in \mathbb{Q} . For example, the fractional ideal (p/q) of \mathbb{Z} has norm $|p/q|$ as expected.

Proposition 17.4. *If I is an ideal, then*

$$N(I)^2 = \text{disc}(w_1, \dots, w_n) / \text{disc}(K)$$

where w_1, \dots, w_n is a \mathbb{Z} -basis for I (which always exists).

Proof. The basis always exists since ideals are rank n \mathbb{Z} -modules for $n = [K : \mathbb{Q}]$. And as we saw before, the norm is the determinant of the matrix giving I as a sublattice of \mathcal{O}_K , from which the result follows. \square

We take a break for a few enjoyable consequences.

Theorem 17.5. *Fermat's Little Theorem. Let K/\mathbb{Q} be a number field of degree n , and P a prime ideal of \mathcal{O}_K . Take $\alpha \in \mathcal{O}_K$ such that $P \nmid (\alpha)$ (i.e. $(\alpha) \not\supset P$). Then $\alpha^{N(P)-1} \equiv 1 \pmod{P}$.*

Proposition 17.6. *If I is an ideal of a number field \mathcal{O}_K , then*

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

Proof. Suppose that $a_1, \dots, a_{N(P)} \equiv 0$ are a complete set of residues modulo I . Then $1 + a_1, \dots, 1 + a_{N(P)}$ is also a complete set of residues. Thus, the sums of both sets are the same, i.e. $N(I) \equiv 0 \pmod{I}$. \square

Corollary 17.7. *For any $n \in \mathbb{Z}$, $n > 0$, there are only finitely many ideals in \mathcal{O}_K with norm n .*

Proof. If an ideal has norm n then $n \in I$. Thus $I \supset (n) = P_1 \dots P_n$, i.e. $I \mid P_1 \dots P_n$. There are only finitely many such I . \square

18. GEOMETRY OF NUMBERS

Definition 18.1. *A topological group G is a group together with a topology on the underlying set under which composition and inverse are continuous. A discrete subgroup H of G is a subgroup which is discrete in the inherited subspace topology.*

For us, we are interested in the case $G = \mathbb{R}^n$, addition, standard topology. In this case, a subgroup $H \subset G$ is discrete if and only if $H \cap K$ is finite for all compact subsets K of G .

Theorem 18.2. *A subgroup H of \mathbb{R}^n is discrete if and only if H is a \mathbb{Z} -module generated by $r \leq n$ independent vectors over \mathbb{R} .*

Proof. Suppose H is discrete. Let e_1, \dots, e_r be an independent set of vectors in H of maximal size, i.e. they span H over \mathbb{R} . The set

$$P = \left\{ \sum_{i=1}^r \alpha_i e_i, q \leq \alpha_i \leq 1 \right\}$$

is compact, so $P \cap H$ is finite, and contains e_1, \dots, e_r . Let $x \in H$ with

$$x = \sum_{i=1}^r \lambda_i e_i$$

for $\lambda_i \in \mathbb{R}$. Let

$$x_j = jx - \sum_{i=1}^r [j\lambda_i] e_i.$$

Then x_j is in H since it is an integer combination of x, e_i . But the coefficients, $j\lambda_i - [j\lambda_i]$ of x_j as a linear combination of the e_i lie in $[0, 1]$, so x_j is in P also: $x_j \in P \cap H$. Since $x = x_1 - \sum [\lambda_i] e_i$, $P \cap H$ generates H over \mathbb{Z} .

Now, since $P \cap H$ is finite, $x_j = x_k$ for some $j \neq k$. So $(j - k)\lambda_i = [j\lambda_i] - [k\lambda_i]$. Thus, $\lambda_i \in \mathbb{Q}$. Let d be the common denominator of the λ_i 's.

Now

$$dH \subset \sum \mathbb{Z}e_i \subset H$$

is a chain of \mathbb{Z} -modules. But $dH \cong H$ as \mathbb{Z} -modules. Since $\sum \mathbb{Z}e_i$ is free of rank r , then dH is free of rank $\leq r$. But then H is free, and it must have rank $\geq r$. So H is free of rank exactly r .

Conversely, to show that such a \mathbb{Z} -module is discrete, it suffices to show that $\min |x - y|$ is bounded away from zero for $x, y \in H$ (every point is isolated). Choose an isomorphism of \mathbb{R}^n taking the independent vectors generating H to standard basis vectors. Under this isomorphism, the image satisfies $\min |x - y| = 1$ for $x \neq y$ in H . But isomorphisms of \mathbb{R}^n are homeomorphisms, so H is discrete if and only if its image is discrete. \square

A subgroup satisfying the conditions of the theorem is called a *lattice*. In greater generality,

Definition 18.3. *Let μ be a measure on a topological group G . The covolume of a discrete subgroup H of a topological group is the measure of the quotient $\mu(G/H)$. A lattice in a topological group is a discrete subgroup with finite covolume.*

For us, the Lebesgue measure is used, and a lattice is exactly something satisfying the theorem above of rank n . The covolume of the lattice is the measure of the fundamental parallelogram, $v(H)$. This is $|\det(M)|$ where M is the matrix of basis elements for H , so this is independent of choice of basis.

Theorem 18.4. (*Minkowski*) Let H be a lattice in \mathbb{R}^n , and $S \subset \mathbb{R}^n$ a measurable subset, with $\mu(S) > v(H)$. Then there exist $x, y \in S$, $x \neq y$ with $x - y \in H$.

Proof. Let e_i be a basis for H . Let P_e be the fundamental parallelogram $\{\sum \alpha_i e_i, 0 \leq \alpha_i < 1\}$. Then S is the disjoint union of $S \cap (h + P_e)$ as h runs over H . So $\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_e)) = \sum_{h \in H} \mu((-h + S) \cap P_e)$ by translation invariance of the measure. But $\mu(P_e) = v(H) < \mu(S)$, so these are not all disjoint. So $P_e \cap (-h + S) \cap (-h' + S) \neq \emptyset$ for some $h \neq h'$. So $-h + x = -h' + y$ and so $x - y = h - h' \in H$ is non-zero. \square

Corollary 18.5. (*Blichfeldt*) Let H be a lattice in \mathbb{R}^n , and S a measurable set in \mathbb{R}^n which is convex and symmetric about 0. If either

- (1) $\mu(S) > 2^n v(H)$; or
- (2) $\mu(S) \geq 2^n v(H)$ and S is compact

then $S \cap (H \setminus \{0\}) \neq \emptyset$.

Proof. In the case (1): Consider the set $S' = \frac{1}{2}S$. Then $\mu(S') = 2^{-n} \mu(S) > v(H)$. So there are $x \neq y$ in S' with $x - y \in H$. But $x - y = 1/2(2x + (-2y))$ is also in S since S is convex and symmetric about 0.

In the case (2): Consider the set $(1 + \epsilon)S$ and apply part (1) to obtain that $(H \setminus \{0\}) \cap (1 + \epsilon)S$ is nonempty. It is discrete (since H is) and compact (since S is). The set $\bigcap_{\epsilon > 0} (H \setminus \{0\}) \cap (1 + \epsilon)S$ is nonempty since it is the nested limit of nonempty compact sets. Any any point in this nested limit is in S since S is compact. \square

19. GEOMETRY OF CANONICAL EMBEDDING; CLASS GROUPS

For this section let K be a number field of degree n . Then there are r_1 embeddings of K into \mathbb{R} , call them $\sigma_1, \dots, \sigma_{r_1}$. The remaining embeddings take values in \mathbb{C} and come in conjugate pairs. Call these $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ and their partners $\sigma_{r_1+r_2+1}, \dots, \sigma_{r_1+r_2+r_2}$. Then $r_1 + 2r_2 = n$. We define the *canonical embedding* to be the map

$$\sigma : K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$$

defined by $\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x))$.

This is a ring homomorphism and \mathbb{Q} -linear. By the linear independence of the σ_i 's, the image $\sigma(M)$ of any \mathbb{Z} -module $M \subset K$ is a lattice. Let's compute the covolume of this lattice.

Suppose that x_i form a basis for M . Then the matrix of σ (into \mathbb{R}^n) has columns

$$(\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), R(\sigma_{r_1+1}(x_i)), I(\sigma_{r_1+1}(x_i)), \dots, R(\sigma_{r_1+r_2}(x_i)), I(\sigma_{r_1+r_2}(x_i)))$$

But R and I are \mathbb{R} -linear and $I(x) = (1/2i)(z - \bar{z})$, $R(z) = z - I(z)$. And $\sigma_{r_1+r_2+i}(x) = \overline{\sigma_{r_1+i}(x)}$. So changing basis from the matrix $(\sigma_i(x_j))$ (mapping into \mathbb{C}) to the matrix above means an alteration of the determinant by $\pm(2i)^{-r_2}$.

Hence,

$$v(\sigma(M)) = 2^{-r_2} |\text{disc}(x_i)|^{1/2} = 2^{-r_2} |\text{disc}(K)|^{1/2} N(M)$$

if M is an ideal.

Proposition 19.1. *Let K be a number field of degree $n = r_1 + 2r_2$, $d = \text{disc}(K)$ and $I \subset \mathcal{O}_K$ an ideal. Then there exists a non-zero $x \in I$ with*

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_1} \frac{n!}{n^n} |d|^{1/2} N(I).$$

Proof. Let $t > 0$ be real. Set

$$B_t = \{(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t\}$$

which is compact, convex and symmetric around $0 \in \mathbb{R}^n$.

We will prove in an appendix that

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

Choose t satisfying $\mu(B_t) = 2^n v(\sigma(I))$ i.e. $t^n = 2^{n-r_1} \pi^{-r_2} n! |d|^{1/2} N(I)$.

Then by Corollary 18.5, there exists a non-zero $x \in I$ with $\sigma(x) \in B_t$.

So

$$\begin{aligned} N(x) &= \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2 \\ &\leq \left(\frac{1}{n} \sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n} \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right)^n \\ &\leq \frac{t^n}{n^n} = \frac{2^{2r_2} n!}{\pi^{r_2} n^n} |d|^{1/2} N(I). \end{aligned}$$

□

Corollary 19.2. *Let K be a number field. Then every ideal class of K contains an integral ideal I with*

$$N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}.$$

Proof. Suppose that J is a fractional ideal of the ideal class. Multiplying by a principal ideal, we can assume that J^{-1} is an integral ideal (multiply by (d) where d is a denominator for J^{-1}). Let $x \in J^{-1}$ be as in the Theorem. Then $I = xJ$ is integral and in the same class as J . And

$$N(I) = N(x)N(J) \leq \left(\frac{4}{\pi}\right)^{r_1} \frac{n!}{n^n} |d|^{1/2}.$$

□

Finally, with this result we now can show

Theorem 19.3. (*Dirichlet*) *Let K be a number field. Then the ideal class group of a number field is finite.*

Proof. Every ideal class contains an integral ideal of norm $< c_K$, some constant depending on K and not the ideal class. But there exists only finitely many ideals of a given norm. □

Example 19.4. *Let's compute the class group of $\mathbb{Q}(i)$, which we know should be trivial, since $\mathbb{Q}(i)$ is a PID. We have*

$$n = 2, \quad r_1 = 0, \quad r_2 = 1, \quad \text{disc}(K) = -4.$$

So every ideal class contains an ideal I with

$$N(I) \leq \left(\frac{4}{\pi}\right) \frac{2!}{2^2} |-4|^{1/2} = \frac{4}{\pi} \leq 2.$$

So every ideal class has an ideal of norm 1, i.e. every ideal class is trivial.

Example 19.5. *Let's compute the class group of $\mathbb{Q}(\sqrt{-23})$.*

$$n = 2, \quad r_1 = 0, \quad r_2 = 1, \quad \text{disc}(K) = -23.$$

So every ideal class contains an ideal I with

$$N(I) \leq \frac{4}{\pi} \frac{2!}{2^2} |-23|^{1/2} = \frac{2\sqrt{23}}{\pi} < \frac{10}{\pi} < 4.$$

If we have the prime factorisation $I = \prod P_i$. The finite field \mathcal{O}_K/P_i has some characteristic p prime, meaning $p \in P_i$ or $P_i \mid (p)$; further, $N(P_i) \mid N(p) = p^2$, hence $p \mid N(P_i)$. Thus we need only look at prime ideals dividing (p) for $p < 4$.

With this in mind, we will factor (2) and (3).

The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-23}}{2}$ has minimal polynomial $\alpha^2 - \alpha + 6 = 0$.

To factor the ideal (2) for example, consider the quotient ring

$$\mathcal{O}_K/(2) = (\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x).$$

This is not a field since $x^2 + x \equiv x(x+1) \pmod{2}$, so (2) is not prime. But it has quotients

$$\mathcal{O}_K/(2, x+1), \quad \mathcal{O}_K/(2, x),$$

which are fields of size 2. These correspond to the ideals

$$P = \left(2, \frac{3 + \sqrt{-23}}{2}\right) = \left(2, \frac{1 - \sqrt{-23}}{2}\right), \quad P' = \left(2, \frac{1 + \sqrt{-23}}{2}\right),$$

which are both of norm 2.

We have

$$(2) = \left(2, \frac{1 - \sqrt{-23}}{2}\right) \left(2, \frac{1 + \sqrt{-23}}{2}\right) = PP',$$

$$(3) = \left(3, \frac{1 - \sqrt{-23}}{2}\right) \left(3, \frac{1 + \sqrt{-23}}{2}\right) = QQ'.$$

where $N(P) = N(P') = 2$, $N(Q) = N(Q') = 3$. So the full list of ideals of norm less than 4 is

$$(1), P, P', Q, Q'$$

So the class group is at most five elements. We know $PP' \sim (1)$ and $QQ' \sim (1)$. We can also calculate

$$PQ = \left(6, 2 \left(\frac{1 - \sqrt{-23}}{2}\right), 3 \left(\frac{1 - \sqrt{-23}}{2}\right), \left(\frac{1 - \sqrt{-23}}{2}\right)^2\right).$$

But since

$$6 = \left(\frac{1 - \sqrt{-23}}{2}\right) \left(\frac{1 + \sqrt{-23}}{2}\right),$$

we have $PQ = \left(\frac{1 - \sqrt{-23}}{2}\right) \sim (1)$. Similarly, $P'Q' \sim (1)$.

So $P \sim PP'Q' \sim Q'$ and $P' \sim P'PQ \sim Q$. So we are left with

$$(1), P, P'$$

Now, $P \not\sim (1)$ since if $P = \left(\frac{a+b\sqrt{-23}}{2}\right)$, then $2 = N(P)$, i.e. $a^2 + 23b^2 = 8$ which has no solutions. Similarly, $P' \not\sim (1)$.

Finally, how do we know $P \not\sim P'$? Note that

$$N\left(\frac{3 - \sqrt{-23}}{2}\right) = 8$$

So there is a principal ideal of norm 8. The full list of ideals of norm 8, however, is

$$P^3, P^2P', PP'^2, P'^3$$

If $P \sim P'$ then these ideals are either all principal or none principal; necessarily all. But

$$PPP' \sim P \not\sim (1).$$

So $P \not\sim P'$.

20. HERMITE'S THEOREM ON DISCRIMINANTS

Another corollary to Proposition 19.1 / Corollary 19.2.

Corollary 20.1. *Let K be a number field of degree n with discriminant d . For $n \geq 2$,*

$$|d| \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}$$

Proof. Let I be a non-zero integral ideal of \mathcal{O}_K . Then $N(I) \geq 1$, so

$$|d|^{1/2} \geq \left(\frac{\pi}{4}\right)^{r_2} \left(\frac{n^n}{n!}\right)$$

from the Corollary 19.2 to Proposition 19.1.

But $\pi < 4$ and $2r_2 \leq n$, so $\left(\frac{\pi}{4}\right)^t$ decreases as t increases. So

$$a_n := \left(\frac{\pi}{4}\right)^n \left(\frac{n^{2n}}{n!}\right) \leq |d|$$

Now, using the binomial expansion of $(1 + 1/n)^{2n}$, we obtain

$$\begin{aligned} \frac{a_{n+1}}{a_n} &= \frac{\pi}{4} \left(\frac{n+1}{n}\right)^{2n} \\ &= \frac{\pi}{4} (1 + 2 + \text{positive terms}) \\ &\geq \frac{3\pi}{4}. \end{aligned}$$

So since $a_2 = \pi^2/4$,

$$|d| \geq \frac{\pi^2}{4} \left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}.$$

□

In particular, if $n \geq 2$, then since $3\pi/4 > 1$, the right-hand side grows with n and

$$|d| \geq \pi^2/4 > 1$$

which gives us

Theorem 20.2. *(Hermite-Minkowski) If K is a number field not equal to \mathbb{Q} , then the discriminant of K is not ± 1 .*

Hermite also proved the stronger theorem.

Theorem 20.3. *In \mathbb{C} there are only finitely many number fields with a given discriminant.*

Proof. The degree of the number field is bounded in terms of the discriminant, by Corollary 20.1. So it suffices to analyse finitely many possible signatures (r_1, r_2) . We will define a subset $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and apply Blichfeldt's Theorem 18.5. In this way we will obtain an $x \in \mathcal{O}_K$ such that $\mathbb{Q}(x) = K$ and x 's embedded images are bounded in norm.

In the case that $r_1 > 0$, define

$$B = \left\{ (y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) : \begin{array}{l} |y_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d|^{1/2} \\ |y_i| \leq \frac{1}{2}, i = 1, \dots, r_1 \\ |z_j| \leq \frac{1}{2}, j = 1, \dots, r_2 \end{array} \right\}$$

In the case that $r_1 = 0$, define

$$B = \left\{ (y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) : \begin{array}{l} |z_1 - \bar{z}_1| \leq 2^n \left(\frac{\pi}{2}\right)^{1-r_2} |d|^{1/2} \\ |z_1 + \bar{z}_1| \leq \frac{1}{2} \\ |z_j| \leq \frac{1}{2}, j = 2, \dots, r_2 \end{array} \right\}$$

In either case, B is compact, convex and symmetric about 0 in \mathbb{R}^n . And in either case, the volume of B can be computed to be $2^{n-r_2} |d|^{1/2}$. For example, in the first case, one has

$$2^n \left(\frac{\pi^{-r_2}}{2} |d|^{1/2} 2^{1-r_1} \left(\frac{pi}{4}\right)^{r_2} \right) = 2^{n-r_2} |d|^{1/2}.$$

Thus, we can apply Blichfeldt with $H = \sigma(\mathcal{O}_K)$ which has volume $2^{-r_2} |d|^{1/2}$. We obtain a non-zero point $x \in B \cap \sigma(\mathcal{O}_K)$. Thus

$$|N(x)| = \prod_{i=1}^n |\sigma_i(x)|$$

is a positive integer, while $|\sigma_i(x)| \leq 1/2$ for all $i \neq 1$ appearing in the canonical embedding. So $|\sigma_i(x)| \geq 1$. In particular, $\sigma_1(x)$ is distinct from all other $\sigma_i(x)$ (except possibly $\overline{\sigma_1(x)}$ in case b) if $\sigma_1(x) \in \mathbb{R}$; but then $R(\sigma_1(x)) \leq 1/4 < |\sigma_1(x)|$ so $\sigma_1(x) \notin \mathbb{R}$.

