Algebraic Number Theory, Fall 2018

Notes and exercises from class

Professor: Igor Rapinchuck

Joshua Ruiter

October 16, 2019

Contents

1 Background material **3**
- 1.1 Prime vs irreducible elements . . . 3
- 1.2 Vandermonde determinants . . . 3

2 Definitions **4**
- 2.1 Integral elements, integral closure, rings of integers . . . 4
- 2.2 Norm, trace, and discriminant . . . 4
- 2.3 Dedekind domains, unique factorization . . . 6
- 2.4 Factorization of ideals, ramification . . . 7
- 2.5 Discrete valuations . . . 8
- 2.6 Eisenstein extensions . . . 8
- 2.7 Lattice theory . . . 8
- 2.8 Dirichlet unit theorem . . . 9
- 2.9 S-units . . . 10
- 2.10 Absolute values . . . 11
- 2.11 Valuations, relationship with absolute values . . . 12
- 2.12 p-adic numbers . . . 13
- 2.13 Local fields . . . 13
- 2.14 p-adic integers . . . 14
- 2.15 Ramified and unramified extensions . . . 15

3 Theorems **16**
- 3.1 Integral elements, integral closure, rings of integers . . . 16
- 3.2 Norm, trace, and discriminant . . . 17
- 3.3 Dedekind domains, unique factorization . . . 21
- 3.4 Factorization of primes, ramification . . . 23
- 3.5 Quadratic extensions . . . 25
- 3.6 Lagrange's theorem on sum of four squares . . . 26
- 3.7 Discrete valuations . . . 27

3.8 Eisenstein extensions . . . 27
3.9 Finiteness of the class group, lattice theory . . . 27
3.10 Class groups of quadratic number fields . . . 29
3.11 A cubic extension with trivial class group . . . 31
3.12 Dirichlet unit theorem . . . 32
3.13 Applications of the Dirichlet unit theorem . . . 35
3.13.1 Quadratic number fields . . . 35
3.13.2 A higher degree example . . . 36
3.14 Generalization of unit theorem for S-units . . . 36
3.15 Cyclotomic fields . . . 37
3.16 Special case of Fermat's last theorem . . . 39
3.17 Local fields . . . 39
3.17.1 Hensel's Lemma . . . 44
3.17.2 Applications of Hensel's lemma . . . 44
3.17.3 Extending absolute values . . . 46
3.17.4 Unramified extensions . . . 49
3.17.5 Totally ramified extensions . . . 50
3.18 Results beyond our class . . . 52

4 Exercises **53**
4.1 Informal exercises from lectures . . . 53
4.1.1 Discriminants . . . 53
4.1.2 Class groups . . . 54
4.1.3 $\mathbb{Q}_p$ . . . 55
4.2 Homework set 1 . . . 56
4.3 Homework set 2 . . . 64

1 Background material

1.1 Prime vs irreducible elements

Definition 1.1.1. In a ring A, an element $p \in A$ is **prime** if whenever $p|ab$, then $p|a$ or $p|b$.

Definition 1.1.2. In an integral domain A, an element $\pi \in A$ is **irreducible** if it nonzero, not a unit, and if $\pi = ab$, then one of a, b is a unit. (That is, π cannot be written as the product of two non-units.)

Proposition 1.1.3. *In an integral domain, every prime element is irreducible. In a UFD, every irreducible element is prime.*

$$\text{prime} \xrightarrow{\text{domain}} \text{irreducible} \qquad \text{irreducible} \xrightarrow{\text{UFD}} \text{prime}$$

Proposition 1.1.4. *The principal ideal generated by a prime element is a prime ideal.*

1.2 Vandermonde determinants

Theorem 1.2.1. *Let $x_1, \ldots, x_n$ be elements of a commutative ring A. Then*

$$\det(x_i^{j-1}) = \det \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & x_2^3 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & x_n^3 & \ldots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i)$$

2 Definitions

2.1 Integral elements, integral closure, rings of integers

Definition 2.1.1. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. The **minimal polynomial** of α over K is the monic polynomial $f \in K[x]$ of minimal degree so that $f(\alpha) = 0$. (Note that the minimal polynomial is always irreducible.)

Definition 2.1.2. A **number field** is a finite field extension of $\mathbb{Q}$.

Definition 2.1.3. Let $A \subset B$ be rings. An element $b \in B$ is **integral** over A if there is a monic polynomial $f \in A[x]$ so that $f(b) = 0$. The ring B is **integral** over A if every element of A is integral over A.

Definition 2.1.4. Let K be a number field. An element $\alpha \in K$ is a **algebraic integer** if it is integral over $\mathbb{Z}$. That is, α satisfies a monic polynomial in $\mathbb{Z}[x]$. The set of algebraic integers is dentoed $\mathcal{O}_K$, which is called the **ring of integers** of K.

Definition 2.1.5. Let A be a ring and M an A-module. M is **faithful** if $aM = 0 \implies a = 0$. That is, the annihilator of M is trivial.

Definition 2.1.6. Let A be an integral domain contained in a field L. The ring of elements of L that are integral over A is the **integral closure** of A in L. (This is most often used in the case where L is the fraction field of L.)

Definition 2.1.7. An integral domain A is **integrally closed** if A is equal to its integral closure in its field of fractions.

Definition 2.1.8. Let d be a square-free integer, and $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ a quadratic extension. If $d > 0$, we call $\mathbb{Q}(\sqrt{d})$ a **real quadratic field**. If $d < 0$, it is called an **imaginary quadratic field**.

2.2 Norm, trace, and discriminant

Definition 2.2.1. Let $A \subset B$ be rings so that B is a free A-module of rank n. Every $\beta \in B$ defines an A-linear map $m_\beta : B \to B, x \mapsto \beta x$, so m_β has a matrix with respect to a fixed basis. The **norm** and **trace** of β are the respective determinant and trace of the matrix of m_β.

$$\mathrm{N}_A^B(\beta) = \det m_\beta \qquad \mathrm{Tr}_A^B(\beta) = \mathrm{Tr}(m_\beta)$$

Definition 2.2.2. Let $T : V \to V$ be a linear transformation of a finite dimensional vector space V. The **characteristic polynomial** of T, denoted $c_T(x)$, is $\det(xI - T)$.

Definition 2.2.3. For a finite field extension L/K, and $\alpha \in L$, the **characteristic polynomial** of α, denoted $c_\alpha(x)$, is the characteristic polynomial of the linear map $m_\alpha : L \to L$.

$$c_\alpha(x) = c_{m_\alpha(x)}$$

Definition 2.2.4. Let V be a finite dimesional K-vector space. A **bilinear form** on V is a K-bilinear map $\phi : V \times V \to K$. A bilinear form is **symmetric** if $\phi(v, u) = \phi(u, v)$ for all $u, v \in V$.

Definition 2.2.5. Let $\phi : V \times V \to K$ be a bilinear form. Given a basis $B = \{e_1, \ldots, e_n\}$ of V over K, the **matrix** of ϕ with respect to the given basis is the matrix $A_{\phi,B} = \big(\phi(e_i, e_j)\big)$. This is defined so that for $u, v \in V$, write them as column vectors $[u]_B, [v]_B$ in terms of the basis B, and then

$$\phi(u, v) = [u]_B^T A_{\phi,B} [v]_B$$

Definition 2.2.6. Let $\phi : V \times V \to K$ be a bilinear form, and fix a basis $B = \{e_1, \ldots, e_n\}$ of V. The **discriminant** of ϕ with respect to B is

$$D_\phi(e_1, \ldots, e_n) = \det(A_{\phi,B})$$

Definition 2.2.7. A bilinear form is **nondegenerate** if it has nonzero discriminant with respect to some basis. (Since base change only affects the discriminant by a nonzero square, this is equivalent to having nonzero discriminant with respect to every basis.)