Thus we have shown that $K = \mathbb{Q}(x)$ for some $x \in \mathcal{O}_K$ with $\sigma(x) \in B$. The conjugates are bounded in norm, hence so are the elementary symmetric functions. Thus, the coefficients of the minimal polynomial are bounded, but these are integers, so this implies there are only finitely many possible polynomials, and thus only finitely many possible roots $x \in \mathbb{C}$ and K . \square

21. DIRICHLET'S UNIT THEOREM

We now consider the *logarithmic embedding* of a number field K , i.e.

$$L : K^* \rightarrow \mathbb{R}^{r_1+r_2}$$

such that

$$x \mapsto (\log |\sigma_1(x)|, \dots, \log |\sigma_{r_1+r_2}(x)|).$$

Lemma 21.1. *Let B be a compact subset of $\mathbb{R}^{r_1+r_2}$, and K a number field. Then $\mathcal{O}_K \cap L^{-1}(B)$ is finite.*

Proof. Since B is bounded, there exists some α , a real number larger than 1, such that

$$\alpha^{-1} \leq |\sigma_i(x)| \leq \alpha \quad \forall i = 1, \dots, n, x \in B.$$

Thus the elementary symmetric functions in the conjugates are also bounded in absolute value. Suppose that $x \in L(\mathcal{O}_K \setminus \{0\})$. Then the elementary symmetric functions in the conjugates, which are the coefficients of the minimal polynomial, are rational integers. So there are only finitely many possible polynomials for x , and hence only finitely many possible $x \in K$. \square

Now consider the set $\mu_K = \ker(L) \cap \mathcal{O}_K = \{x \in \mathcal{O}_K : |\sigma_i(x)| = 1 \forall i\}$. Since $B = \{0\}$ is compact, this is finite. If $x \in \mu_K$, then so are the powers of x , so x has finite multiplicative order in K^* . Thus $x \in \mathcal{O}_K^*$ is a root of unity. Conversely, roots of unity x are all in \mathcal{O}_K^* since $x^n - 1 = 0$, and they are in the kernel of L since $1 = |\sigma_i(1)| = |\sigma_i(x^n)| = |\sigma_i(x)|^n$ so $|\sigma_i(x)| = 1$. So μ_K is the collection of roots of unity in the field K .

Proposition 21.2. *Let K be a field. If G is a finite subgroup of K^* , then $G \subset \mu_K$ and is cyclic.*

Proof. Since G is commutative,

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$$

where $a_1 \mid a_2 \mid \dots \mid a_n$, $a_i \neq 0$.

The element $x = (0, 0, \dots, 0, 1)$ has order a_n and every element of G has order dividing a_n . But in a field, there are at most a_n elements that are roots of $X^{a_n} - 1$, so $|G| = a_n$ and so

$$G \cong \mathbb{Z}/a_n\mathbb{Z}.$$

\square

These are roots of unity, of which $\phi(a_n)$ are primitive.

Recall from the beginning of semester that the units \mathcal{O}_K^* are exactly those elements of \mathcal{O}_K with norm ± 1 .

We are now in a position to prove Dirichlet's Unit Theorem

Theorem 21.3. (*Dirichlet*) *Let K be a number field with signature (r_1, r_2) . Then*

$$\mathcal{O}_K^* \cong \mathbb{Z}^{r_1+r_2-1} \times \mu_K.$$

Proof. $L(\mathcal{O}_K^*)$ is a discrete subgroup of $\mathbb{R}^{r_1+r_2}$ by Lemma 21.1. Thus it is a lattice of rank $s \leq r_1 + r_2$. In fact, $L(\mathcal{O}_K^*)$ lies in a hyperplane

$$W = \left\{ (y_i) : \sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0 \right\};$$

one sees this by taking the logarithm of the relation $|N(x)| = 1$.

Thus the rank of $L(\mathcal{O}_K^*)$ is at most $r = r_1 + r_2 - 1$. Note that W projects isomorphically onto \mathbb{R}^r .

To show that the rank of $L(\mathcal{O}_K^*)$ is exactly r , we will consider linear forms on W : actually, defined on $\mathbb{R}^{r_1+r_2}$ but constant with respect to the last variable, so

$$f(y) = c_1 y_1 + \cdots + c_r y_r.$$

For each, find hope to find some $u \in \mathcal{O}_K^*$ such that $f(L(u)) \neq 0$.

The main tool in the proof is Blichfeldt's theorem and the canonical embedding.

Choose an $\alpha \geq 2^n \left(\frac{1}{2\pi}\right)^{r_2} |d|^{1/2}$ fixed for the remainder of the proof.

Let $\lambda_1, \dots, \lambda_r$ be any elements of \mathbb{R} and determine λ_{r+1} such that

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha.$$

Set the notation $\lambda_* = (\lambda_1, \dots, \lambda_{r+1}) \in \mathbb{R}^{r+1}$.

The set we use will be

$$B = \{(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) : |y_i| \leq \lambda_i, |z_j| \leq \lambda_{j+r_1}\}$$

in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, which is compact, convex and symmetric about the origin in \mathbb{R}^n . Its volume is

$$\mu(B) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r_1+r_2} \pi\lambda_j^2 = 2^{r_1} \pi^{r_2} \alpha$$

which is greater than or equal to $2^{n-r_2} |d|^{1/2} = 2^n v(\sigma(\mathcal{O}_K))$. Thus by Blichfeldt, we get an $x_{\lambda_*} \in \mathcal{O}_K$, such that $\sigma(x_{\lambda_*}) \in B$.

The norm $1 \leq |N(x_{\lambda_*})| \leq \alpha$ by definition, and hence there are only finitely many distinct possible ideals (x_{λ_*}) . Thus, if we can find infinitely many such x_{λ_*} in such a way that their images under $f \circ L$

are *distinct*, then there will be a unit u such that $x_{\lambda_*} = ux_{\lambda'_*}$ for some λ_* and λ'_* , and then

$$f(L(u)) = f(L(x_{\lambda_*})) - f(L(x_{\lambda'_*})) \neq 0$$

and we will have found the $u \in \mathcal{O}_K^*$ we seek for the form f .

The rest of the proof is devoted to actually finding an infinite set of such x_{λ_*} .

The trick is that the bounds for the coordinates of $\sigma(x_{\lambda_*})$ in terms of the coordinates of λ_* bound $f(L(x_{\lambda_*}))$ close to $f(\log \lambda_*)$ (here \log means coordinatewise \log), and then it suffices to space out the $\log \lambda_*$'s.

First, we calculate the bound referred to. We have

$$|\sigma_i(x_{\lambda_*})| = |N(x_{\lambda_*})| \prod_{i \neq j} |\sigma_j(x_{\lambda_*})|^{-1} \geq \prod_{i \neq j} \lambda_j^{-1} = \lambda_i \alpha^{-1}.$$

Thus

$$\lambda_i \alpha^{-1} \leq |\sigma_i(x_{\lambda_*})| \leq \lambda_i$$

from which we have

$$1 \leq \frac{\lambda_i}{|\sigma_i(x_{\lambda_*})|} \leq \alpha.$$

Hence

$$0 \leq \log \lambda_i - \log |\sigma_i(x_{\lambda_*})| \leq \log \alpha$$

Now

$$\begin{aligned} & |f(L(x_{\lambda_*})) - f(\log \lambda_*)| \\ &= \left| \sum_{i=1}^r c_i (\log |\sigma_i(x_{\lambda_*})| - \log \lambda_i) \right| \\ &\leq \sum_{i=1}^r |c_i| \log \alpha \end{aligned}$$

Now we design a collection of sufficiently spaced out $\lambda_{*,h}$'s, one for each positive integer h .

For this part of the proof, choose some $\beta > \sum_{i=1}^r |c_i| \log \alpha$. Then choose $\lambda_{*,h}$ such that $f(\log \lambda_{*,h}) = 2\beta h$ (as before, $\lambda_{r+1,h}$ is determined from the first r choices). Find corresponding $x_h = x_{\lambda_{*,h}} \in \mathcal{O}_K$.

Then

$$|f(L(x_h)) - 2\beta h| = |f(L(x_h)) - f(\lambda_{*,h})| \leq \sum |c_i| \log \alpha < \beta.$$

So

$$(2h - 1)\beta < f(L(x_h)) < (2h + 1)\beta.$$

which suffices to show that the $f(L(x_h))$ are distinct, and as promised, this gives a unit u such that $f(L(u)) \neq 0$.

So the rank of $L(\mathcal{O}_K^*)$ is $r = r_1 + r_2 - 1$.

Finally, we have an exact sequence of abelian groups

$$0 \rightarrow \mu_K \rightarrow \mathcal{O}_K^* \rightarrow L(\mathcal{O}_K^*) \rightarrow 0$$

in which $L(\mathcal{O}_K^*)$ is torsion free, and so

$$\mathcal{O}_K^* \cong L(\mathcal{O}_K^*) \times \mu_K \cong \mathbb{Z}^{r_1+r_2-1} \times \mu_K.$$

□

Thus, we have a sort of unique factorisation for units. Once you choose a basis $u_1, \dots, u_{r_1+r_2-1}$ for the free part (sometimes called a system of fundamental units), every unit factors uniquely in the form

$$u = zu_1^{n_1} \cdots u_{r_1+r_2-1}^{n_{r_1+r_2-1}}$$

up to reordering, where z is a root of unity.

Some examples:

- (1) The units of \mathbb{Q} are $\{\pm 1\}$.
- (2) In imaginary quadratic fields, $r_1 + r_2 - 1 = 0$ and all units are roots of unity.
- (3) In real quadratic fields, $r_1 + r_2 - 1 = 1$ and there exists a single *fundamental unit* generating all units other than the roots of unity as powers. We proved this earlier in the course.
- (4) $\mathbb{Q}(\zeta_p)$ where p is prime, odd, has no real embeddings. So $r_1 + r_2 - 1 = \frac{p-1}{2} - 1 = \frac{p-3}{2}$.
- (5) Real cubic fields also have $r_1 + r_2 - 1 = 1$ and a *fundamental unit*.

The image $L(\mathcal{O}_K^*)$ is a lattice in a subspace of $\mathbb{R}^{r_1+r_2}$, and its covolume is an important invariant of the field K . There are many ways to define this, which differ by a scaling factor depending on r_1 and r_2 . The most common definition is the following.

Definition 21.4. *The regulator r_K of the field K is the absolute value of the determinant of the matrix*

$$(a_i \log |\sigma_j(w_i)|)_{1 \leq i, j \leq r_1+r_2-1}$$

where the w_i form a system of fundamental units, and where $a_j = 1$ or 2 depending upon whether σ_j is real or complex, respectively. If $r_1 + r_2 - 1 = 0$ ($K = \mathbb{Q}$ or K is quadratic imaginary), then we say $r_K = 1$ (the determinant of an empty matrix). It is independent of the choice of system of fundamental units.

For example, $K = \mathbb{Q}(\sqrt{5})$ has $r_1 = 2, r_2 = 0$ and a fundamental unit $\frac{1+\sqrt{5}}{2}$. The roots of unity in \mathbb{R} are $\{\pm 1\}$. So

$$\mathcal{O}_K^* = \left\{ \pm \left(\frac{1 + \sqrt{5}}{2} \right)^n, n \in \mathbb{Z} \right\}.$$

And the regulator is $r_K = \left| \log \frac{1+\sqrt{5}}{2} \right|$.

We have now seen all the standard invariants of a number field. We pause for a tiny bit of analytic number theory to see these come together. Recall the famous Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s} \right)^{-1}$$

which continues analytically to the whole complex plane and has a single simple pole at $s = 1$. We can generalise this for any field K to its *Dedekind zeta function*,

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(I)^s} = \prod_{P \subset \mathcal{O}_K} \prod_{\text{prime}} \left(1 - \frac{1}{N_{K/\mathbb{Q}}(P)^s} \right)^{-1}$$

which also extends analytically to the whole of \mathbb{C} and has a single simple pole at $s = 1$. We then have the famous *Analytic Class Number Formula*:

$$\text{Res}_{s=1}(\zeta_K(s)) = \frac{2^{r_1} (2\pi)^{r_2} h_K r_K}{|\mu_K| \sqrt{\text{disc}(K)}}.$$

(The notation h_K is standard for $|C(K)|$.) We will compute some class numbers this way after we talk about splitting of primes.

22. RINGS OF FRACTIONS / LOCALISATION

Let A be a ring, and $S \subset A$ a multiplicatively closed subset of A which contains 1 and does not contain 0. Define $S^{-1}A$ as all pairs (a, s) of $a \in A$ and $s \in S$ under the equivalence relation

$$(a, s) \sim (b, t) \iff (at - bs)u = 0 \text{ for some } u \in S,$$

and give it addition and multiplication defined by

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

where (a, s) is denoted by a fraction $\frac{a}{s}$. Exercise: check that this is an equivalence relation and the resulting construction is a ring. Also check that $f : A \rightarrow S^{-1}A$ given by $f(a) = a/1$ is a ring homomorphism.

This is a *ring of fractions* or a *localisation*. We generally say we are localising *at* the set $A \setminus S$.

The kernel of f is all $a \in A$ such that $as = 0$ for some $s \in S$. Thus, in the case that A is an integral domain, $A \setminus \{0\}$ is a multiplicatively closed, and the resulting ring K is a field, the *field of fractions*. In this case, f is injective and we can identify $S^{-1}A$ (for any other multiplicatively closed $S \subset A$ containing 1 and not 0) with the set

$$\{x \in K : x = a/s, a \in A, s \in S\}.$$

Thus, for number theory, we could use this as the definition (Samuel does).

Example 22.1. Let $P \subset A$ be a prime ideal of A . Then $S = A \setminus P$ is a multiplicatively closed subset containing 1 but not 0. This is, in fact, the definition of prime: if $a \notin P, b \notin P$, then $ab \notin P$. We write $S^{-1}A = A_P$ and call this the localisation of A at P . Consider the subset M of A_P defined by

$$M = \left\{ \frac{a}{s}, a \in P, s \in S \right\}.$$

This is clearly an ideal. If $\frac{b}{t} \notin M$ then $b \notin P$, so $b \in S$. Thus $\frac{b}{t}$ is a unit in A_P and so M is the only maximal ideal of A_P (any ideal not entirely contained in it will contain a unit).

Example 22.2. Suppose that $a \in A$. Then we can take $S = \{a^n\}$. We then write $S^{-1}A = A_a$. (Note that $A_{(p)} \neq A_p$.)

Example 22.3. Suppose that $A = \mathbb{Z}$. Then $A_n = \mathbb{Z}[\frac{1}{n}]$ and $A_{(p)}$ is the set of all rationals with denominator not divisible by p .

Example 22.4. If $A = K[X_1, \dots, X_n]$ a polynomial ring over an infinite field K , and P is a prime of A , then A_P is the collection of all rational functions f/g where $g \notin P$. If we consider the variety defined by P ,

$$V = \{(x_1, \dots, x_n) \in K^n : f(x) = 0 \forall f \in P\}$$

then A_P is all rational functions on K^n defined at almost all points of V .

Now consider contraction of ideals in the extension $A \subset S^{-1}A$.

$$\{\text{ideals of } S^{-1}A\} \rightarrow \{\text{ideals of } A\}, \quad I \mapsto I \cap A.$$

Proposition 22.5. $I^{ce} = I$

Proof. $I^{ce} = (I \cap A)S^{-1}A \subset I$ since I is an ideal. Conversely, suppose that $x \in I$. Then $x = a/s$ where $a \in A, s \in S$. So $a = sx \in I \cap A$ since I is an ideal and $a \in A$. So $x = \frac{1}{s}a \in (I \cap A)S^{-1}A$ since this is an ideal. \square

Proposition 22.6. *Contraction gives an isomorphism of posets*

$$\{\text{primes ideals of } S^{-1}A\} \rightarrow \{\text{primes ideals of } A \text{ not intersecting } S\}$$

whose inverse is ideal extension.

Proof. As we already know, on the set of ideals, contraction preserves the inclusion ordering and takes primes to primes. If a prime P of $S^{-1}A$ has $s \in S \cap P$, then $1 = \frac{1}{s} \cdot s \in P$, a contradiction.

The map is injective by the previous proposition, and extension is a retraction. We now show that extension is a section.

Let Q be a prime of A with $S \cap Q = \emptyset$. Any $x \in QS^{-1}A$ has the form

$$x = \sum \frac{a_i}{s_i} q_i = \sum \frac{b_i}{s} q_i = \frac{\sum b_i q_i}{s}$$

where the middle equality follows from taking $s = s_1 \cdots s_n$ and $\frac{b_i}{s} = \frac{a_i}{s_i}$. Thus

$$QS^{-1}A = \{x \in S^{-1}A : x = q/s, q \in Q, s \in S\}.$$

So $1 \notin QS^{-1}A$ since $Q \cap S = \emptyset$.

Now we show that $QS^{-1}A$ is prime. Let $a/t, b/r \in S^{-1}A$ with $\frac{ab}{tr} \in QS^{-1}A$, so $\frac{ab}{tr} = \frac{q}{s}$ for some $q \in Q, s \in S$. Then $abs = qtr \in Q$ since $q \in Q, tr \in A$. But $s \notin Q$ so $ab \in Q$ by primality, and hence $a \in Q$ or $b \in Q$. Thus a/s or b/s is in $QS^{-1}A$.

Finally, $Q \subset QS^{-1}A \cap A$ is clear. For the other inclusion, suppose $x \in QS^{-1}A \cap A$. Then $x = q/s, q \in Q, s \in S$, and so $sx = q \in Q$, but $s \notin Q$ so $x \in Q$ by primality. \square

Corollary 22.7. *If A is Noetherian, then $S^{-1}A$ is Noetherian.*

Proof. The poset of ideals injects from $S^{-1}A$ to A , so the maximality condition is preserved. \square

Proposition 22.8. *Let R be an integral domain with a subring A , and let S be a multiplicatively stable subset of A containing 1 but not 0. Let B be the integral closure of A in R . Then $S^{-1}B$ is the integral closure of $S^{-1}A$ in $S^{-1}R$.*

Proof. Suppose that $b \in B, s \in S$. Then

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

and so

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s} \left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0.$$

Conversely, suppose r/s is integral over $S^{-1}A$, $r \in R$, $s \in S$. Then

$$\left(\frac{r}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}} \left(\frac{r}{s}\right)^{n-1} + \cdots + \frac{a_0}{t_0} = 0,$$

and if $t = t_0 t_1 \cdots t_n$ then

$$\left(\frac{rt}{s}\right)^n + \frac{a_{n-1}t}{t_{n-1}} \left(\frac{rt}{s}\right)^{n-1} + \cdots + \frac{a_0 t^n}{t_0} = 0.$$

Thus rt/s is integral over A and so is in B . Thus $\frac{r}{s} = \frac{1}{t} \cdot \frac{rt}{s} \in S^{-1}B$. \square

Corollary 22.9. *If A is integrally closed, then $S^{-1}A$ is integrally closed.*

Proposition 22.10. *If A is a Dedekind domain, then $S^{-1}A$ is a Dedekind domain.*

Proof. $S^{-1}A$ is Noetherian and integrally closed by previous results. The map from ideals of $S^{-1}A$ to ideals of A given by contraction is order preserving and injective. It takes prime ideals to prime which are maximal, but the preimage of a maximal ideal must be maximal by injectivity. \square

Proposition 22.11. *If A is a Dedekind domain, and P is a prime ideal of A , and $S = A \setminus P$, then $S^{-1}A$ is a principal ideal domain and there exists a prime Q of $S^{-1}A$ such that all non-zero ideals of $S^{-1}A$ are non-negative powers of Q .*

Proof. The non-zero primes of $S^{-1}A$ are in bijection with the non-zero primes of A disjoint with S , but the latter set consists of exactly one member, P . So let $Q = PS^{-1}A$. Since $S^{-1}A$ is a Dedekind domain, it has unique factorisation, so all non-zero ideals are of the form Q^n for some $n \geq 0$. If $Q = Q^2$, then by cancellation of ideals, $S^{-1}A = Q$, a contradiction. Therefore, let $q \in Q \setminus Q^2$. Then $(q) \subset Q$, but $(q) \not\subset Q^n$ for $n > 1$. So $Q = (q)$ and $Q^n = (q)^n = (q^n)$. \square

Proposition 22.12. *Let A be an integral domain with a multiplicatively stable subset S containing 1 and not 0. Let $M \subset A$ be a maximal ideal not intersecting S . Then*

$$S^{-1}A/MS^{-1}A \cong A/M.$$

Proof. Consider the composition

$$A \rightarrow S^{-1}A \rightarrow S^{-1}A/MS^{-1}A$$

It has kernel $MS^{-1}A \cap A = M$. So there exists an injective homomorphism

$$\phi : A/M \rightarrow S^{-1}A/MS^{-1}A$$

We will now show that ϕ is surjective. Let $x = a/s \in S^{-1}A$. Denote its residue modulo $MS^{-1}A$ by \bar{x} . Then $s \notin M$ so it must be a unit modulo M . Let b be such that $bs \equiv 1$ modulo M . Then

$$\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in MS^{-1}A$$

and so ϕ takes ab to \bar{x} . □

23. SPLITTING OF PRIMES

Our situation is the following:

$$\begin{array}{ccccc}
 L & B & \mathfrak{p}B = \prod_{i=1}^q \mathcal{P}_i^{e_i} & B/\mathfrak{p}B & B/\mathcal{P}_i \\
 \left| \begin{array}{c} n \\ \hline \end{array} \right. & \left| \right. & \left| \right. & \left| \right. & \left| \begin{array}{c} f_i \\ \hline \end{array} \right. \\
 K & A & \mathfrak{p} & A/\mathfrak{p} & A/\mathfrak{p}
 \end{array}$$

Start with a Dedekind domain A , and let K be its field of fractions. Consider a field extension L of K of finite degree n . Let B be the integral closure of A in L , which is also a Dedekind domain (for us, frequently $A = \mathcal{O}_K$ and $B = \mathcal{O}_L$). Let \mathfrak{p} be a prime of A and consider its extension $\mathfrak{p}B$ in B . Since B is a Dedekind domain, this ideal splits as a product of primes $\prod_{i=1}^q \mathcal{P}_i^{e_i}$.

Since B is a finitely generated A -module, and $\mathfrak{p}B \cap A = \mathfrak{p}$, the ring $B/\mathfrak{p}B$ can be seen as a finitely generated A/\mathfrak{p} -module: that is, $B/\mathfrak{p}B$ is a vector space over A/\mathfrak{p} of finite degree. And B/\mathcal{P}_i will be a field extension of A/\mathfrak{p} , each of some degree f_i . To see this last remark, we need to note that $\mathcal{P}_i \cap A = \mathfrak{p}$ so we can think of A/\mathfrak{p} as a subring of B/\mathcal{P}_i .

Proposition 23.1. *The primes \mathcal{P}_i are exactly those primes of B which restrict to \mathfrak{p} .*

Proof. $\mathcal{P} \mid \mathfrak{p}B \iff \mathfrak{p}B \subset \mathcal{P} \iff \mathcal{P} \cap A = \mathfrak{p}$. The last double arrow is clear in one direction, and in the other notice that \mathfrak{p} is maximal and $\mathcal{P} \cap A$ contains it but does not contain 1. □

We say that the \mathcal{P}_i lie over \mathfrak{p} . If $\mathfrak{p}B$ is prime, we say \mathfrak{p} is *inert*. If $\mathfrak{p}B$ has $e_i > 1$ for some i in its product, we say that \mathfrak{p} *ramifies*. If $\mathfrak{p}B$ is a product of n distinct primes, we say it *splits completely*. Other cases lie in between. The value e_i is called the *ramification index* and f_i is the *residual degree* of \mathcal{P}_i over A .

24. SPLITTING IN QUADRATIC FIELDS

It is very valuable at this point to work out an extended example. The student is encouraged to read the first part of what follows, i.e. the case of $\mathbb{Q}(\sqrt{d})$ where $d \equiv 2, 3 \pmod{4}$, and then work out the second part ($d \equiv 1 \pmod{4}$) in similar detail as an exercise and compare to what is here.

Consider the example $A = \mathbb{Z}$, so $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$, and $B = \mathbb{Z}[\alpha] = \mathcal{O}_L$. The primes of \mathbb{Z} are (p) for p a prime integer. And

$$\alpha = \begin{cases} \sqrt{d} & d \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod{4} \end{cases}$$

Let's consider the case $d \equiv 2, 3 \pmod{4}$ first. Here

$$\mathbb{Z}[\alpha]/(p)\mathbb{Z}[\alpha] \cong (\mathbb{Z}/p\mathbb{Z})[x]/(x^2 - d)$$

This is a field \mathbb{F}_{p^2} if d is not a square modulo p , and then $(p)\mathbb{Z}[\alpha]$ is prime.

If d is a square with two distinct roots, then suppose $d \equiv a^2 \pmod{p}$, so that $x^2 - d = (x - a)(x + a)$ and $a \not\equiv -a \pmod{p}$. This happens if and only if d is a quadratic residue mod p (in particular, non-zero mod p) and $p \neq 2$. Then by Chinese Remainder Theorem,

$$\begin{aligned} \mathbb{Z}[\alpha]/(p)\mathbb{Z}[\alpha] &\cong (\mathbb{Z}/p\mathbb{Z})[x]/((x - a)(x + a)) \\ &\cong ((\mathbb{Z}/p\mathbb{Z})[x]/(x - a)) \times (\mathbb{Z}/p\mathbb{Z})[x]/(x + a) \\ &\cong (\mathbb{Z}/p\mathbb{Z})^2 \end{aligned}$$

since $(x - a)$ and $(x + a)$ are relatively prime polynomials. Let a also represent any lift of $a \pmod{p}$ to the integers. Then, $(p, \alpha - a)$ and $(p, \alpha + a)$ are prime ideals whose norms are p (since the residue field of either is $\mathbb{Z}/p\mathbb{Z}$). Furthermore, they must be relatively prime, since $x - a$ and $x + a$ are relatively prime mod p (the condition for both statements is that $xp + y(\alpha - a) + z(\alpha + a) = 1$ has a solution in $x, y, z \in \mathbb{Z}[\alpha]$).

But their product $(p, \alpha - a)(p, \alpha + a)$ is contained in (p) since

$$(\alpha - a)(\alpha + a) \equiv \alpha^2 - d \equiv 0 \pmod{p}$$

So by comparing norms, it must be that

$$(p) = (p, \alpha - a)(p, \alpha + a).$$

If $a \equiv 0 \pmod{p}$ or if $p = 2$ and $a \equiv 1 \pmod{p}$, then we can't use CRT since the polynomial factors as a square of a linear polynomial $x^2 - d = (x + a)^2$. Then the quotient ring is

$$\mathbb{Z}[\alpha]/(p)\mathbb{Z}[\alpha] \cong (\mathbb{Z}/p\mathbb{Z})[x]/(x - a)^2,$$

which has a nilpotent and so is a new ring – neither \mathbb{F}_{p^2} nor $(\mathbb{Z}/p\mathbb{Z})^2$ – with a unique maximal ideal $(x - a)$, which has residue field $\mathbb{Z}/p\mathbb{Z}$. So there is a unique prime dividing (p) , and it has norm p :

$$(p) = (p, \sqrt{d} + a)^2.$$

(Again, a denotes any lift of $a \pmod p$ to the integers.)

Now we move on to the case $d \equiv 1 \pmod 4$. In this case, the ring of integers is $\mathbb{Z}[\alpha]$ where α satisfies $(2\alpha - 1)^2 - d = 0$ or $x^2 - x + \frac{d-1}{4} = 0$. The first case is when this is irreducible: this occurs if and only if d is not a square modulo p . In this case (p) is inert.

Suppose instead that d has two distinct square roots $\pm a$ modulo p . This happens unless $d \equiv 0 \pmod p$ and we ignore the case $p = 2$ for now. Then we have

$$x^2 - x + \frac{d-1}{4} = \left(x - \frac{1+a}{2}\right) \left(x + \frac{1-a}{2}\right)$$

As before, the Chinese Remainder Theorem gives

$$\mathbb{Z}[\alpha]/(p)\mathbb{Z}[\alpha] \cong (\mathbb{Z}/p\mathbb{Z})^2$$

and

$$(p) = \left(p, \alpha - \frac{1+a}{2}\right) \left(p, \alpha - \frac{1-a}{2}\right) = \left(p, \frac{\sqrt{d}-a}{2}\right) \left(p, \frac{\sqrt{d}+a}{2}\right).$$

(Importantly, note that here the notation $\frac{1+a}{2}$ denotes a lift to \mathbb{Z} .)

In the case that d has a single square root a of multiplicity two, i.e. $p \mid d$ and $a \equiv 0 \pmod p$ (we ignore the case $p = 2$ for now). Then

$$x^2 - x + \frac{d-1}{4} = \left(x - \frac{1-a}{2}\right)^2$$

In this case the quotient ring is

$$\mathbb{Z}[\alpha]/(p)\mathbb{Z}[\alpha] \cong (\mathbb{Z}/p\mathbb{Z})[x]/\left(x - \frac{1-a}{2}\right)^2 \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y)^2$$

And

$$(p) = \left(p, \alpha - \frac{1-a}{2}\right)^2.$$

Finally, we have to examine the case $p = 2$ separately. In this case, $x^2 - x + \frac{d-1}{4}$ is either $x(x + 1)$ if $d \equiv 1 \pmod 8$, or is the irreducible $x^2 + x + 1$ if $d \equiv 5 \pmod 8$. In the latter case, (2) is inert. In the former case, there are two distinct roots of the polynomial and we have

$$(2) = (2, \alpha)(2, \alpha + 1).$$

We will now summarise the result. Note that a *quadratic residue modulo p* is a non-zero square modulo p , and a *quadratic non-residue modulo p* is a non-zero non-square modulo p . The number 0 is neither a quadratic residue nor a quadratic non-residue.

Proposition 24.1. *Let p be a rational prime and let d be a squarefree integer. Let $K = \mathbb{Q}(\sqrt{d})$. Then*

- (1) *If d is a quadratic residue modulo p for $p \neq 2$, or if $p = 2$ and $d \equiv 1 \pmod{8}$, then $(p)\mathcal{O}_K$ is a product of two distinct primes (i.e. (p) splits).*
- (2) *If d is a quadratic non-residue modulo p for $p \neq 2$, or if $p = 2$ and $d \equiv 5 \pmod{8}$, then $(p)\mathcal{O}_K$ is prime (i.e. (p) is inert).*
- (3) *If $d \mid \text{disc}(K)$, then $(p)\mathcal{O}_K$ is a square of a prime (i.e. (p) ramifies).*

Let's check a few examples.

Example 24.2. *Suppose $d = 7 \equiv 3 \pmod{4}$. This is a principal ideal domain.*

Let $p = 5$. Then $d \equiv 2 \pmod{5}$ which is not a square, so (5) must be inert.

Let $p = 3$. Then $d \equiv 1 \pmod{3}$ which is a square with two roots: $\pm \pmod{3}$. So (3) should split where we can take a to be any integer not divisible by 3, for example, $a = 1$ and

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

Check for yourself that $(3, \sqrt{d} + a)$ depends only on the equivalence class of a modulo 3, and that the second equality holds.

Let $p = 7$. Then $d \equiv 0 \pmod{7}$ and so (7) must ramify with a any integer divisible by 7, for example

$$(7) = (7, \sqrt{d})^2 = (\sqrt{d})^2.$$

Check for yourself that $(7, \sqrt{d} - a)$ depends only on the equivalence class of a modulo 7 and that the second equality holds.

Let $p = 2$. Then $d \equiv 1 \pmod{2}$ and so (2) will ramify, and we can take a any odd integer, for example

$$(2) = (2, \sqrt{d} + 1)^2 = (\sqrt{d} + 3)^2.$$

Note that $\sqrt{d} + 1 = (\sqrt{d} + 3)(\sqrt{d} - 2)$.

Example 24.3. *Now let's consider $d = -83$. Then $d \equiv 1 \pmod{4}$. This is not a principal ideal domain. Its class number is 3.*

Let $p = 5$. Then $d \equiv 2 \pmod{5}$, which is a quadratic non-residue and so (5) is inert.

Let $p = 11$. Then $d \equiv 5 \pmod{11}$ and this is a quadratic residue with two roots $\pm a \equiv \pm 4 \pmod{11}$. Choose lifts $a = 15$ so that $\frac{1-a}{2} \in \mathbb{Z}$. Then

$$\begin{aligned} (11) &= \left(11, \frac{1-\sqrt{d}}{2} + 7\right) \left(11, \frac{1-\sqrt{d}}{2} - 8\right) \\ &= \left(11, \frac{4-\sqrt{d}}{2}\right) \left(11, \frac{4+\sqrt{d}}{2}\right). \end{aligned}$$

Let $p = 83$. Then (83) must ramify. According to our analysis, taking $a = 83$ in order that $\frac{1-83}{2} \in \mathbb{Z}$,

$$(83) = \left(83, \alpha - \frac{1-83}{2}\right)^2 = \left(83, \frac{83+\sqrt{d}}{2}\right)^2 = (\sqrt{d})^2.$$

Note that $\frac{1-\sqrt{d}}{2} \cdot \sqrt{d} = \frac{83+\sqrt{d}}{2}$.

Let $p = 2$. Then $d \equiv 1 \pmod{2}$ and $d \equiv 5 \pmod{8}$, so (2) is inert.

Example 24.4. Suppose $d = 17$ so that $d \equiv 1 \pmod{4}$ and $d \equiv 5 \pmod{8}$. Then (2) should split as

$$(2) = \left(2, \frac{1+\sqrt{d}}{2}\right) \left(2, \frac{1+\sqrt{d}}{2} + 1\right) = \left(\frac{1+\sqrt{d}}{2}\right) \left(\frac{3+\sqrt{d}}{2}\right).$$

Note: The 2's disappear since

$$\frac{1+\sqrt{d}}{2} \cdot \frac{3+\sqrt{d}}{2} = 2.$$

In fact, $\mathbb{Q}(\sqrt{17})$ is a principal ideal domain.

Example 24.5. Suppose we consider $d = 65$. Then $d \equiv 1 \pmod{4}$.

Let $p = 5$. Then since $5 \mid d$, (5) must ramify. Taking $a = 5$ in order that $\frac{1-5}{2} \in \mathbb{Z}$,

$$(5) = \left(5, \alpha - \frac{1-5}{2}\right)^2 = \left(5, \frac{5+\sqrt{d}}{2}\right)^2 = (5, \sqrt{d})^2.$$

Note that $\frac{1-\sqrt{d}}{2}\sqrt{d} + (-6)5 = \frac{5+\sqrt{d}}{2}$.

25. SPLITTING OF PRIMES – THE MAIN THEOREMS

One more quick example before we go on. Take $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{2}$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\alpha^3 - 2 = 0$.

Modulo 7, $x^3 - 2$ is irreducible, so (7) is inert in K/\mathbb{Q} ($n = 3, e_1 = 1, f_1 = 3$).

Modulo 29, $x^3 - 2 = (x + 3)(x^2 - 3x + 9)$ so $(29)\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$, $n = 3, e_1 = e_2 = 1, f_1 = 1, f_2 = 2$.

Modulo 31, $x^3 - 2 = (x - 4)(x - 7)(x + 11)$, so $(31)\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$, $n = 3, e_1 = e_2 = e_3 = 1, f_1 = f_2 = f_3 = 1$ and (31) splits completely.

Modulo 3, $x^3 - 2 = (x - 1)^3$, so $(3)\mathcal{O}_K = \mathcal{P}_1^3$ and $n = 3, e_1 = 3, f_1 = 1$, and the prime (3) ramifies in the extension.

These calculations are quick and easy because the ring of integers is monogenic. If $1, \alpha, \alpha^2$ generated only a non-maximal order in the number field, that what we calculated in this way is the splitting in the order, not in \mathcal{O}_K !

Notice that $3 \mid -108 = \text{disc}(K)$. We will shortly prove that the discriminant controls the ramification.

Theorem 25.1. *With the notation set up as usual, $B/\mathfrak{p}B$ is a field extension of A/\mathfrak{p} of degree n and*

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

Proof. We have a chain

$$B \supset \mathcal{P}_1 \supset \mathcal{P}_1^2 \supset \cdots \supset \mathcal{P}_q^{e_1} \supset \mathcal{P}_1^{e_1} \mathcal{P}_2 \supset \cdots \supset \mathcal{P}_1^{e_1} \cdots \mathcal{P}_q^{e_q} = \mathfrak{p}B.$$

There are no ideals strictly between any consecutive elements $I \supset I\mathcal{P}_i$ of this chain, since the \mathcal{P}_i are maximal and we can apply cancellation of ideals (cancel I) in a Dedekind domain. Each \mathcal{P}_i lies over \mathfrak{p} , thus we have that $I/I\mathcal{P}_i$ is a B -module with no proper submodules. It is also an B/\mathcal{P}_i -vector space (since \mathcal{P}_i annihilates it) still with no proper sub-modules (its module structures as a B -module and B/\mathcal{P}_i -module agree). So

$$I/I\mathcal{P}_i \cong B/\mathcal{P}_i$$

as B/\mathcal{P}_i -vector spaces. So $I/I\mathcal{P}_i$ is an A/\mathfrak{p} -vector space of dimension $[B/\mathcal{P}_i : A/\mathfrak{p}] = f_i$.

The total dimension of $B/\mathfrak{p}B$ over A/\mathfrak{p} is then the sum of the degrees of each inclusion in the sequence, i.e.

$$[B/\mathfrak{p}B : A/\mathfrak{p}] = \sum_{i=1}^q e_i f_i.$$

It remains to show the first statement of the theorem. We do it in two cases.