Definition 2.2.8. Let L/K be a finite field extension. The **trace form** of L/K is the symmetric bilinear form $(\alpha, \beta) \mapsto \mathrm{Tr}_K^L(\alpha\beta)$. The **discriminant** of L/K is the discriminant of the trace form.

$$D(L/K) = D_{\mathrm{Tr}_K^L}(e_1, \ldots, e_n) = \det\big(\mathrm{Tr}_K^L(e_i e_j)\big)$$

(Note that the discriminant is only well defined up to multiplying by nonzero squares of K, that is, $D(L/K) \in K^\times/(K^\times)^2$.)

Definition 2.2.9. Let $A \subset B$ be rings so that B is a free A-module of rank m. Given a basis $\{\beta_1, \ldots, \beta_m\}$ of B over A, the **discriminant** of B/A, denoted $\mathrm{disc}(B/A)$, is the discriminant of the trace form Tr_A^B.

$$D(\beta_1, \ldots, \beta_m) = \det\big(\mathrm{Tr}_A^B(\beta_i \beta_j)\big)$$

As in the case of fields, a base change induces multiplication by the square of a unit in A, so the discriminant is well defined as an element of $A^\times/(A^\times)^2$.

In the case where $A = \mathbb{Z}$ and $B = \mathcal{O}_K$ is the ring of integers of a number field K, we occasionally denote $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$ by Δ_K.

Example 2.2.10. In the case $A = \mathbb{Z}$, and any ring B containing $\mathbb{Z}$, the discriminant is a well-defined element of $\mathbb{Z}$, since the only units are ± 1, which both square to 1.

Example 2.2.11. Consider a quadratic $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$, and let α be a root of f, so we have the basis $\{1, \alpha\}$ of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Denote $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}$ by Tr. Then

$$\mathrm{Tr}(1) = 2 \qquad \mathrm{Tr}(\alpha) = -b \qquad \mathrm{Tr}(\alpha^2) = \mathrm{Tr}(-b\alpha - c) = -b\,\mathrm{Tr}(\alpha) - c\,\mathrm{Tr}(1) = b^2 - 2c$$

so the matrix of the trace form with respect to the basis $\{1, \alpha\}$ is

$$\begin{pmatrix} 2 & -b \\ -b & b^2 - 2c \end{pmatrix}$$

which has determinant $b^2 - 4c$, which coincides with the familiar discriminant formula for a quadratic function.

2.3 Dedekind domains, unique factorization

Definition 2.3.1. A **discrete valuation ring** (DVR) is a local PID which is not a field.

Remark 2.3.2. Let R be a DVR.

1. R is Noetherian.
2. Every prime ideal of R is maximal (Krull dimension is one).
3. R is integrally closed.
4. R is a Dedekind domain (this is just a summary of previous three properties).
5. Let $\mathfrak{m}$ be the unique maximal ideal of R. The chain

$$\mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \dots$$

   contains every ideal of R.
6. R is a UFD.
7. R has a unique nonzero prime element π, which generates the maximal ideal $\mathfrak{m}$.

Definition 2.3.3. An integral domain R is a **Dedekind domain** if it is Noetherian, integrally closed, and has Krull dimension one. (Krull dimension one is equivalent to saying that every prime ideal is maximal.)

Definition 2.3.4. Let A be a Dedekind domain, and let $K = \mathrm{Frac}(A)$. A **fractional ideal** of A is a nonzero finitely generated A-submodule of K. The set of all fractional ideals of A is denoted $\mathbf{Id}\,(\boldsymbol{A})$.

When we wish to emphasize that an ideal $\mathfrak{a} \subset A$ is NOT a fractional ideal, we call it an **integral ideal**.