Case I: A is a principal ideal domain. Then B is a free A -module (as the integral closure). So there's a basis x_i for B/A . Claim: this

becomes a basis for $B/\mathfrak{p}B$ over A/\mathfrak{p} . Proof of claim: If we have some

$$\sum a_i x_i \in \mathfrak{p}B$$

for $a_i \in A$, then

$$\sum_i a_i x_i = \sum_j p_j x_j$$

for $p_j \in \mathfrak{p}$. Equating coefficients, by the fact that x_j is a basis, $a_i = p_i \in \mathfrak{p}$ for each i . The claim is proven, and so the first statement of the theorem holds in this case.

Case II: A is not a principal ideal domain. We will reduce to Case I. Let $S = A \setminus \mathfrak{p}$ which is a multiplicatively closed subset contains 1 but not 0. Set the notations:

$$A' = S^{-1}A, \quad B' = S^{-1}B.$$

The first of these is a PID since A is a Dedekind domain. The second of these is the integral closure of $S^{-1}A$ in L . So by Case I,

$$[B'/\mathfrak{p}B' : A'/\mathfrak{p}] = n$$

Since

$$\mathfrak{p}B = \prod_{i=1}^q \mathcal{P}_i^{e_i},$$

and extension of ideals preserves products, we also have

$$\mathfrak{p}B' = \prod_{i=1}^q (\mathcal{P}_i B')^{e_i}.$$

Each $\mathcal{P}_i B'$ is prime in B' since $\mathcal{P}_i \cap A = \mathfrak{p}$ is prime and disjoint from S . But we also have that

$$A'/\mathfrak{p}A' \cong A/\mathfrak{p}, \quad B'/\mathcal{P}_i B' \cong B/\mathcal{P}_i,$$

by Proposition 22.12. So by the first part,

$$\begin{aligned} n &= [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] \\ &= \sum_{i=1}^q e_i [B'/\mathcal{P}_i B' : A'/\mathfrak{p}A'] \\ &= \sum_{i=1}^q e_i [B/\mathcal{P}_i : A/\mathfrak{p}] \\ &= [B/\mathfrak{p}B : A/\mathfrak{p}] \end{aligned}$$

as required. □

It's helpful to illustrate the proof with an example.

$K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-5})$. Modulo 3, we have

$$x^2 + 5 = (x - 1)(x - 2),$$

so (3) splits in the extension.

Let $\mathfrak{p} = (3)$ and $A = \mathbb{Z}$, $B = \mathbb{Z}[\sqrt{-5}]$. Let $S = \mathbb{Z} \setminus (3)$. Then $A' = \mathbb{Z}_{(3)}$, and $B' = S^{-1}B = \mathbb{Z}_{(3)}[\sqrt{-5}]$. By a Proposition 22.12,

$$A'/(3)A' \cong \mathbb{Z}_{(3)}/(3)\mathbb{Z}_{(3)} \cong \mathbb{Z}/3\mathbb{Z}.$$

We can also calculate

$$\begin{aligned} B'/(3)B' &\cong \mathbb{Z}_{(3)}[\sqrt{-5}]/(3)\mathbb{Z}_{(3)}[\sqrt{-5}] \\ &= (\mathbb{Z}_{(3)}[x])/(3)/(x^2 - 1) \\ &= (\mathbb{Z}_{(3)}/(3)\mathbb{Z}_{(3)})[x]/(x^2 - 1) \\ &= (\mathbb{Z}/3\mathbb{Z})[x]/(x^2 - 1) \\ &= (\mathbb{Z}/3\mathbb{Z})^2 \\ &= B/(3)B \end{aligned}$$

Localising at a prime means “ignoring” the other primes and concentrating only on the relevant info – so we think of this as zooming in on a neighbourhood. There is a topological meaning to this which we'll get to soon.

Now we'll do an example with cyclotomic integers. Let p be a prime, r a positive integer. Let $\zeta = \zeta_{p^r}$, a primitive p^r -th root of unity. We will consider the field $K = \mathbb{Q}(\zeta)$. There are a total of $n = p^{r-1}(p - 1)$ primitive p^r -th roots, which we will call z_1, \dots, z_n . Recall that they are roots of the cyclotomic polynomial

$$\Phi_{p^r} = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + \dots + X^{p^{r-1}} + 1$$

Consider the ideals $I_i = (z_i - 1)$ in \mathcal{O}_K . These ideals are in fact all the same, since any z_j is some power of any other z_k . Thus,

$$z_j - 1 = z_k^q - 1 = (z_k - 1)(z_k^{q-1} + \dots + z_k + 1) \in I_k.$$

Now, consider the constant term of $\Phi_{p^r}(X + 1)$. On the one hand, it is p , but on the other, it is (up to sign) the product of the roots $z_j - 1$. Thus, we have

$$p\mathcal{O}_K = \prod_{i=1}^n I_i = I_1^n.$$

But $p\mathcal{O}_K$ must have a prime factorisation $\prod_{i=1}^q \mathcal{P}_i^{e_i}$. By unique factorisation, n divides each e_i and so

$$n \geq [K : \mathbb{Q}] = \text{a multiple of } n$$

Thus, the only possibility is $q = 1$, $e_1 = n$, $f_1 = 1$. We conclude that $n = [K : \mathbb{Q}]$ (in particular, Φ_{p^n} is irreducible), I_1 is of residual degree 1 and $p\mathcal{O}_K = I_1^n$ is the splitting of (p) . So p ramifies in this extension. Recall that $p \mid \text{disc}(K)$.

26. THE DISCRIMINANT AND RAMIFICATION

We need a number of lemmas before we prove that the discriminant governs the ramification of primes.

Lemma 26.1. *Let A be a ring and let $B = \prod_{i=1}^q B_i$ be a product of rings containing A which are also free finitely generated A -modules. Then*

$$\text{disc}(B/A) = \prod_{i=1}^q \text{disc}(B_i/A).$$

Proof. We show that case $q = 2$ and use that the induct for the general case. Let x_1, \dots, x_m be a basis for B_1 and y_1, \dots, y_n be a basis for B_2 over A . Then a basis for $B_1 \times B_2$ is

$$(x_1, 0), \dots, (x_m, 0), (0, y_1), \dots, (0, y_n).$$

But the product of $(x_i, 0)(0, y_j) = (0, 0)$ so $\text{disc}(B/A)$ is the determinant of a block diagonal matrix with $\text{disc}(B_1/A)$ and $\text{disc}(B_2/A)$ as its blocks. \square

Lemma 26.2. *Let $A \subset B$ be rings, and suppose that B is a free finitely generated A -module with basis x_1, \dots, x_n . Suppose that $I \subset A$ is an ideal. Write \bar{x} for the residue of $x \in B$ modulo I . Then \bar{x}_i form a basis of B/IB over A/I and $\text{disc}(\bar{x}_i) = \overline{\text{disc}(x_i)}$.*

Proof. The first statement is exactly as proven in the proof of $n = \sum e_i f_i$. Now, suppose $x \in B$. Then $m_x = (a_{ij})$, and $m_{\bar{x}} = (\bar{a}_{ij})$ in B/IB . Therefore $\text{Tr}(\bar{x}) = \overline{\text{Tr}(x)}$, which is all that is required. \square

Definition 26.3. *A ring A is reduced if it has no non-zero nilpotents.*

For example, $(\mathbb{Z}/p\mathbb{Z})^n$ and \mathbb{F}_p are reduced rings, but $(\mathbb{Z}/p\mathbb{Z})[x]/(x^2)$ is not, since $x^2 = 0$ in this ring.

Lemma 26.4. *In a reduced Noetherian ring A , $(0) = \cap_{i=1}^q P_i$ where P_i are prime and $q < \infty$.*

Proof. Since A is Noetherian, any ideal contains a finite product of primes. Since (0) is minimal as an ideal, it must equal any finite product of primes it contains. So

$$(0) = \prod_{i=1}^q P_i^{e_i}.$$

But suppose that $x \in \cap_{i=1}^q P_i$. Then $x^{e_1+\dots+e_n} \in (0)$. Since A is reduced, $x = 0$ and so

$$(0) = \cap_{i=1}^q P_i.$$

□

Don't forget that in any integral domain, such as \mathbb{Z} , the ideal (0) is prime, so this is trivially true for integral domains.

Consider the ring $A = (\mathbb{Z}/p\mathbb{Z})^2$, which is not an integral domain. Ideals are subgroups under addition, so there are only four candidates, which are in fact all ideals: (0) , $((1, 0))$, $((0, 1))$ and A . In fact, only the middle two of this list are prime. And, $(0) = ((1, 0))((0, 1)) = ((1, 0)) \cap ((0, 1))$.

Consider the ring $A = (\mathbb{Z}/p\mathbb{Z})[x]/(x^2)$. This ring is not reduced. The ideals are only (0) , (x) and A . Now $(0) = (x)^2$ but this is not $(x) \cap (x)$.

Lemma 26.5. *Let K be a field which is finite or of characteristic zero. Let L be a finite dimensional commutative K -algebra. Then L is reduced if and only if $\text{disc}(L/K) \neq 0$.*

Proof. Suppose that L is not reduced. Let $x \neq 0$ be a nilpotent element of L . Choose a basis for the vector space L/K which includes x , say

$$x = x_1, \dots, x_n.$$

Then $x_1 x_j$ is nilpotent and so $m_{x_1 x_j}$ is a nilpotent endomorphism. Thus its eigenvalues are 0 and its trace is 0. So $\text{disc}(L/K) = 0$ since the matrix $(\text{Tr}(x_i x_j))$ includes a zero row.

Conversely, suppose that L is reduced. Then $(0) = \cap_{i=1}^q P_i$ for some primes P_i . For each prime, L/P_i is in integral domain. Since K is a field, it sits naturally inside the K -algebra L , and does not intersect P_i . So L/P_i is still a K -algebra, and still finitely generated (the same elements will work). Thus L/P_i is an integral extension of K since it is finitely generated over K . Integral extensions of fields to integral domains are again fields. So L/P_i is a field and P_i is maximal.

Thus $P_i + P_j = L$ for $i \neq j$. Thus by the Chinese Remainder Theorem,

$$L \cong \prod (L/P_i)$$

and so

$$\text{disc}(L/K) = \prod \text{disc}((L/P_i)/K)$$

from a previous lemma, where the latter are all non-zero since they are discriminants of field extensions of finite fields or characteristic zero fields. \square

We will now extend the definition of the discriminant a little bit. Before, we had said that if A is a ring, and B is a free finitely generated A -module, then we can define the discriminant of a basis x_1, \dots, x_n for B over A . Then, up to squares of units, we can define the discriminant of B/A as the discriminant of this basis. However, we have seen that if L/K is an extension of number fields, then we have an extension of rings \mathcal{O}_L over \mathcal{O}_K , and \mathcal{O}_L is a submodule of a free finitely generated \mathcal{O}_K -module, but *may not be free* over \mathcal{O}_K if \mathcal{O}_K is not a principal ideal domain.

Definition 26.6. *The discriminant $\mathcal{O}_L/\mathcal{O}_K$ is the ideal $\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$ in \mathcal{O}_K generated by $\text{disc}(x_i)$ for all bases x_i of L over K which are contained in B .*

This definition agrees with the usual definition when \mathcal{O}_L is free over \mathcal{O}_K , since in that case any basis for L over K contained in \mathcal{O}_L is of the form $\sum a_{ij}w_i$ for an integral basis w_i and $a_{ij} \in \mathcal{O}_K$, and so $\text{disc}(x_i) = \det(a_{ij})^2 \text{disc}(w_i) \in (\text{disc}(w_i))$.

Also, since $\text{disc}(x_i) \neq 0$ for any basis of L/K , the ideal $\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$ is not the zero ideal.

Example 26.7. *Let $L = \mathbb{Q}(\sqrt{-7}, \sqrt{-14})$, $K = \mathbb{Q}(\sqrt{-14})$. The class group of K is $\mathbb{Z}/4\mathbb{Z}$, and in fact we will see that \mathcal{O}_L over \mathcal{O}_K has no relative integral basis (it's not free). Let's compute the discriminant. The sets*

$$\{1, \sqrt{2}\}, \quad \left\{1, \frac{1 + \sqrt{-7}}{2}\right\}$$

are bases of L/K which are contained in \mathcal{O}_L . We compute

$$\text{disc}(1, \sqrt{2}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = 8,$$

$$\text{disc}\left(1, \frac{1 + \sqrt{-7}}{2}\right) = \det \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix} = -7.$$

Since 8 and -7 are relatively prime in \mathcal{O}_K , we have found

$$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} = (1).$$

Note that in our usual setup (A a Dedekind domain, K its field of fractions, L a finite extension of K , B the integral closure of A in L),

a proper ideal I of A extends to a proper ideal IB of B . This fact is frequently useful. In particular it says that ideals are relatively prime in A if and only if their extensions are relatively prime in B .

Now, suppose that \mathcal{O}_L were free over \mathcal{O}_K . Then there would be a relative basis, w_1, w_2 . I claim that without loss of generality, we can assume that $w_1 = 1$. For, since w_1, w_2 is a basis, we can write

$$1 = aw_1 + bw_2$$

and so a and b are relatively prime in \mathcal{O}_L and so relatively prime in \mathcal{O}_K . So there exist c and d with $ad - bc = 1$. Thus, we can take the basis $1, \beta = cw_1 + dw_2$. So, it must be that

$$\mathcal{O}_L = \mathcal{O}_K[\beta] = \mathbb{Z}[\sqrt{-14}, \beta]$$

What form can β have? Note that $\mathbb{Q}(\sqrt{-14})$ has discriminant -56 and $\mathbb{Q}(\sqrt{-7})$ has discriminant -7 . Also

$$[\mathbb{Q}(\sqrt{-14}, \sqrt{-7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-14}) : \mathbb{Q}][\mathbb{Q}(\sqrt{-7}) : \mathbb{Q}].$$

So from a result from class,

$$\mathcal{O}_L \subset \frac{1}{7}\mathcal{O}_K\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$$

So the ring of integers is certainly contained in

$$\frac{1}{7}\mathbb{Z} \left[1, \sqrt{-14}, \frac{1 + \sqrt{-7}}{2}, \frac{\sqrt{-14} + \sqrt{2}}{2} \right].$$

We can apply the same argument with $\mathbb{Q}(\sqrt{2})$, which has discriminant 8 , telling us the ring of integers is in

$$\frac{1}{8}\mathbb{Z} \left[1, \sqrt{-14}, \sqrt{2}, \sqrt{-7} \right].$$

So we can assume that

$$\beta = a + b\sqrt{-14} + c\frac{\sqrt{2} + \sqrt{-14}}{2} + d\frac{1 + \sqrt{-7}}{2},$$

where $a, b, c, d \in \mathbb{Z}$. The extension L/K is of degree two and has one non-trivial Galois automorphism, σ , fixing K and taking $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{-7} \mapsto -\sqrt{-7}$.

Then,

$$\begin{aligned} \pm 1 &= \text{disc}(\mathcal{O}_L/\mathcal{O}_K) \\ &= \det \begin{pmatrix} \beta & \beta^\sigma \\ 1 & 1 \end{pmatrix}^2 \\ &= (\beta - \beta^\sigma)^2 \\ &= \left(2c \frac{\sqrt{2}}{2} + 2d \frac{\sqrt{-7}}{2} \right)^2 \\ &= (c\sqrt{2} + d\sqrt{-7})^2 \end{aligned}$$

i.e.

$$\pm 1 = 2c^2 - 7d^2 + 2cd\sqrt{-14}$$

from which we conclude that $cd = 0$ and so $1 = 2c^2$ or $1 = 7d^2$ both of which are impossible.

Theorem 26.8. *A non-zero prime \mathfrak{p} of A ramifies in B if and only if $\mathcal{D}_{B/A} \subset \mathfrak{p}$. In particular, there are only finitely many such \mathfrak{p} .*

Proof. The “in particular” statement follows from the fact that $\mathcal{D}_{B/A} \neq (0)$ (since it is generated by elements which are non-zero as discriminants of bases of the field L over K), and so it is a finite product of non-zero prime ideals.

The ring $B/\mathfrak{p}B$ has the form $\prod B/\mathcal{P}_i^{e_i}$ (from the Chinese Remainder Theorem, since \mathcal{P}_i is the only maximal ideal containing $\mathcal{P}_i^{e_i}$ and therefore $\mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j} = B$ for $i \neq j$). This has nilpotents if and only if $e_i > 1$ for some i (otherwise it is a direct product of fields). So \mathfrak{p} ramifies if and only if $B/\mathfrak{p}B$ is not reduced, which occurs if and only if $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$ according to the last lemma.

Now, if B were a free A -module, we could use one basis and the lemma that discriminants reduce. However, this isn’t necessarily the case unless we localise.

Let $S = A/\mathfrak{p}$. Let $A' = S^{-1}A$ which is a principal ideal domain, and $B' = S^{-1}B$ which is a free finitely generated A' module since it is the integral closure of a PID in an extension of the fraction field. So it has a basis e_1, \dots, e_n . Let $\mathfrak{p}' = \mathfrak{p}A$. Then we also have

$$A/\mathfrak{p} \cong A'/\mathfrak{p}', \quad B/\mathfrak{p}B \cong B'/\mathfrak{p}'B'.$$

Even stronger, the second isomorphism restricts to the first. This has the following consequence. Since the residues $\overline{e}_1, \dots, \overline{e}_n$ modulo \mathfrak{p} form a basis for $B/\mathfrak{p}B$ over A/\mathfrak{p} (we have seen this argument several times now), then in fact $B'/\mathfrak{p}'B'$ is a vector space over A'/\mathfrak{p}' with basis $\overline{e}_1, \dots, \overline{e}_n$ as well.

Therefore, $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$ as ideals in A/\mathfrak{p} if and only if $\mathcal{D}_{(B'/\mathfrak{p}'B')/(A'/\mathfrak{p}')} = (0)$ as ideals in A'/\mathfrak{p}' . The latter happens if and only if $\overline{\text{disc}(e_i)} = \text{disc}(\bar{e}_i) = 0$, i.e. $\text{disc}(e_i) \in \mathfrak{p}'$.

If we hadn't had to localise to ensure B was free over A , we'd be done. But it remains to show that $\text{disc}(e_i) \in \mathfrak{p}'$ if and only if $\mathcal{D}_{B/A} \subset \mathfrak{p}$.

For any basis x_i of L/K with $x_i \in B \subset B'$, we have $x_i = \sum a_{ij}e_j$ with $a_{ij} \in A'$ (since e_i form a basis for B' over A'). So

$$\text{disc}(x_i) = \det(a_{ij})^2 \text{disc}(e_i)$$

but $\text{disc}(x_i) \in A$, so if $\text{disc}(e_i) \in \mathfrak{p}'$, then $\text{disc}(x_i) \in A \cap \mathfrak{p}' = \mathfrak{p}$ for all such bases x_i .

Conversely, if $\mathcal{D}_{B/A} \subset \mathfrak{p}$, then write $e_i = y_i/s$ where $y_i \in B$ and $s \in S$. Then

$$\text{disc}(e_i) = s^{-2n} \text{disc}(y_i)$$

since the trace from B' down to A' is A' -linear and $1/s \in A'$. Therefore, $\text{disc}(e_i) \in A'\mathcal{D}_{B/A} \subset A'\mathfrak{p} = \mathfrak{p}'$. \square

27. QUADRATIC RECIPROCITY

This is perhaps a not completely inappropriate moment to catch up some famous elementary number theory: the theory of quadratic reciprocity. As we saw in the last section, for quadratic fields $\mathbb{Q}(\sqrt{d})$, the ramification of primes is determined by whether d is a quadratic residue mod p .

Definition 27.1. *Let p be an odd prime and d an integer not divisible by p . Then the Legendre symbol is the symbol*

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & d \text{ is a quadratic residue mod } p \\ -1 & d \text{ is a quadratic non-residue mod } p \end{cases}$$

In other words, the Legendre symbol is a composition

$$\mathbb{Z} \setminus p\mathbb{Z} \rightarrow \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \rightarrow \{\pm 1\}_{\text{mult}}$$

so

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

Proposition 27.2. *(Euler's Criterion) Let p be an odd prime, $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Proof. Let w be a primitive root modulo p . Then $a \equiv w^j \pmod p$ for some $0 \leq j \leq p-2$. Then

$$\left(\frac{a}{p}\right) = 1 \iff j \text{ is even.}$$

In other words,

$$\left(\frac{a}{p}\right) = (-1)^j.$$

The unique element of order 2 in \mathbb{F}_p^* is $w^{\text{frac}p-12} \equiv -1 \pmod p$. So

$$\left(\frac{a}{p}\right) \equiv w^{j\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod p.$$

□

The famous theorem of Quadratic Reciprocity is

Theorem 27.3. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

We also have the ‘Complementary Formulae.’

Theorem 27.4. *Let p be an odd prime. Then*

- (1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$
- (2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$

As an example, we can calculate whether 19 is a quadratic residue modulo 63 (these are both primes). We have

$$\begin{aligned} \left(\frac{19}{63}\right) &= (-1)^{\frac{62 \cdot 18}{4}} \left(\frac{63}{19}\right) = - \left(\frac{63}{19}\right) = - \left(\frac{6}{19}\right) = - \left(\frac{2}{19}\right) \left(\frac{3}{19}\right) \\ &= -(-1)^{\frac{18^2-1}{8}} \left(\frac{3}{19}\right) = -(-1)^{\frac{20 \cdot 18}{8}} \left(\frac{3}{19}\right) = \left(\frac{3}{19}\right) \\ &= (-1)^{\frac{18 \cdot 2}{4}} \left(\frac{19}{3}\right) = - \left(\frac{19}{3}\right) = - \left(\frac{1}{3}\right) = -1 \end{aligned}$$

Lemma 27.5. (*Eisenstein*) *Let p be an odd prime and q a positive integer coprime to p . Then*

$$\left(\frac{q}{p}\right) \equiv (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{2qn}{p} \right\rfloor} \pmod p.$$

Proof. Let $S = \{2, 4, 6, \dots, p-1\}$. Define $r(s)$ to be the least positive residue of qs . Then define $\phi : S \rightarrow S$ by $\phi(s) = (-1)^{r(s)}r(s)$. This takes values in S since whenever $r(s)$ is odd, $(-1)^{r(s)} = -1$ and $\phi(s) = -r(s)$ is even, while when $r(s)$ is even, $\phi(s) = r(s)$. Furthermore, ϕ is injective, since if $r(s) = r(s')$ then $qs \equiv \pm qs' \pmod{p}$ and so $s \equiv \pm s' \pmod{p}$. But s and s' are both even residues, so $s = s'$.

Thus, ϕ is a bijection and the product of the elements of S can be expressed two ways:

$$\prod_{n=1}^{\frac{p-1}{2}} 2n \equiv (-1)^{\sum_{n=1}^{\frac{p-1}{2}} r(2n)} \prod_{n=1}^{\frac{p-1}{2}} 2nq^{\frac{p-1}{2}} \pmod{p}.$$

Cancelling, we obtain

$$(-1)^{\sum_{n=1}^{\frac{p-1}{2}} r(2n)} \equiv q^{\frac{p-1}{2}} \pmod{p}.$$

But by definition

$$\frac{qs}{p} = \left\lfloor \frac{qs}{p} \right\rfloor + \frac{r(s)}{p}.$$

Considering the consequent equation $qs = \lfloor \frac{qs}{p} \rfloor p + r(s)$ modulo 2, one concludes that $\lfloor \frac{qs}{p} \rfloor$ is even if and only if $r(s)$ is even.

So

$$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \equiv (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{2qn}{p} \right\rfloor} \pmod{p}.$$

□

Proof. (Of Quadratic Reciprocity due to Eisenstein, using his lemma)

This proof requires a diagram which I am too lazy to code right now. I'll get around to this... maybe.... □

Proof. (Of complementary formulae)

The first formula is just Euler's criterion.

The second formula follows from the observation that the sum

$$\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{4n}{p} \right\rfloor$$

is equal to the number of even numbers x in the range $\frac{p+1}{2} \leq x \leq \frac{p-1}{2}$ (since the sum has a contribution from each such $n = x/2$; this can

be seen in a diagram similar to that of the proof of QR). This is $\frac{p-1}{4}$ if $\frac{p-1}{2}$ is even and $\frac{p+1}{4}$ otherwise (i.e. $\frac{p+1}{2}$ is even). But this is then $\frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}$. \square

We may as well extend the Legendre symbol for convenience. Extend it a bit and it's called the Jacobi symbol; extend a bit more and it's called the Kronecker symbol. First, one can reasonably define $\left(\frac{n}{p}\right) = 0$ whenever $p \mid n$. Then multiplicativity continues to hold. Because of quadratic reciprocity, it also makes sense to allow composite denominators and define $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right)$ etc.

We may as well also say for p an odd prime, that

$$\left(\frac{p}{2}\right) = (-1)^{\frac{p-1}{4}} \left(\frac{2}{p}\right)$$

which would extend the symbol to allow 2 in the bottom slot while preserving the quadratic reciprocity formula. From this we obtain

$$\left(\frac{p}{2}\right) = (-1)^{\frac{(p-1)^2(p+1)}{32}}$$

which is 1 if and only if $4 \mid \frac{p-1}{2}$ or $8 \mid \frac{p+1}{2}$. I'm interested in the case of $p \equiv 1 \pmod{4}$, which case $\frac{p+1}{2}$ is odd and we have

$$\left(\frac{p}{2}\right) = 1 \iff p \equiv 1 \pmod{8}.$$

One can check that this extends to composite n , thus

$$\left(\frac{n}{2}\right) = 1 \iff n \equiv 1 \pmod{8}.$$

One advantage of this language is that now the splitting of primes in a quadratic extension is particularly simply stated: p splits if $\left(\frac{D}{p}\right) = 1$, is inert if $\left(\frac{D}{p}\right) = -1$ and ramifies if $\left(\frac{D}{p}\right) = 0$.

I'll leave it as an exercise to work out the full generalisation to the Kronecker symbol preserving the appropriate properties.

28. AN EXAMPLE CLASS NUMBER FORMULA

Let's now consider the class number formula for quadratic extensions of \mathbb{Q} . Let $K = \mathbb{Q}(\sqrt{d})$ and let $D = \text{disc}(K)$ which, as you recall, is d if $d \equiv 1 \pmod{4}$ and $4d$ otherwise.

Recall the splitting of primes in a quadratic extension: if the prime p splits or ramifies, the primes above it have norm p ; otherwise p is inert

and the prime above it has norm p^2 . Then the Dedekind zeta function for K is

$$\begin{aligned}
\zeta_K(s) &= \prod_{P \subset \mathcal{O}_K} \left(1 - \frac{1}{N_{K/\mathbb{Q}}(P)^s}\right)^{-1} \\
&= \prod_{\left(\frac{D}{p}\right)=-1} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\left(\frac{D}{p}\right)=0} \left(1 - \frac{1}{p^s}\right)^{-1} \\
&= \prod_{\left(\frac{D}{p}\right)=-1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{D}{p}\right)=-1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\left(\frac{D}{p}\right)=0} \left(1 - \frac{1}{p^s}\right)^{-1} \\
&= \zeta(s) \prod_{\left(\frac{D}{p}\right)=-1} \left(1 + \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-1} \\
&= \zeta(s) L\left(\left(\frac{D}{\cdot}\right), s\right)
\end{aligned}$$

where

$$L\left(\left(\frac{D}{\cdot}\right), s\right) = \prod_p \left(1 - \frac{\left(\frac{D}{p}\right)}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{\left(\frac{D}{n}\right)}{n^s}.$$

The function L is a Dirichlet L -series. I'll completely ignore the analytic details here, and just say that the L -series is defined at $s = 1$ and

$$\operatorname{Res}_{s=1} \zeta_K = \operatorname{Res}_{s=1} \zeta(s) L(1).$$

The function $\chi(n) = \left(\frac{D}{n}\right)$ is an example of a *Dirichlet character* $\chi : \mathbb{Z} \rightarrow \mathbb{C}$.

Now recall the class number formula:

$$\operatorname{Res}_{s=1}(\zeta_K(s)) = \frac{2^{r_1} (2\pi)^{r_2} h_K r_K}{|\mu_K| \sqrt{|\operatorname{disc}(K)|}}.$$

In the case of $K = \mathbb{Q}$, this becomes

$$\frac{2 \cdot 1 \cdot 1 \cdot 1}{2 \cdot 1} = 1$$

Now consider the case where $K = \mathbb{Q}(i)$. We have $\operatorname{disc}(K) = -4$. For this field, the only units are easily shown to be $\pm 1, \pm i$, so $r_1 = 0$, $r_2 = 1$, $r_K = 1$, $|\mu_K| = 4$ and $\sqrt{|\operatorname{disc}(K)|} = 2$. We compute

$$L(1) = \operatorname{Res}_{s=1} \zeta_K = \frac{2\pi h_K}{8} = \frac{\pi}{4} h_K.$$

Thus, if we could compute $L(1)$, we could show compute h_K . But, then, leaving aside justifications for convergence etc.,

$$\begin{aligned} L(1) &= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots \\ &= \int_0^1 (1 - x^2 + x^4 - x^6 + \cdots) dx \\ &= \int_0^1 \frac{dx}{1 + x^2} = \frac{\pi}{4} \end{aligned}$$

which shows that $h_K = 1$.

Amazing. Note that in other circumstances the computation of $L(1)$ may be much more difficult but can be done numerically if the error can be bounded; it is an integer we are looking for!

29. GALOIS EXTENSIONS

With out usual setup (A, K, L, B) , suppose in addition for this section that L/K is Galois. Then it has a Galois group

$$\text{Gal}(L/K) = \{\sigma_i : L \rightarrow L, i = 1, \dots, n\}.$$

Each σ_i fixes K and it takes an algebraic integer to an algebraic integer (since it preserves coefficients of minimal polynomials over K , it preserves the algebraic relation of being an algebraic integer). Thus $\text{Gal}(L/K)$ is a ring isomorphism from B to itself when restricted, and as such it fixes elements of A inside B . Even better: it takes ideals to ideals and prime ideals to prime ideals. Since it fixes A , and every prime \mathcal{P} of B lies over exactly one prime \mathfrak{p} of A (contraction of ideals), $\sigma_i(\mathcal{P})$ also lies over \mathfrak{p} . Therefore, $\text{Gal}(L/K)$ acts on the set $\{\mathcal{P} : \mathcal{P} \cap A = \mathfrak{p}\}$.

We've already seen this. For example, every degree 2 extension of number fields is Galois. Suppose $K = \mathbb{Q}(i)$. In this case $\text{Gal}(K/\mathbb{Q}) = \{e, \sigma\}$, where e denotes the identity and $\sigma : i \mapsto -i$. Then

$$(5) = (1 + 2i)(1 - 2i)$$

and σ switches the two primes lying above (5).

In the case of $K = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_{p^r}$ is a primitive p^r -th root of unity, and p is an odd prime, then we recently calculated the prime decomposition

$$(p)\mathcal{O}_K = \mathcal{P}^{p^{r-1}(p-1)}$$

where $\mathcal{P} = (1 - \zeta)\mathcal{O}_K$. $\text{Gal}(K/\mathbb{Q})$ is the set of all σ_j where $\sigma_j : \zeta \mapsto \zeta^j$ and j is coprime to p . In this case σ_j takes \mathcal{P} to itself, since we saw that $(1 - \zeta^j)\mathcal{O}_K = (1 - \zeta)\mathcal{O}_K$.

Proposition 29.1. *The action of $\text{Gal}(L/K)$ on the \mathcal{P}_i lying above \mathfrak{p} is transitive, i.e. there exists a $\sigma \in \text{Gal}(L/K)$ such that $\sigma(\mathcal{P}_i) = \mathcal{P}_j$ for every i, j .*

Proof. Let h_L be the class number of the field L . Fix $1 \leq i \leq [L : K]$. Label the elements of $\text{Gal}(L/K)$ as $\sigma_1, \dots, \sigma_{[L:K]}$. Then $\mathcal{P}_i^{h_L} = (\beta)$ for some $\beta \in B$. Thus

$$N_{L/K}(\beta) = \prod_{l=1}^n \sigma_l(\beta) \in (\beta) \subset \mathcal{P}_i.$$

Since $N_{L/K}(\beta) \in A$, actually $N_{L/K}(\beta) \in \mathcal{P}_i \cap A = \mathfrak{p} \subset \mathcal{P}_j$ for all j .

Therefore, for each j , there exists some k so that $\sigma_k(\beta) \in \mathcal{P}_j$. Then

$$\sigma_k(\mathcal{P}_i)^{h_L} = (\sigma_k(\beta))B \subset \mathcal{P}_j$$

which implies that $\mathcal{P}_j \mid \sigma_k(\mathcal{P}_i)^{h_L}$. But this is only possible if $\mathcal{P}_j = \sigma_k(\mathcal{P}_i)$. \square

Theorem 29.2. *When L/K is Galois in usual setup, then the \mathcal{P}_i are all conjugate with $e_i = e_j = e$ and $f_i = f_j = f$. Thus*

$$\mathfrak{p} = \left(\prod_{i=1}^q \mathcal{P}_i \right)^e$$

and $n = efq$.

Proof. Each $\sigma \in \text{Gal}(L/K)$ preserves multiplication of ideals. Choosing a σ taking \mathcal{P}_i to \mathcal{P}_j , unique factorisation implies that $e_i = e_j$. Also, the isomorphism σ on B gives an isomorphism

$$B/\mathcal{P}_i \cong B/\sigma(\mathcal{P}_i)$$

so the residual degrees of conjugate primes agree, i.e. $f_i = f_j$. \square

Example 29.3. *All quadratic fields are Galois. There, the only decomposition of primes that is allowed is*

$$\mathfrak{p}B = \mathcal{P}, \quad \mathcal{P}_1\mathcal{P}_2, \quad \mathcal{P}^2$$

These are the only solutions to $2 = efq$.

Example 29.4. *In $K = \mathbb{Q}(\sqrt[3]{2})$, we can have $\mathfrak{p} = \mathcal{P}_1\mathcal{P}_2$. It is not Galois.*

Note that since $\text{Gal}(L/K)$ is a group acting on a set, the group falls into cosets of size ef taking \mathcal{P}_1 to \mathcal{P}_i (one for each $i = 1, \dots, q$). (These are the cosets of the subgroup of σ fixing \mathcal{P}_1 .)

Let's do a more extended example

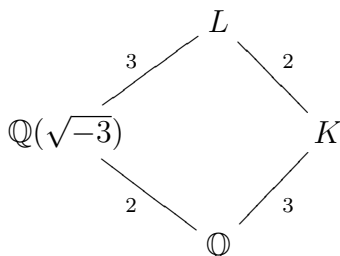
Example 29.5. Let $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Then L is Galois as an extension of K or of \mathbb{Q} . We can write

$$\text{Gal}(L/\mathbb{Q}) = \{e, \sigma_1, \sigma_2, \sigma_1^2, \sigma_1\sigma_2, \sigma_1^2\sigma_2\}.$$

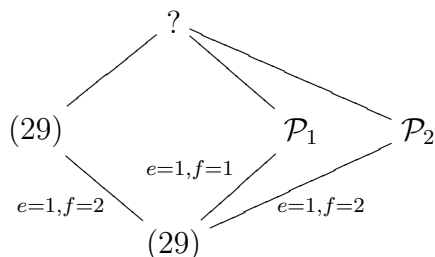
where

$$\sigma_1 : \begin{matrix} \sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{matrix}, \quad \sigma_2 : \begin{matrix} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{matrix}.$$

We have a diagram

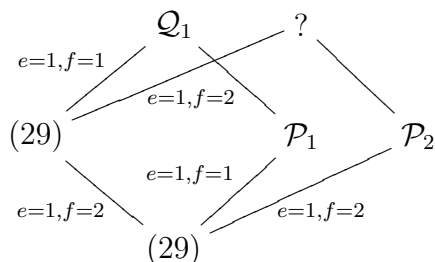


We know that (29) is inert in $\mathbb{Q}(\sqrt{-3})$ and is a product of two primes in K , so



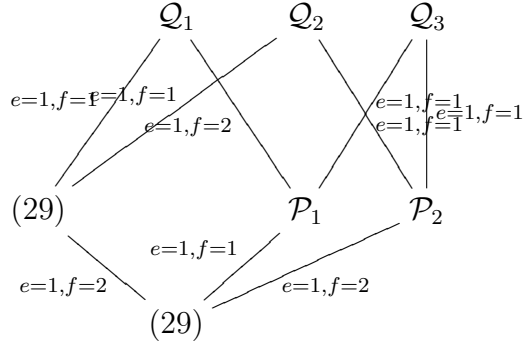
Our task is to sort out the ‘?’ in the diagram. First, any prime \mathcal{Q} up top has $1 \leq f_{L/\mathbb{Q}} \leq 4$ and by the left hand side and multiplicativity of residual degrees, $2 \mid f_{L/\mathbb{Q}}$. Of course, $1 \leq f_{L/K} \leq 2$.

So, if it lies over \mathcal{P}_1 , we see that $f_{L/K} = 2$, $f_{L/\mathbb{Q}(\sqrt{-3})} = 1$ and $f_{L/\mathbb{Q}} = 2$. Since the degree of the extension L/K is two, this means that \mathcal{Q} is the only prime over \mathcal{P}_1 , call it \mathcal{Q}_1 .



What about primes \mathcal{Q} over \mathcal{P}_2 ? A priori, perhaps \mathcal{P}_2 could be inert in the extension L/K . However, we know that L is Galois over \mathbb{Q} , and

so the primes \mathcal{Q} lying above (29) all have the same e 's and f 's. We already know this data: $e = 1, f = 2$. So in order that $efq = n = 6$, we have $q = 3$, i.e. \mathcal{P}_2 must split into two primes in the extension to L . Filling in the rest of the diagram, we have



(I have to find a way to squeeze in all those tags).

30. RELATIVE NORMS OF IDEALS

We now remove the general assumption that L/K is Galois and will mention each instance when it holds.