Remark 2.3.5. Let A be a Dedekind domain. Since A is Noetherian, an A-submodule $\mathfrak{a} \subset \mathrm{Frac}(A)$ is a fractional ideal if and only if there exists a nonzero element $d \in A$ so that

$$d\mathfrak{a} = \{da : a \in A\}$$

is an ideal of A.

Definition 2.3.6. Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of a Dedekind domain A. The **product** of these is

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

which is a fractional ideal of A.

Remark 2.3.7. If A is a DVR with maximal ideal $\mathfrak{p} = (\pi)$, then $\mathrm{Id}(A) \cong \mathbb{Z}$ via $(\pi^n) \mapsto n$. (This is a group isomorphism.)

Definition 2.3.8. Let A be a Dedekind domain, and let $P(A) \subset \mathrm{Id}(A)$ be the subgroup of principal fractional ideals. The **ideal class group** of A is $\mathbf{Cl}(A) = \mathrm{Id}(A)/P(A)$. If $\mathrm{Cl}(A)$ is a finite group, its order is the **class number** of A.

If K is a number field, we frequently abuse terminology by referring to the class group/number of K, which really means the class group/number of $\mathcal{O}_K$.

Remark 2.3.9. In light of the fact that A is a PID if and only if the class number is one, we may think of the class number/class group as an obstruction to the fact that a Dedekind domain is a PID. That is, we might say that the size of the class group measures the distance A is from being a PID.

Definition 2.3.10. Let K be a number field, and $\mathfrak{a} \subset \mathcal{O}_K$ a nonzero ideal. Then **norm** of $\mathfrak{a}$ is

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$$

Remark 2.3.11. The use of the term "norm" is justified by a proposition which says that the two notions agree (up to sign) for principal ideals, that is,

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

and the fact that the ideal norm is also multiplicative, $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

2.4 Factorization of ideals, ramification

Definition 2.4.1. Let A be a Dedekind domain, and let $K = \mathrm{Frac}(A)$. Let L/K be a finite separable field extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \subset A$ be a prime ideal, and factor $\mathfrak{p}B$ into a product of prime ideals of B,

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

Then we may view $A/\mathfrak{p}$ as a subring of $B/\mathfrak{P}_i$. Note that $\mathfrak{p}$ is maximal, so $A/\mathfrak{p}$ is a field. We know that B is a finitely generated A-module, so $B/\mathfrak{P}_i$ is a finite dimensional $A\mathfrak{p}$ vector space. The **residual field degree** of $\mathfrak{P}_i$ is

$$f_i = \dim_{A/\mathfrak{p}} B/\mathfrak{P}_i$$

The **ramification index** of $\mathfrak{P}_i$ is the exponent e_i. If any $e_i > 1$, then $\mathfrak{p}$ **ramifies** in B. If all $e_i = 1$, then $\mathfrak{p}$ is **unramified**. If $e_i = f_i = 1$ for all i, then $\mathfrak{p}$ **splits completely** in B. If $\mathfrak{p}B$ is prime, then $\mathfrak{p}$ is **inert**.

Definition 2.4.2. Let K, L be number fields with $K \subset L$, with respective rings of integers $\mathcal{O}_K, \mathcal{O}_L$. Let $\mathfrak{p}_K \subset \mathcal{O}_K$ be a prime ideal, and let $\mathfrak{p}_L \subset \mathcal{O}_L$ be a prime ideal with $\mathfrak{p}_L \cap \mathcal{O}_K = \mathfrak{p}_K$. This is equivalent to saying that $\mathfrak{p}_L$ appears in the (unique) factorization of the ideal $\mathfrak{p}_K\mathcal{O}_L$.

$$\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_L^{e} \dots \mathfrak{p}_r^{e_r}$$

The power of $\mathfrak{p}_L$ in this factorization is defined to be $e(\mathfrak{p}_L/\mathfrak{p}_K)$. Similarly, we define $f(\mathfrak{p}_L/\mathfrak{p}_K)$ to be

$$f(\mathfrak{p}_L/\mathfrak{p}_K) = \dim_{\mathcal{O}_K/\mathfrak{p}_K} \mathcal{O}_L/\mathfrak{p}_L$$

Definition 2.4.3. Let $K \subset L$ be number fields, and let $A \subset K$ be a Dedekind domain, and let B be the integral closure of A in L. The **discriminant ideal** of B over A, denoted $\mathscr{D}_{B/A}$ is the ideal of A generated by discriminants of bases of L/K that are contained in B. Note that $\mathscr{D}_{B/A}$ is a nonzero integral ideal of A.