Definition 30.1. Suppose in our usual setup that \mathcal{P} lies above \mathfrak{p} . Then we define the norm of \mathcal{P} from L down to K as

$$N_{L/K}(\mathcal{P}) = \mathfrak{p}^{f_{L/K}(\mathcal{P})}$$

which is an ideal in A (note that $f_{L/K}(\mathcal{P})$ denotes the residual degree of \mathcal{P} over its contraction in K). Furthermore, for any ideal I of B such that $I = \prod_{i=1}^q \mathcal{P}_i^{e_i}$, we define

$$N_{L/K}(I) = \prod_{i=1}^q (\mathcal{P}_i \cap A)^{e_i f_{L/K}(\mathcal{P}_i)}$$

which is an ideal in A .

If this is going to be a good definition, it had better agree with the definition we gave earlier, which was that $N(I) = |A/I|$ (A a Dedekind domain and K its field of fractions). In fact,

$$N_{K/Q}(I) = (N(I)).$$

To see this, first verify this for primes P lying over $p \in \mathbb{Z}$, where $N(P) = p^f$ for $f = [A/P : \mathbb{Z}/p\mathbb{Z}]$. Then extend multiplicatively.

Note that if L/K is Galois, then

$$\prod_{\sigma \in \text{Gal}(L/K)} \sigma(\mathcal{P}) = \prod_{i=1}^q \mathcal{P}_i^{e_i f_i} = (\mathfrak{p}\mathcal{O}_K)^f = N_{L/K}(\mathcal{P})\mathcal{O}_K.$$

So the norm is still, in some sense, a product of conjugates (a sensible statement can be made for L/K not Galois also).

Example 30.2. Let $K = \mathbb{Q}(\sqrt{5})$ and $L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$. Then we have the picture

$$\begin{array}{ccc} L & \left(\frac{1-3\sqrt{5}}{2} \right) \left(\frac{1+3\sqrt{5}}{2} \right) & \\ \downarrow & \left| e_1=e_2=1, f_1=f_2=2 \right. & \\ K & \left(\frac{1-3\sqrt{5}}{2} \right) \left(\frac{1+3\sqrt{5}}{2} \right) & \\ \downarrow & \left| e_1=e_2=1, f_1=f_2=1 \right. & \\ \mathbb{Q} & (11) & \end{array} \tag{11}$$

From the homework, the e 's and f 's are multiplicative in extensions. So $e_1 = e_2 = 1$ and $f_1 = f_2 = 2$ for the full degree 4 extension. Call the upper primes \mathcal{P}_i in \mathcal{O}_L for $i = 1, 2$. We can calculate

$$\begin{aligned} N_{L/\mathbb{Q}}(\mathcal{P}_i) &= (11)^2\mathbb{Z} \\ N_{L/K}(\mathcal{P}_i) &= (\mathcal{P}_i \cap \mathcal{O}_K)^2\mathcal{O}_K \\ N_{K/\mathbb{Q}}(\mathcal{P}_i \cap \mathcal{O}_K) &= (11)^2\mathbb{Z} \end{aligned}$$

In the previous example one can verify the following.

Proposition 30.3. Let $F \subset K \subset L$ be a tower of number fields and \mathcal{P} a prime in \mathcal{O}_L . Then

$$N_{L/F}(\mathcal{P}) = N_{K/F}(N_{L/K}(\mathcal{P})).$$

Proof.

$$\begin{aligned} &N_{K/F}(N_{L/K}(\mathcal{P})) \\ &= N_{K/F}(\mathcal{P} \cap \mathcal{O}_K^{f_{L/K}(\mathcal{P})}) \\ &= \mathcal{P} \cap \mathcal{O}_F^{f_{L/K} \cdot f_{K/F}} \\ &= \mathcal{P} \cap \mathcal{O}_F^{f_{L/F}} \end{aligned}$$

□

31. THE DIFFERENT

For this section we have the usual setup: A is a Dedekind domain, K its field of fractions, L a separable extension and B the integral closure of A in L . We wish to consider the set

$$B^\vee = \{x \in L : \text{Tr}_{K/L}(xB) \subset A\}$$

In the next proposition we will show that this is a fractional ideal, and we will call its inverse the *different*, $\mathcal{D}if(L/K)$.

Proposition 31.1. *The different is an integral ideal.*

Proof. B^\vee is an A -module containing B . Let N be the module generated by a basis for L/K consisting of elements of B . Then let M be the A -module generated by a dual basis to this basis. Since $B \supset N$, then $M \supset B^\vee$. Since M is finitely generated, it is a fractional ideal and so B^\vee is a fractional ideal containing B . Thus its inverse is an integral ideal. \square

Note: Often B is a free A -module, so that B^\vee is the span of a dual basis to a basis of B over A .

Proposition 31.2. *Let $K \subset L \subset N$ be a tower of number fields with $A \subset B \subset C$ the respective rings of integers. Then*

$$\mathcal{D}if(N/K) = \mathcal{D}if(N/L)\mathcal{D}if(L/K).$$

Proof.

$$\begin{aligned} \alpha &\in \mathcal{D}if(N/K)^{-1} \\ &\iff \text{Tr}_{N/K}(\alpha\beta) \in A, \forall \beta \in C \\ &\iff \text{Tr}_{N/K}(\alpha\beta\gamma) = \text{Tr}_{L/K}(\gamma\text{Tr}_{N/L}(\alpha\beta)) \in A \forall \beta \in C, \gamma \in B \\ &\iff \text{Tr}_{N/L}(\alpha\beta) \in \mathcal{D}if(L/K)^{-1} \forall \beta \in C \\ &\iff \lambda \text{Tr}_{N/L}(\alpha\beta) = \text{Tr}_{N/L}(\alpha\lambda\beta) \in B \forall \beta \in C \gamma \in \mathcal{D}if(L/K) \\ &\iff \alpha\lambda \in \mathcal{D}if(N/L)^{-1} \forall \lambda \in \mathcal{D}if(L/K) \\ &\iff \alpha \in \mathcal{D}if(N/L)^{-1} \mathcal{D}if(L/K)^{-1} \end{aligned}$$

\square

We'll see in a moment that the different controls ramification and gives a little finer information than the discriminant. First let's see some examples.

Example 31.3. *Consider $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$. The trace pairing is*

$$\begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$$

By inspection, or by finding the inverse of this matrix, the dual basis is

$$1^\vee = \frac{1}{2}, \quad \sqrt{3}^\vee = \frac{1}{2\sqrt{3}}.$$

The inverse different is generated by these two numbers. Thus the different is the inverse ideal:

$$\mathcal{D}if(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = (2\sqrt{3})\mathbb{Z}[\sqrt{3}].$$

Now let's consider the splitting of some ideals. The ideal (2) splits as $(1 + \sqrt{3})^2$ and (3) splits as $(\sqrt{3})^2$. The different factors as

$$\mathcal{D}if = (\sqrt{3})(1 + \sqrt{3})^2.$$

In the last example, notice that the ideal norm of the different $(2\sqrt{3})$ down to \mathbb{Q} is (12), which is the discriminant. In fact, in general we have

$$N_{L/K}(\mathcal{D}if(L/K)) = \mathcal{D}_{L/K}.$$

In the case of $K = \mathbb{Q}$ this is particularly easy to see, since the ideal norm is the size of $\mathcal{O}_L/\mathcal{D}if$, which is the size of $\mathcal{D}if^{-1}/\mathcal{O}_L$, which is given by the determinant of the trace pairing.

Example 31.4. A slightly more complicated example now. Let α be such that $\alpha^3 - 9\alpha - 6 = 0$. The ring of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$, and this extension has trace pairing

$$\begin{pmatrix} 3 & 0 & 18 \\ 0 & 18 & 18 \\ 18 & 18 & 162 \end{pmatrix}$$

and discriminant $2^3 3^5$. To determine the splitting of primes, since this is a monogenic extension, we can look at the splitting of the minimal polynomial of α . We consider those primes that ramify (which we know from the discriminant).

Modulo 2: $x^3 - 9x - 6 \equiv x(x + 1)^2$. So (2) splits as a product $P_1 P_2^2$ where $P_1 = (26 + 2\alpha - 3\alpha^2)$ and $P_2 = (1 + \alpha)$.

Modulo 3: $x^3 - 9x - 6 \equiv x^3$. So (3) splits as P_3^3 where $P_3 = (3 + 5\alpha + \alpha^2)$.

In the case of a monogenic number field over \mathbb{Q} , the dual is fairly easy to compute:

$$\mathbb{Z}[\alpha]^\vee = \frac{1}{m'_{\alpha, \mathbb{Q}}(\alpha)} \mathbb{Z}[\alpha].$$

For example, this tells us that for $\mathbb{Q}(\sqrt{3})$, the different is $(m'(\alpha)) = 2\sqrt{3}$ (here, of course, the minimal polynomial is $x^2 - 3$). For our most

recent example, the different is $(3\alpha^2 - 9)$. This factors as

$$(3)(\alpha^2 - 3) = (3)(\alpha + 1)^2 = P_3^3 P_2^2$$

where, notice that $(\alpha + 1)^2 = (\alpha^2 + 2\alpha + 1) = (\alpha^2 + 3)$ since 2 is in the ideal.

In fact, the prime divisors of the different are exactly those primes which ramify *up above*; it carries somewhat more information about ramification than the discriminant, which lies *below*. The power of the prime divisors appearing in the discriminant is more subtle. We will not prove this, but in fact \mathcal{P} appears to power $e - 1$ in the different, where e is its index of ramification. This is the exact power unless the characteristic of the residue field divides e , in which case it could be higher.

We will prove the weaker statement which follows.

Theorem 31.5. *A prime \mathcal{P} ramifies over \mathfrak{p} if and only if $\mathcal{P} \supset \mathcal{D}if(L/K)$.*

The proof makes use of a small lemma.

Lemma 31.6.

$$\mathfrak{p}\{x \in L : Tr(xB) \subset A\} = \{y \in L : Tr(yB) \subset \mathfrak{p}\}.$$

Proof. Suppose y is in the second set. Then $Tr(\mathfrak{p}^{-1}yB) = \mathfrak{p}^{-1}Tr(yB) \subset \mathcal{O}_K$. So $\mathfrak{p}^{-1}y \in B^\vee$, which entails $y \in \mathfrak{p}B^\vee$.

Conversely, suppose that y is of the form $\sum p_i x_i$ where $p_i \in \mathfrak{p}$ and $x_i \in B^\vee$. Then $Tr((\sum p_i x_i)B) = \sum p_i Tr(x_i B) \subset \mathfrak{p}$. \square

Proof. (Proof of theorem) The proof consists of a chain of equivalences. Suppose that \mathfrak{p} splits as $\prod \mathcal{P}_i^{e_i}$, where $\mathcal{P} = \mathcal{P}_1$ and $e = e_1$.

\mathcal{P} ramifies over \mathfrak{p} if and only if the $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ -algebra $B_{\mathcal{P}}/\mathfrak{p}B_{\mathcal{P}}$ has nilpotents. This is so because in the extension of Dedekind domains $B_{\mathcal{P}}/A_{\mathfrak{p}}$, the prime \mathfrak{p} below splits as \mathcal{P}^e above.

This occurs if and only if the trace pairing of $B_{\mathcal{P}}/\mathfrak{p}B_{\mathcal{P}}$ down to $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is non-degenerate (also from previous results).

This occurs if and only if there exists some $x \neq 0$ such that $Tr(xB_{\mathcal{P}}/\mathfrak{p}B_{\mathcal{P}}) = 0$.

This occurs if and only if there exists some $x \notin \mathfrak{p}B_{\mathcal{P}}$ with $Tr(xB_{\mathcal{P}}) \subset \mathfrak{p}$ where now the trace is taken from $B_{\mathcal{P}}$ down to $A_{\mathfrak{p}}$.

This occurs if and only if there exists an $x \notin \mathfrak{p}B_{\mathcal{P}}$ which is however in $\mathfrak{p}B^\vee$ (by the lemma).

This occurs if and only if $\mathcal{D}if(B_{\mathcal{P}}/A_{\mathfrak{p}}) \neq (1)$.

This occurs if and only if $\mathcal{D}if(B_{\mathcal{P}}/A_{\mathfrak{p}}) \subset \mathcal{P}B_{\mathcal{P}}$.

This occurs if and only if $\mathcal{D}if(B/A) \subset \mathcal{P}$. This step is left as a homework exercise. \square

32. GALOIS EXTENSIONS, DECOMPOSITION, INERTIA

Suppose in addition to our usual setup that L/K is Galois.

Definition 32.1. *The decomposition group is the group*

$$D_{\mathcal{P}}(L/K) = \{\sigma \in \text{Gal}(L/K) : \sigma(\mathcal{P}) = \mathcal{P}\}.$$

We sometimes call the fixed field of the decomposition group the decomposition field, denoted $Z_{\mathcal{P}}(L/K)$.

For \mathcal{P}/\mathfrak{p} , we have the data q (number of conjugates), e (ramification index) and f (residual degree). Then

$$|D_{\mathcal{P}}| = n/q = ef.$$

Each $\sigma \in D_{\mathcal{P}}$ induces an automorphism of B/\mathcal{P} over A/\mathfrak{p} , call it $\bar{\sigma}$. The map $\sigma \mapsto \bar{\sigma}$ is a map from the decomposition group to the Galois group of B/\mathcal{P} over A/\mathfrak{p} , and its kernel is a normal subgroup of the decomposition group called the *inertia group*.

Definition 32.2. *The inertia group is the group*

$$I_{\mathcal{P}} = \{\sigma \in D_{\mathcal{P}} : \sigma(x) - x \in \mathcal{P} \forall x \in B\}.$$

Here's a simple but useful proposition.

Proposition 32.3. *Let $\sigma \in \text{Gal}(L/K)$. Then*

$$D_{\sigma(\mathcal{P})} = \sigma D_{\mathcal{P}} \sigma^{-1}, \quad I_{\sigma(\mathcal{P})} = \sigma I_{\mathcal{P}} \sigma^{-1}.$$

Proof. For the first statement, for $\tau \in D_{\mathcal{P}}$, we have

$$\sigma \tau \sigma^{-1}(\sigma(\mathcal{P})) = \sigma \tau(\mathcal{P}) = \sigma(\mathcal{P}).$$

from which we have $\sigma D_{\mathcal{P}} \sigma^{-1} \subset D_{\sigma(\mathcal{P})}$. Exactly similarly, $D_{\mathcal{P}} \supset \sigma^{-1} D_{\sigma(\mathcal{P})} \sigma$, from which the equality follows.

For the second statement, for $\tau \in I_{\mathcal{P}}$, for all $x \in B$,

$$\sigma \tau \sigma^{-1}(x) - x = \sigma(\tau \sigma^{-1}(x) - \sigma^{-1}(x)) \in \sigma(\mathcal{P})$$

from which we deduce that $\sigma I_{\mathcal{P}} \sigma^{-1} \subset I_{\sigma(\mathcal{P})}$. Exactly similarly, we deduce that $\sigma^{-1} I_{\sigma(\mathcal{P})} \sigma \subset I_{\mathcal{P}}$. \square

Note that if L/K is abelian, these results imply that $D_{\sigma(\mathcal{P})} = D_{\mathcal{P}}$ and $I_{\sigma(\mathcal{P})} = I_{\mathcal{P}}$.

It will be helpful to begin a running example as we work through this section. We will use an example we studied when talking about Galois extensions at ramification a couple sections previous. Let $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. The Galois group is isomorphic to S_3 :

$$G = \text{Gal}(L/\mathbb{Q}) = \{e, \sigma_1, \sigma_2, \sigma_1^2, \sigma_1\sigma_2, \sigma_1^2\sigma_2\}.$$

where

$$\sigma_1 : \begin{array}{l} \sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{array}, \quad \sigma_2 : \begin{array}{l} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{array}.$$

The prime (29) splits as a product $Q_1 Q_2 Q_3$. The prime (29) splits as $P_1 P_2$ in $\mathbb{Q}(\sqrt[3]{2})$, where the residual degrees are 1 and 2 respectively. So we label the Q_i 's such that Q_1 lies over P_1 and Q_2 and Q_3 lie over P_2 . Then, the decomposition group D_{Q_1} is of order $2 = ef$ and so must be one of the three groups $\langle \sigma_2 \rangle$, $\langle \sigma_1 \sigma_2 \rangle$, or $\langle \sigma_1^2 \sigma_2 \rangle$. Now, since Q_1 must map to itself under any automorphism fixing $\mathbb{Q}(\sqrt{3})$ (since it lies over P_1), the first of these is D_{Q_1} , while the others are the conjugate subgroups $D_{\sigma_1(Q_1)}$ and $D_{\sigma_1^2(Q_1)}$ in some order.

The prime (3) ramifies in the extension L/K , and in fact it splits completely as Q_4^6 . Thus, its decomposition group must be all of G . This is the only prime carrying ramification in L/K since the discriminant of the field is -3^{11} .

Theorem 32.4. *Suppose that A/\mathfrak{p} is finite or characteristic zero. Then B/\mathcal{P} is a Galois extension of A/\mathfrak{p} of degree f and the map $D_{\mathcal{P}} \rightarrow \text{Gal}((B/\mathcal{P})/(A/\mathfrak{p}))$ given by $\sigma \mapsto \bar{\sigma}$ is surjective.*

Note that this implies that the kernel is of size e and in particular, \mathcal{P}/\mathfrak{p} is unramified if and only if $I_{\mathcal{P}}$ is trivial.

Before we proceed to the proof, let us go back to our example. The inertia groups I_{Q_i} for $i = 1, 2, 3$ are trivial, since (29) is unramified. This means that D_{Q_1} is isomorphic to the Galois group of \mathcal{O}_L/Q_1 over $\mathbb{Z}/29\mathbb{Z}$, which is of degree 2. That is σ_2 maps to the Frobenius element generating this extension, $\sigma_2(x) \equiv x^{29} \pmod{Q_1}$ (we will discuss this more after the proof of the theorem).

The inertia group I_{Q_4} is the kernel of $\sigma \mapsto \bar{\sigma}$. Since f is 1, this means I_{Q_4} is all of G .

Proof. We have the following setup:

$$\begin{array}{ccccc} L & & B & & \mathcal{P} \\ | & & | & & | \\ \mathbb{Z}_{\mathcal{P}} & & A_D = B \cap \mathbb{Z}_{\mathcal{P}} & & \mathfrak{p}_D \\ | & & | & & | \\ K & & A & & \mathfrak{p} \end{array}$$

The values e and f denote the ramification index and residual degree of \mathcal{P} over \mathfrak{p} , while e' and f' denote those values for \mathcal{P} over \mathfrak{p}_D . By the setup, \mathcal{P} is the only prime lying over \mathfrak{p}_D . So $e'f' = |D_{\mathcal{P}}| = ef$ but in towers it must be that $e' \leq e, f' \leq f$. So $e = e', f = f'$.

We have an identification of A/\mathfrak{p} as a subfield of A_D/\mathfrak{p}_D , and this must be of degree 1. Hence they are isomorphic. The extension B/\mathcal{P} over A/\mathfrak{p} is of degree f , and we wish to show that it is Galois.