2.5 Discrete valuations

Definition 2.5.1. Let K be a field. A **discrete valuation** on K is a nonzero map $v : K^\times \to \mathbb{Z}$ which is a group homomorphism, so $v(ab) = v(a) + v(b)$, and also satisfying

$$v(a+b) \geq \min(v(a), v(b))$$

If v is surjective, we say v is **normalized**. If v is not normalized, then the image is $m\mathbb{Z}$ for some $m \in \mathbb{Z}$, and we can replace v with the normalized valuation $\frac{1}{m}v$. Sometimes we extend v to K by setting $v(0) = \infty$.

Note: The next definition is more of a theorem than a definition, sorry.

Definition 2.5.2. Let $v : K^\times \to \mathbb{Z}$ be a discrete valuation. The **associated ring** is

$$A = \{a \in K | v(a) \geq 0\} \cup \{0\}$$

which is a local PID with unique maximal ideal

$$\mathfrak{m} = \{a \in K | v(a) > 0\} \cup \{0\}$$

If the image of v is $m\mathbb{Z}$, and $\pi \in K^\times$ with $v(\pi) = m$, then $\mathfrak{m} = (\pi)$, and the element π is called a **uniformizer**.

Definition 2.5.3. Let A be a Dedekind domain, and $K = \mathrm{Frac}(A)$, and let $\mathfrak{p} \subset A$ be a prime ideal. The associated discrete valuation is $v_\mathfrak{p} : K^\times \to \mathbb{Z}$ is defined by taking $v_\mathfrak{p}(c)$ to be the power of $\mathfrak{p}$ in the factorization of the fractional ideal (c).

Remark 2.5.4. If $(A, \mathfrak{m})$ is a local PID, and $v_\mathfrak{m} : \mathrm{Frac}(A) \to \mathbb{Z}$ is the discrete valuation as desribed above, then A is exactly the associated ring of $v_\mathfrak{m}$, as in Defnition 2.5.2.

2.6 Eisenstein extensions

Definition 2.6.1. Let A be a Dedekind domain and let $K = \mathrm{Frac}(A)$. Let L/K be a finite separable extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \subset A$ be a prime ideal, and let $v_\mathfrak{p} : K \to \mathbb{Z}$ be the associated discrete valuation. A polynomial

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in A[x]$$

is **Eisenstein at** $\mathfrak{p}$ if $v_\mathfrak{p}(a_i) > 0$ for $i = 1, \ldots, m-1$ and $v_\mathfrak{p}(a_0) = 1$.

2.7 Lattice theory

Definition 2.7.1. Let V be a finite dimensional real vector space. A **lattice** in V is a subgroup of the form $\Lambda = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_r$ with $e_1, \ldots, e_r$ linearly independent. If $r = n$, then Λ is a **full lattice**. Equivalently, Λ is a discrete subgroup of V.

Definition 2.7.2. Let V be an n-dimensional real vector space, and let $\Lambda = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$ be a full lattice. The **fundamental domain** of Λ is

$$D = \left\{ \sum_{i=1}^{n} a_i e_i : 0 \leq a_i < 1 \right\}$$

The quotient map $V \to V/\Lambda$ induces a bijection between D and V/Λ. That is, D is a set of representatives for V/Λ. Another way to say this is that every point of V is congruent, modulo Λ, to a point of D.

Definition 2.7.3. Let Λ be a full latice in $\mathbb{R}^n$, with fundamental domain D. Let μ be Lebesgue measure on $\mathbb{R}^n$. The **volume** of Λ, denoted $V(\Lambda)$, is $\mu(D)$. Note that by a key lemma, this is independent of the choice of basis of Λ. Note that if Λ is spanned by $x_1, \ldots, x_n$ and we set T to be the matrix whose columns are $x_1, \ldots, x_n$ written in terms of the standard basis of $\mathbb{R}^n$, then

$$V(\Lambda) = |\det T|$$

Definition 2.7.4. A subset $S \subset \mathbb{R}^n$ is **symmetric about the origin** or **centrally symmetric** if $x \in S \implies -x \in S$.

Definition 2.7.5. Let $K/\mathbb{Q}$ be a number field with $[K : \mathbb{Q}] = n$. Since $\mathbb{Q}$ has characteristic zero, this is a separable extension, so there are n distinct embeddings $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ which restrict to the identity on $\mathbb{Q}$. If $\sigma_i(K) \subset \mathbb{R}$, we call σ_i a **real embeddings**. Otherwise, we call it a **complex embedding**.

Note that complex embeddings come in conjugate pairs. By convention, we denote the number of real embeddings by r_1 and the number of pairs of complex embeddings by r_2, so that $r_1 + 2r_2 = n$. By convention, we order $\sigma_1, \ldots, \sigma_n$ so that $\sigma_1, \ldots, \sigma_{r_1}$ are the real embeddings, and for $1 + r_1 \leq j \leq r_2$, σ_j and σ_{j+r_2} are a conjugate pair. (That is, the first $r_1 + r_2$ embeddings determine all of them.)

Definition 2.7.6. Let $K/\mathbb{Q}$ be a number field with $[K : \mathbb{Q}] = n$, and with r_1 real embeddings and r_2 conjugate pairs of complex embeddings, ordered as above. The **canonical embedding** $\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ is

$$\sigma(x) = \Big(\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)\Big)$$

K is **totally real** if $r_2 = 0$. If $r_1 = 0$, K is **totally imaginary**.

Definition 2.7.7. Let K be a number field. A finite extension L/K is **unramified over** K if no prime ideal of $\mathcal{O}_K$ ramifies in L.

2.8 Dirichlet unit theorem

Definition 2.8.1. Let K be a number field with ring of integers $\mathcal{O}_K$. While the phrase "units of K" is mostly vacuous, since every nonzero element of K is invertible, we abuse terminology and use "units of K" to refer to units of $\mathcal{O}_K$. We frequently denote this by U_K.

Definition 2.8.2. Let K be a field. The roots of unity in K form a multiplicative group, which we denote by $\mu(K)$. If K is a number field, then $\mu(K)$ is a finite group, hence it is cyclic (every finite subgroup of a multiplicative group of a field is cyclic). Note that if K has a real embedding, then $\mu(K) = \{\pm 1\}$.

Definition 2.8.3. Let K be a number field. By Dirichlet's unit theorem, $U_K \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1}$. A **fundamental system of units** for K is a set of elements $u_1, \ldots, u_{r_1+r_2-1}$ which is a basis for the free part of U_K.

Definition 2.8.4. Let K be a number field with associated r_1, r_2. Set $r = r_1 + r_2 - 1$, and let $u_1, \ldots, u_r$ be a fundamental system of units in U_K. Define

$$\ell(u_k) = \Big(\log|\sigma_1 u_i|, \ldots, \log|\sigma_{r_1} u_i|, 2\log|\sigma_{r_1+1} u_i|, \ldots, 2\log|\sigma_{r_2+1} u_i| \Big)$$

By considerations arising the proof of the Dirichlet unit theorem, $\ell(u_1), \ldots, \ell(u_r)$ generate a full lattice in $W \cong \mathbb{R}^{r_1+r_2-1}$. The **regulator** of K, denoted $\mathrm{Reg}(K)$, is the determinant of the matrix with ith row $\ell(u_i)$. Thus, up to sign, $\mathrm{Reg}(K)$ is the volume of the lattice spanned by $\ell(u_1), \ldots, \ell(u_r)$.