Let $x \in B$ be such that $\bar{x} \in B/\mathcal{P}$ is a primitive element for the extension B/\mathcal{P} over A/\mathfrak{p} . Let the minimal polynomial of x be $P(X)$ over K_D : then its roots are $\sigma(x)$ as σ ranges over $D_{\mathcal{P}}$, which is the Galois group of L/K_D . Thus, the reduced polynomial $\bar{P}(X)$ taking coefficients in $A_D/\mathfrak{p}_D \cong A/\mathfrak{p}$ has roots $\bar{\sigma}(\bar{x})$, which are all in B/\mathcal{P} (since σ ranges over $D_{\mathcal{P}}$). Hence the extension B/\mathcal{P} over A/\mathfrak{p} is Galois, and its Galois group is $D_{\mathcal{P}}/I_{\mathcal{P}}$ (the group of $\bar{\sigma}$). \square

33. FINITE FIELDS

Here's the story of finite fields. I won't break it all up into separate propositions, but I'll highlight the important statements in bold.

If K is a finite field, then it has prime characteristic. The characteristic must be finite, by pigeonhole principle, and if 1 has additive order n , where $p \mid n$ but $p \neq n$ for some prime p , then n/p has additive order p and so it is a zero divisor ($p \cdot (n/p) = 0$), which cannot exist in a field.

Thus, the additive cyclic group generated by 1 is $\mathbb{Z}/p\mathbb{Z}$ for some prime p and this is in fact a subfield of K . Hence K is a field extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of some degree k . Then it must have p^k elements. So **all finite fields are of cardinality a prime power.**

The polynomial $X^q - X$ for $q = p^k$ has no repeated roots in any extension of \mathbb{F}_p since its derivative is -1 (remember we are working in characteristic p).

Now we show that **any finite subgroup G of K^* for any field K is cyclic.** For, let n be the least common multiple of the orders of the elements (which must all be finite). Then there exists an element of order n (this is a result for finite abelian groups), call it g_0 . The subgroup generated by g_0 has order n , but all elements of G satisfy $x^n - 1$ and hence there are at most n elements of G (any polynomial over a field has at most a number of roots equal to its degree). Thus G is the cyclic group generated by g_0 .

Let $q = p^k$ and let L be any field in which $X^q - X$ splits over $\mathbb{Z}/p\mathbb{Z}$. Let $\phi(x) = x^q$ be a map on L . Then $\phi(ab) = \phi(a)\phi(b)$. Also, since the characteristic p will divide the intermediate terms of a binomial expansion, $(a + b)^p = a^p + b^p$ and consequently, by composition of this result, $\phi(a + b) = \phi(a) + \phi(b)$. Thus ϕ is an automorphism of L . The roots of $X^q - X$ are the elements fixed by ϕ , which is a subfield K of order q . But then $|K^*| = q - 1$ and so all elements of K satisfy

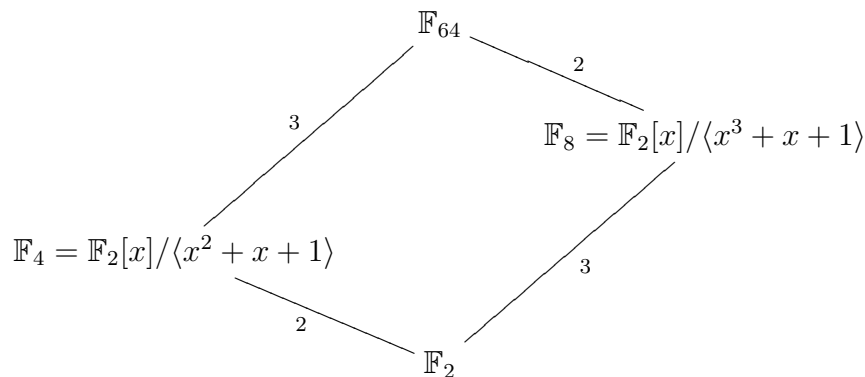
$X^q - X$. Hence **the splitting field of $X^q - X$ consists of the set of its roots.**

In fact, **all fields of size $q = p^k$ are isomorphic.** For, suppose there were two such fields, K and K' , both considered as extensions of \mathbb{F}_p . Then their multiplicative groups are both cyclic. Let $K^* = \langle \alpha \rangle$. Then $K = \mathbb{F}_p(\alpha)$ where α has some minimal polynomial $f(X)$. Since f is irreducible and $\alpha^q = \alpha$, necessarily $f(X) \mid X^q - X$. Since $X^q - X$ factors in K' , f has a root $\alpha' \in K'$. So $K' \supset \mathbb{F}_p(\alpha') = \mathbb{F}_p(\alpha) = K$. But their cardinalities are equal, so $K' = K$.

Now, we have seen that the field \mathbb{F}_q of size $q = p^k$ is the splitting field of any irreducible polynomial of degree k over \mathbb{F}_p . Thus it is Galois over \mathbb{F}_p . Now consider any finite field extension \mathbb{F}_{q^n} over \mathbb{F}_q (this has degree n). Then $\phi : x \mapsto x^q$ is an automorphism of \mathbb{F}_{q^n} . So $\phi \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_p)$ and so it generates a subgroup $H = \langle \phi \rangle$. The subgroup is necessarily normal and its fixed field is \mathbb{F}_q , so the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois with Galois group H . The map ϕ is a canonical choice of generator called the *Frobenius*.

Finally, \mathbb{F}_{q^n} **has a subfield \mathbb{F}_{q^r} if and only if $r \mid n$.** By the degree condition on field extensions, r must divide n . Now suppose that $r \mid n$. Then $q^r - 1 \mid q^n - 1$ and so $X^{q^r} - X \mid X^{q^n} - X$. In fact, this shows $X^q - X$ factors as all irreducible polynomials of degree dividing n .

As an example, we may have the fields



Don't fall into the trap of thinking that \mathbb{F}_4 is a subfield of \mathbb{F}_8 because $4 \mid 8$: instead, what's relevant is that $2 \nmid 3$!

34. DECOMPOSITION IN NUMBER FIELDS

In the case of number fields, B/\mathcal{P} over A/\mathfrak{p} is an extension of finite fields and the last theorem applies. Extensions of finite fields are cyclic with generator $\bar{\sigma} : \bar{x} \mapsto \bar{x}^q$ where $q = |A/\mathfrak{p}|$, the so-called *Frobenius*. Thus $\text{Gal}((B/\mathcal{P})/(A/\mathfrak{p})) = \langle \bar{\sigma} \rangle$.

If, furthermore, \mathcal{P} is unramified over \mathfrak{p} , then $D_{\mathcal{P}} = \langle \sigma \rangle$, $I_{\mathcal{P}} = \langle id \rangle$, where $\sigma(x) \equiv x^q \pmod{\mathcal{P}}$, the *Frobenius of \mathcal{P}* , denoted $(\mathcal{P}, L/K)$.

If L/K is abelian (which is to say, its Galois group is abelian), then $(\mathcal{P}, L/K)$ depends only on \mathfrak{p} of A , i.e. $(\tau(\mathcal{P}), L/K) = (\mathcal{P}, L/K)$. In this case, we write

$$\left(\frac{L/K}{\mathfrak{p}} \right)$$

which should remind you of the Legendre symbol. It's called the Artin symbol.

As an example, let $L = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}$. Then $\left(\frac{L/K}{p} \right)$ is trivial if and only if $f = 1$ for the prime p , i.e. p splits. If p ramifies, it is an element of order 2. Thus, it agrees with the usual Legendre symbol, if we identify the Frobenius of a degree 2 extension with -1 and the identity map with 1. This is the beginning of a vast generalisation of the ideas of quadratic reciprocity.

Proposition 34.1. *Consider the tower of number fields*

$$\begin{array}{ccc} L & \mathcal{O}_L & \mathcal{P} \\ | & | & | \\ F & \mathcal{O}_F & \mathfrak{p}' \\ | & | & | \\ K & \mathcal{O}_K & \mathfrak{p} \end{array}$$

Suppose that \mathcal{P} is unramified over \mathfrak{p} . Let e and f be the ramification index and residual degree of \mathfrak{p}' over \mathfrak{p} . Then

- (1) $(\mathcal{P}, L/F) = (\mathcal{P}, L/K)^f$
- (2) If F/K is Galois, then $(\mathcal{P}, L/K)$ restricted to F is $(\mathfrak{p}', F/K)$.

Proof. Part a) first. Use the notation $\sigma := (\mathcal{P}, L/K)$. Then $D_{\mathcal{P},F}$ is a subgroup of $D_{\mathcal{P},K}$ of index f , since

$$|D_{\mathcal{P},F}| = [\mathcal{O}_L/\mathcal{P} : \mathcal{O}_F/\mathfrak{p}'] = 1/f[\mathcal{O}_L/\mathcal{P} : \mathcal{O}_K/\mathfrak{p}] = 1/f|D_{\mathcal{P},K}|$$

Since $D_{\mathcal{P},K}$ is cyclic, this subgroup must be the unique subgroup of this size, i.e. $\langle \sigma^f \rangle$. Now, $\sigma^f(x) \equiv x^{q^f} \pmod{\mathcal{P}}$ since $\sigma^f(\mathcal{P}) = \mathcal{P}$, and $q^f = |\mathcal{O}F/\mathfrak{p}|$, so σ^f is the canonical generator $(\mathcal{P}, L/F)$.

For the second part b), write σ' for the restriction, and note that $\sigma'(\mathfrak{p}') = \mathfrak{p}'$, so $\sigma'(x) \equiv x^q \pmod{\mathfrak{p}'}$. □

Theorem 34.2. (1) No prime not dividing n ramifies in $\mathbb{Q}(\zeta_n)$.
 (2) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.

In this proof we do not assume that we know the degree of the extension. Instead, that is derived with the proof (hence the proof is another proof of the irreducibility of the cyclotomic polynomial). The proof itself will be useful when we prove quadratic reciprocity immediately afterward.

Proof. Part a). This was a homework exercise. Part b). First, note that the extension is Galois since all the other primitive n -th roots are in the extension. Let $G = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Each $\sigma \in G$ is determined by the equation

$$\sigma(\zeta_n) = \zeta_n^{j(\sigma)}$$

for some $j(\sigma)$. In fact, we have a homomorphism

$$j : G \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

which is injective.

Now, take $p \nmid n$. By part a), the Frobenius $\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p}\right)$ is defined, call it σ_p . Then let $j = j(\sigma_p)$. Let \mathcal{P} be a prime lying over p and we have

$$\sigma_p(x) \equiv x^p \pmod{\mathcal{P}}$$

for all x in the ring of integers. So

$$\zeta_n^j \equiv \zeta_n^p \pmod{\mathcal{P}}$$

Letting $P(X) = X^n - 1$, we obtain

$$n\zeta_n^{p(n-1)} = P'(\zeta_n^p) = \prod_{\substack{0 \leq r \leq n-1 \\ r \not\equiv p \pmod{n}}} (\zeta_n^p - \zeta_n^r)$$

by differentiation and substitution. But since $p \nmid n$, then $\mathcal{P} \nmid n(\zeta_n^{p(n-1)})$ (examine the norm). Hence there are no multiple roots and so $\zeta_n^p \equiv \zeta_n^j \pmod{\mathcal{P}}$ must imply that $p = j \pmod{n}$.

This tells us that the map j is surjective (since it hits every residue class of primes mod n , which is all those in $(\mathbb{Z}/n\mathbb{Z})^*$). \square

Theorem 34.3. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

Proof. Let $K = \mathbb{Q}(\zeta_q)$. The Galois group $G = \text{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_q^*$ is of even order with a unique subgroup of index 2 consisting of all squares $(\mathbb{F}_q)^2 < \mathbb{F}_q$. Thus there is a unique quadratic field F/\mathbb{Q} contained in K . No prime $p \neq q$ ramifies in F since otherwise it would ramify in K , but by the previous proposition, this only occurs if $p \mid q$. Thus, F must have

discriminant divisible only by q , hence if we put $q^* = (-1)^{\text{frac}q-1}q$, then

$$F = \mathbb{Q}(\sqrt{q^*}) = \begin{cases} \mathbb{Q}(\sqrt{q}) & q \equiv 1 \pmod{4} \\ \mathbb{Q}(\sqrt{-q}) & q \equiv 3 \pmod{4} \end{cases}$$

Now, let $p \neq q$ be the other prime. Let $\sigma_p = \left(\frac{K/\mathbb{Q}}{p}\right)$ be the Frobenius. Restricting this to F , we get

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \begin{cases} id & \sigma_p \in H, \text{ i.e. } j(\sigma_p) \text{ a QR} \pmod{q} \\ non - id & \text{otherwise} \end{cases}.$$

If we label $\text{Gal}(F/\mathbb{Q}) \cong G/H$ as $\{\pm 1\}$, then this is exactly the Legendre symbol

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right).$$

But equally well, we have

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \begin{cases} id & p \text{ splits in } F \\ non - id & p \text{ is inert} \end{cases}$$

So if p is odd, then

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \left(\frac{q^*}{p}\right).$$

So

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$$

while $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ from which the result follows. □

The complementary formula is proven similarly, based on the proof up to the assumption that p is odd near the end. The prime $p = 2$ splits in F if and only if $q^* \equiv 1 \pmod{8}$, and is inert in the other case: $q^* \equiv 5 \pmod{8}$. But then

$$(-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{q^*2-1}{8}} = \begin{cases} 1 & q^* \equiv 1 \pmod{8} \\ -1 & q^* \equiv 5 \pmod{8} \end{cases}$$

So

$$\left(\frac{2}{q}\right) = \left(\frac{F/\mathbb{Q}}{2}\right) = (-1)^{\frac{q^2-1}{8}}.$$

If this appeals to you, learn class field theory!

35. P-ADIC NUMBERS

In this section, I am essentially following Neukirch's Algebraic Number Theory, Chapter II. He gives quite a nice explanation, and somewhat more leisurely.

Think of an integer, suggestively named $f \in \mathbb{Z}$, as a function on the primes of \mathbb{Z} : the 'value' $f(p)$ of f and a prime p is the residue modulo p in \mathbb{F}_p . This is a strange sort of function: its domain is always changing! This idea, however, is the first step in unifying the study of algebraic number fields and curves. The primes in a ring of algebraic integers are the 'points' in the geometric perspective. We'll talk more about this soon.

In this view that integers are functions, what about the derivative? That question can be thought of as the source of the *p-adic numbers*.

Returning to the case of $f(z) \in \mathbb{C}[z]$, if we expand $f(z)$ in terms of $(z - a)$:

$$f(z) = a_0 + a_1(z - a) + \dots + a_n(z - a)^n,$$

the coefficients contain the information of the derivatives of f at a . Similarly for $f(z)/g(z)$ where $(z - a) \nmid g(z)$: it has a Taylor expansion. Notice that the ideals $(z - a)$ are the non-zero primes for $\mathbb{C}[z]$.

For $f \in \mathbb{Z}$, we can always write

$$f = a_0 + a_1p + \dots + a_np^n$$

where $0 \leq a_i < p$. And if $f/g \in \mathbb{Z}_{(p)}$, i.e. $p \nmid g$, then we have an expansion also. For example,

$$\frac{-1}{4} = \frac{1}{1-5} = 1 + 5 + 5^2 + \dots$$

We wish to collect together the formal infinite series

$$a_0 + a_1p + \dots$$

where $0 \leq a_i < p$. The name of this collection is \mathbb{Z}_p , the *p*-adic integers. Exercise for the reader (do it now!): any $f \in \mathbb{Z}_{(p)}$ determines such a sequence by its successive residues modulo p^n .

More generally, a *p-adic number* is like a Laurent series: a formal infinite series

$$\sum_{v=m}^{\infty} a_v p^v$$

where $m \in \mathbb{Z}$ (possibly negative!) and $0 \leq a_i < p$. We'll call this collection \mathbb{Q}_p .

Now any $a/b \in \mathbb{Q}$ determines a unique such sequence, by writing $a/b = (a'/b')p^m$ where $a'b'$ is relatively prime to p .

Thus we identify \mathbb{Q} with a subset of \mathbb{Q}_p and the identification restricts to an identification of \mathbb{Z} with a subset of $\mathbb{Z}_p \subset \mathbb{Z}_p$. Another example:

$$-1 = (p - 1) + (p - 1)p + (p - 1)p^2 + \dots$$

The right way to think of this is as a projective limit. Any $s = \sum_{v=0}^{\infty} a_v p^v \in \mathbb{Z}_p$ determines and is determined by a sequence of residues $s_n \in \mathbb{Z}/p^n\mathbb{Z}$ such that

$$s_n \equiv s \pmod{p^n}$$

i.e.

$$s_n \equiv \sum_{v=0}^{n-1} a_v p^v \pmod{p^n}$$

There are canonical projections

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} \dots$$

such that $\lambda_n(s_{n+1}) = s_n$.

The more general definition is as follows:

Definition 35.1. Let A_i be a collection of rings indexed by a poset I . Suppose that for every $i \leq j$ there is a homomorphism

$$\lambda_{ij} : A_j \rightarrow A_i$$

and the collection is such that λ_{ii} is the identity, and $\lambda_{ik} = \lambda_{ij} \circ \lambda_{jk}$. Then the projective limit (or inverse limit)

$$\lim_{\leftarrow n} A_i$$

is the subset of $\prod_I A_i$ of (x_i) such that $x_i = \lambda_{ij}(x_j)$. This is naturally a ring.

The canonical projections for all $\mathbb{Z}/p^n\mathbb{Z}$ actually determine $\lambda_{ij} : \mathbb{Z}/p^j\mathbb{Z} \rightarrow \mathbb{Z}/p^i\mathbb{Z}$ in an obvious way. We have observed the following:

Proposition 35.2. We have a bijection $\mathbb{Z}_p \cong \lim_{\leftarrow n} \mathbb{Z}/p^n\mathbb{Z}$.

This gives \mathbb{Z}_p a ring structure. Extending the operations to \mathbb{Q}_p (since these are just ‘translates’ to the left) gives a ring structure there also. The restrictions to \mathbb{Z} and \mathbb{Q} agree with the usual rings structure of these rings.

Why are the p -adics useful? By Chinese Remainder Theorem, the study of solutions of equations modulo any m can be reduced to the study modulo powers of primes. The p -adics carry this information.

Theorem 35.3. Let $F(x_1, \dots, x_n)$ be a polynomial with integer coefficients, and fix a prime p . Then $F(x_1, \dots, x_n) \equiv 0$ has solutions modulo p^v for all $v \geq 1$ if and only if $F(x_1, \dots, x_n) = 0$ has a solution in \mathbb{Z}_p .

Proof. One direction is quick: if there is a p -adic solution $(x_1^{(v)}, \dots, x_n^{(v)})_{v \in \mathbb{N}}$, then $(x_1^{(v)}, \dots, x_n^{(v)})$ is a solution modulo p^v .

In the other direction, suppose one has solutions $(x_1^{(v)}, \dots, x_n^{(v)})$ for each $v \in \mathbb{N}$. These do not necessarily satisfy the condition $x_i^{(v)} = \lambda_v(x_i^{(v+1)})$, but we will locate a subsequence which works. Without loss of generality, we can assume that $n = 1$ (otherwise take the subsequence which works and find a further subsequence to guarantee the condition for the next position in the n -tuple, etc.) So we can simplify notation and write $(x_v)_{v \in \mathbb{N}}$.

Now, viewing the x_v as integers, there are infinitely many congruent to some y_1 modulo p by the pigeonhole principle. Thus, we can choose a subsequence $x_v^{(1)}$ of x_v satisfying

$$x_v^{(1)} \equiv y_1 \pmod{p}, \quad F(x_v^{(1)}) \equiv 0 \pmod{p}$$

Repeat this process to find

$$x_v^{(2)} \equiv y_2 \pmod{p^2}, \quad F(x_v^{(2)}) \equiv 0 \pmod{p^2}$$

etc. We find $x_v^{(k)}, y_k$ for $k \in \mathbb{N}$. Then by construction, $y = (y_k)_{k \in \mathbb{N}} \in \mathbb{Z}_p$ and $F(y_k) \equiv 0 \pmod{p^k}$ so y is a p -adic solution. \square

36. VALUATIONS, ABSOLUTE VALUES

Definition 36.1. Let K be a field. A map $|| : K \rightarrow \mathbb{R}$ is an absolute value if

- (1) $|x| \geq 0$ and $|x| = 0 \iff x = 0$.
- (2) $|xy| = |x||y|$.
- (3) $|x + y| \leq |x| + |y|$ (the triangle inequality).

There is a trivial absolute value taking the value 1 everywhere except 0. We'll generally ignore it.

Using $d(x, y) = |x - y|$ gives a metric space which in particular is a topological space. Two absolute values are called *equivalent* if they define the same topology.

We denote by $||_\infty$ the usual absolute value on \mathbb{C} or any subfield. Any $||_\infty^s$ for positive s is also an absolute value.

On \mathbb{Q} there is an absolute value $||_p$ for each prime p defined by $|x| = \frac{1}{p^n}$ where n is such that $x = p^n(a/b)$ and $\gcd(ab, p) = 1$. There's also a notation for this n by itself: $n = v_p(x)$. Note that $v_p(0) = \infty$ by convention and $|0|_p = 0$.

Proposition 36.2. Let $0 \neq a \in \mathbb{Q}$. Then $\prod_p |a|_p = 1$ where p runs over all primes and ∞ .

Proof. The element a has a factorisation

$$a = \pm \prod_{p \neq \infty} p^{v_P(a)}$$

wherein the sign is given by $a/|a|_\infty$. Thus,

$$a = \frac{a}{|a|_\infty} \prod_{p \neq \infty} \frac{1}{|a|_p}$$

from which the result follows. □

Definition 36.3. A valuation is a map

$$v : K \rightarrow \mathbb{R} \cup \{\infty\}$$

such that

- (1) $v(x) = \infty \iff x = 0$.
- (2) $v(xy) = v(x) + v(y)$.
- (3) $v(x + y) \geq \min\{v(x), v(y)\}$.

A discrete valuation is a valuation admitting a smallest positive value s . Then $v(K^*) = s\mathbb{Z}$. Surjectivity is clear, and if there were some t_1, t_2 with $|v(t_1) - v(t_2)| < s$, then $|v(\frac{t_1}{t_2})| < s$, a contradiction to minimality.

Neukirch calls this an *exponential valuation*, reserving the term *valuation* for absolute values! This is unusual.

Again, there is a trivial valuation $v(x) = 0$ for all $x \neq 0$ which we will ignore.

The example at hand is the valuation $v_p(x)$ already defined.

Whenever we have a valuation, we get an absolute value. Take $q > 1$ real and let $|x| = q^{-v(x)}$. If we change q (or use $sv(x)$ as the valuation for some positive s), then we get an equivalent absolute value. (A theorem on equivalences is coming up but another example first.)

Example 36.4. Now consider $K = k(t)$ the field of rational functions over a field k . It is the fraction field of the polynomial ring $k[t]$. The primes $\mathfrak{p} \neq (0)$ in $k[t]$ are $(p(t))$ where p is a monic irreducible polynomial. Then there is a valuation and absolute value associated to \mathfrak{p} , as follows. Let $f(t) = \frac{g(t)}{h(t)} \in K$. Then it can be expressed as $p(t)^m \frac{g'(t)}{h'(t)}$ where p is coprime to $g'h'$. We define

$$v_{\mathfrak{p}}(f) = m, \quad |f|_{\mathfrak{p}} = q_{\mathfrak{p}}^{-v_{\mathfrak{p}}(f)}$$

where $q_{\mathfrak{p}} = q^{d_{\mathfrak{p}}}$, $d_{\mathfrak{p}}$ is the degree of $k[t]/\mathfrak{p}$ over k (i.e. the degree of p) and $1 < q \in \mathbb{R}$. Also, of course, $v_{\mathfrak{p}}(0) = \infty$, $|0|_{\mathfrak{p}} = 0$. For $\mathfrak{p} = (t - a)$, $v_{\mathfrak{p}}(f)$ is the order of a zero or pole at $t = a$.

Also, there is a valuation $v_\infty : k(t) \rightarrow \mathbb{Z} \cup \{\infty\}$ given by $v_\infty(f) = \deg(h) - \deg(g)$. This is the order of a zero or pole at infinity, i.e. the order of a zero/pole of $f(1/t)$ at $t = 0$. We will see this as follows, with reference to the discussion of projective space which follows later in these notes.

There are many copies of \mathbb{A}^1 in \mathbb{P}^1 of which we will consider two:

$$\phi_1 : \mathbb{A}^1 \rightarrow \mathbb{P}^1, \quad t \mapsto [t, 1],$$

$$\phi_2 : \mathbb{A}^1 \rightarrow \mathbb{P}^1, \quad a \mapsto [1, a].$$

On the overlap, we have $a = 1/t$. The first misses what we usually think of as the point at infinity, $[1, 0]$, while the second misses the point $[0, 1]$ which we usually think of as zero (since we usually think of the ‘affine piece’ given by ϕ_1). Now, suppose that $f(t)$ is a rational map $g(t)/h(t)$ (where $g(t)$ and $h(t)$ are polynomials) on \mathbb{A}^1 . Then, on $\phi_1(\mathbb{A}^1)$, the map looks like

$$f([X, Y]) = [g(X/Y), h(X/Y)].$$

This tells us that we can write it as $f([1, a]) = [g(1/a), h(1/a)]$ on the intersection $\phi_1(\mathbb{A}^1) \cap \phi_2(\mathbb{A}^1)$. But we have

$$f(t) = f(1/a) = g(1/a)/h(1/a) = p(a)/q(a)$$

for some polynomials p and q obtained by multiplying top and bottom of the fraction by an appropriate power of a . So, we have

$$f([1, a]) = [p(a), q(a)]$$

on $\phi_2(\mathbb{A}^1)$. So now the order of a zero or pole of $f(t)$ “at infinity” is the order of a zero or pole of $f(1/a)$ “at $a = 0$,” which is to say, the power m such that $f(1/a) = a^m p'(a)/q'(a)$ where $(p'q'(a), a) = 1$. Pausing for a moment to reflect, we see that this is $m = \deg h - \deg g$ (try it with $\frac{t^2-1}{t^3+t}$ for example, and you will obtain a $(\frac{1-a^2}{1+a^2})$).

Proposition 36.5. *The following are equivalent:*

- (1) $|\cdot|_1$ and $|\cdot|_2$ are equivalent.
- (2) There exists a real $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in K$.

Proof. To be Tex'd. □

Proposition 36.6. *(Weak Approximation) Let $|\cdot|_1, \dots, |\cdot|_n$ be pairwise inequivalent non-trivial absolute values of K . Let $a_1, \dots, a_n \in K$. Then for any $\epsilon > 0$, there exists $x \in K$ such that $|x - a_i|_i < \epsilon$ for all $i = 1, \dots, n$.*

Proof. To be Tex'd. □

Definition 36.7. *An absolute value is non-archimedean if $|n|$ is bounded as n ranges through the natural numbers. It is archimedean otherwise.*

For example, the p -adic absolute value is non-archimedean.

Proposition 36.8. *An absolute value $|\cdot|$ is non-archimedean if and only if $|x + y| \leq \max\{|x|, |y|\}$ for all x, y .*

The inequality in the statement is called the strong triangle inequality.

Proof. Not yet Tex'd. □

Note: for a non-archimedean absolute value, if $|x| \neq |y|$ then $|x+y| = \max\{|x|, |y|\}$, i.e. all triangles are isoceses.

Theorem 36.9. *(Ostrowski) Every non-trivial absolute value of \mathbb{Q} is equivalent to $|\cdot|_p$ for some prime p or to $|\cdot|_\infty$.*

Proof. Not yet Tex'd. □

37. INSERT HERE AMEYA AND FRANCOIS'S NOTES ON VALUATIONS FROM THEIR FATEFUL MONDAY!

These notes are available as a separate document on the website right now.

38. BABY ALGEBRAIC GEOMETRY: AFFINE AND PROJECTIVE SPACE

In this section we give the very basic definition of affine and projective spaces and varieties, with special attention to curves.

Let K be a field, and \bar{K} its algebraic closure. Then n dimensional *affine space* is the collection

$$\mathbb{A}^n = \{(x_1, \dots, x_n) : x_i \in \bar{K}\}.$$

(This should be a very familiar object.)

Let $\bar{K}[X_1, \dots, X_n]$ be the polynomial ring in n variables. An *affine variety* is a subset V_S associated to a subset S of the polynomial ring, given by

$$V_S = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in S\}.$$

Please note that some authors call this an *affine set* and reserve the term 'variety' for something more specific².

As an example, consider the ideal

$$I = (X^n + Y^n - 1) \subset \bar{\mathbb{Q}}[X, Y]$$

²that the variety is irreducible

Then Fermat's Last Theorem can be stated as follows: The variety V_I , where $n \geq 3$, has exactly the following rational points (points with rational coordinates): if n odd, $(1, 0), (0, 1)$; if n is even, $(\pm 1, 0), (0, \pm 1)$. (In general, the K -points of a variety are those $P \in \mathbb{A}^n$ with $x_i \in K \subset \overline{K}$ for all i .)

We can also start with an affine variety and extract an ideal:

$$I(V) = \{f \in \overline{K}[X_1, \dots, X_n] : f(P) = 0 \text{ for all } P \in V\}$$

(Please check that this is an ideal!). This will be an ideal containing the set S that defined V to begin with.

The quotient $\overline{K}[V] := \overline{K}[X_1, \dots, X_n]/I(V)$ is called the *coordinate ring* or *ring of regular functions* of the affine variety. It is the collection of polynomial functions which are defined on V , since $g = h$ on V if and only if $g - h \in I(V)$.

This ring has a field of fractions, called the *field of rational functions* on V , denoted $\overline{K}(V)$.

We will be interested in elliptic curves E defined by an equation of the form $y^2 = x^3 + Ax + B$. The coordinate ring is

$$\overline{K}[E] = \overline{K}[X, Y]/(Y^2 - X^3 - AX - B)$$

and the field of rational functions is

$$\overline{K}(E) = \overline{K}(X, Y)/(Y^2 - X^3 - AX - B).$$

To see this, one must verify that $I(E)$ is the ideal generated by the single function $Y^2 - X^3 - AX - B$. This involves a digression to discuss the *Hilbert Nullstellensatz*, which I will not engage in here except to state that the ideal $I(V_S)$ of a variety is the radical of the ideal generated by S . In this example, the ideal at hand $(Y^2 - X^3 - AX - B)$ is prime, and so it is equal to its own radical. In these notes I am concerned only with special cases where the ideal will usually agree with the reader's first guess. However, be warned that there is deep mathematics lurking here. For more, see any text on algebraic geometry.

We say that a variety is *defined over* K if

$$I(V) = (I(V) \cap K[X_1, \dots, X_n])\overline{K}[X_1, \dots, X_n],$$

i.e. the generators for $I(V)$ can be given with K coefficients. In the example above, E is defined over \mathbb{Q} . In this case, we can discuss $K[V]$ and $K(V)$.

Now we turn to projective space, which you have probably also heard of. Projective n -dimensional space \mathbb{P}^n is the set

$$\{[X_0, \dots, X_n] \in \mathbb{A}^{n+1}, X_i \text{ not all zero}\}$$

modulo the relation $[X_0, \dots, X_n] \sim [\lambda X_0, \dots, \lambda X_n]$ for any $\lambda \in \overline{K}^*$. Now the question whether a polynomial vanishes at a point in projective space makes sense only for homogeneous polynomials³.

One can see projective space as the collection of one-dimensional subspaces of affine space of one higher dimension. The space \mathbb{P}^1 , for example, consists of pairs $[a, b]$ which may be identified with lines $ax + by = 0$ in \mathbb{A}^2 . The slope is a/b unless $b = 0$, when the line is vertical.

As in the affine case, if we have a collection of homogeneous polynomials in $\overline{K}[X_0, \dots, X_n]$, we say that the set

$$V_S = \{P \in \mathbb{P}^n : f(P) = 0 \forall f \in S\}$$

is a projective variety (the same caveat holds for nomenclature: some only call this a projective set). We can again generate a homogeneous ideal: $I(V)$ is the ideal generated by all homogeneous $f \in \overline{K}[X_0, \dots, X_n]$ such that $f(P) = 0$ for all $P \in V$.

As before, V is defined over K if $I(V)$ can be generated by homogeneous polynomials in $K[X_0, \dots, X_n]$.

The notion of K -rational points is trickier for \mathbb{P}^n . We say that $[x_0, \dots, x_n]$ is K -rational if there exists some λ such that $\lambda x_i \in K$ for all i simultaneously.

When discussing a projective variety, we often look at some *affine piece*, that is, the part V' of the variety V contained in the subset \mathbb{A}^n of \mathbb{P}^n (for example, \mathbb{A}^n injects into \mathbb{P}^n by $[x_1, \dots, x_n] \mapsto [x_1, \dots, x_{k-1}, 1, x_k, \dots, x_n]$). Then we can talk about the field of rational functions $\overline{K}(V) = \overline{K}(V')$ for any such *affine piece* and in fact all of these will be isomorphic.

Of particular interest to us will be the affine piece \mathbb{A}^2 of \mathbb{P}^2 given by

$$(x, y) \mapsto [x, y, 1].$$

The functions on \mathbb{A}^2 are of the form

$$\frac{p(x, y)}{q(x, y)}$$

and the functions on \mathbb{P}^2 can be given as the *homogenisations* of those on \mathbb{A}^2 . This is best explained by example:

$$\frac{x^2 + y}{xy + 1}$$

becomes under homogenisation

$$\frac{X^2 + YZ}{XY + Z^2}.$$

³consider for example that it may happen that $x_1^2 = x_2$ but $(\lambda x_1)^2 \neq \lambda x_2$

Then it can be considered as a well-defined function on \mathbb{P}^2 . The functions on \mathbb{P}^2 can be viewed as the collection of all ratios of homogeneous polynomials of the same degree.

In general, for any variety $V \subset \mathbb{P}^n$, the functions are

$$\frac{f(X_0, \dots, X_n)}{g(X_0, \dots, X_n)}$$

where f and g are homogeneous of the same degree, with $g \notin I(V)$ and where $f/g = f'/g'$ whenever $f'g - f'g \in I(V)$.

39. INTRODUCTION TO ELLIPTIC CURVES

We are motivated by the following question: when are there rational solutions to a polynomial equation in two variables? For example, we considered the equation $x^2 + y^2 = 1$ on the first day of class, and found all rational solutions: the Pythagorean triples. Another famous equation was considered by Bachet:

$$y^2 - x^3 = c$$

for a constant c . He noticed something really fascinating about the rational solutions to this equation: if (x, y) was a rational solution, then

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3} \right)$$

is another. In this way, in fact, we obtain infinitely many distinct solutions (this is not a priori obvious).

By contrast, we may ask about integral solutions. Fermat posed the problem in the 1650's to find all integer solutions to Bachet's equation with $c = -2$. In fact, the only integer solutions are $(3, \pm 5)$, but it was some time until a correct proof was given.

Not yet Tex'd: Define elliptic curves and their models in \mathbb{P}^2 , and dimension and singular points, discriminant, the group law.

40. CURVES AND RINGS OF INTEGERS: INTRODUCTION

Let K be algebraically closed for this section. Let C be an affine variety of dimension 1 (a curve) and irreducible (we will define this momentarily). Let $K(C)$ be the field of rational functions, which has transcendence degree 1 (this is the meaning of it being dimension 1), and $K[C]$ the coordinate ring which has $K(C)$ as its field of fractions.

Now, $K[C]$ has the following properties.

- (1) **It is an integral domain.** This is because it is of the form $K[X_1, \dots, X_n]/I(C)$ where $I(C)$ is prime – primality here is the definition of “irreducible” above.

- (2) **It is Noetherian.** This is clear since it is a quotient of a polynomial ring.
- (3) **Every non-zero prime is maximal.** This is equivalent to being dimension 1, though we do not prove it at the moment.
- (4) **It is integrally closed.** We will come back to this one in a little while.

From which we conclude: it is a Dedekind domain!

I think it is very important to get a feel for points on curves. Consider as a first case the coordinate ring $K[X]$ of \mathbb{A}^1 . We think of it as the ring of functions on \mathbb{A}^1 . Each maximal ideal is of the form $(X - a)$ (and all such ideals are maximal), and we think of these as the point of \mathbb{A}^1 . For each maximal ideal, there is a map

$$K[X] \rightarrow K[X]/(X - a) \cong K$$

given by

$$f(x) \mapsto f(a) \in K.$$

Now we wish to generalise this thinking to the coordinate ring of a curve. Consider $K[C] = K[X_1, \dots, X_n]/I$. A surjective map $K[C] \rightarrow K$ is just a surjective map $K[X_1, \dots, X_n] \rightarrow K$ factoring through $K[C]$ which in turn corresponds to a maximal ideal $M = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$ of $K[X_1, \dots, X_n]$ containing I . In turn, this corresponds to a point (a_1, \dots, a_n) on C (since $g \in I$ satisfies $g(a_1, \dots, a_n) = 0$). So points are maps and maps are points. The map associated to this ideal is $K[C] \rightarrow K[C]/M \cong K$ given by $f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n)$.

Points are prime ideals are maps!

Example 40.1. Consider the elliptic curve $E : Y^2 = X^3 - 1$ and the point $(1, 0)$ on the curve. The coordinate ring is $K[C] = K[X, Y]/(Y^2 - X^3 - 1)$ and the maximal ideal associated to the point is $M = (X - 1, Y)$. The map we get is $K[C] \rightarrow K[C]/M = K[X, Y]/(Y^2 - X^3 - 1, X - 1, Y) = K[X, Y]/(X - 1, Y) \cong K$ given by $f(X, Y) \mapsto f(1, 0)$. For example, $X \mapsto 1$ and $XY + X \mapsto 1$.

So we have a bit of a dictionary:

$$\begin{aligned} \text{functions} &\leftrightarrow \text{ring} \\ \text{points} &\leftrightarrow \text{non-zero prime ideals} \\ \text{evaluate fn at point} &\leftrightarrow \text{take quotient of ring at ideal} \end{aligned}$$

This tells us that for the ring of integers, we can think of the primes as points, and looking modulo a prime as “evaluating” an integer at a prime.

Now we return to the question of integral closure (point # 4 above).