Definition 2.8.5. A **CM field** is a totally imaginary quadratic extension of a totally real number field. (CM stands for complex multiplication.)

2.9 S-units

Definition 2.9.1. Let K be a number field, and let $S \subset \operatorname{spec} \mathcal{O}_K$ be a finite set of nonzero prime ideals of $\mathcal{O}_K$. For a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, let $v_\mathfrak{p}$ be the associated discrete valuation. The **ring of S-integers** is

$$\mathcal{O}_K(S) = \{\alpha \in K : v_\mathfrak{p}(\alpha) \geq 0, \ \ \forall \mathfrak{p} \in (\operatorname{spec} \mathcal{O}_K) \setminus S\}$$

The **S-units** of K are the units of $\mathcal{O}_K(S)$, that is,

$$U_K(S) = \mathcal{O}_K(S)^\times = \big\{\alpha \in K^\times : v_\mathfrak{p}(\alpha) = 0, \ \ \forall \mathfrak{p} \in (\operatorname{spec} \mathcal{O}_K) \setminus S\big\}$$

Example 2.9.2. Let $K = \mathbb{Q}, S = \{2, 3\}$. The S-integers are

$$\begin{aligned}
\mathbb{Z}(S) &= \left\{ \frac{a}{b} \in \mathbb{Q} : v_p\left(\frac{a}{b}\right) \geq 0, \ \ \forall p \neq 2, 3 \right) \\
&= \left\{ \frac{a}{b} \in \mathbb{Q} : \gcd(a,b) = 1, v_5\left(\frac{a}{b}\right) \geq 0, v_7\left(\frac{a}{b}\right) \geq 0, \ldots \right\} \\
&= \left\{ \frac{a}{b} \in \mathbb{Q} : \gcd(a,b) = 1, b \text{ not divisible by } 5, 7, 11, \ldots \right\} \\
&= \left\{ \frac{a}{b} \in \mathbb{Q} : \gcd(a,b) = 1, b \text{ only divisible by } 2, 3 \right\} \\
&= \left\{ \frac{a}{2^n 3^m} \in \mathbb{Q} : a, n, m \in \mathbb{Z} \right\}
\end{aligned}$$

The S-units are

$$\begin{aligned}
U_K(S) &= \left\{ \frac{a}{b} \in \mathbb{Q} : v_p\left(\frac{a}{b}\right) = 0, \forall p \neq 2, 3 \right\} \\
&= \left\{ \frac{a}{b} \in \mathbb{Q} : \gcd(a,b) = 1, a, b \text{ only divisible by } 2, 3 \right\} \\
&= \{2^n 3^m : n, m \in \mathbb{Z}\}
\end{aligned}$$

2.10 Absolute values

Definition 2.10.1. Let K be a field. An **absolute value** on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that

1. $|x| = 0$ if and only if $x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

If $|\cdot|$ additionally satisfies the nonarchimedean triangle inequality $|x + y| \leq \max(|x|, |y|)$, it is a **nonarchimedean** absolute value.

Example 2.10.2. The usual absolute value on $\mathbb{Q}$ or $\mathbb{R}$ or the norm on $\mathbb{C}$ are all absolute values. They are denoted by $|\cdot|_\infty$ to distinguish them.

Example 2.10.3. For any field K, there is the trivial absolute value,

$$|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$$

For example, on a finite field, the trivial absolute value is the only possible absolute value.

Remark 2.10.4. The property $|xy| = |x||y|$ may be rephrased as saying that an absolute value gives a group homomorphism $K^\times \to (\mathbb{R}_{>0}, \times)$. Consequently, any root of unity in K gets mapped to $1 \in \mathbb{R}$, since $\mathbb{R}$ has no torsion. As a consequence of this, if K is finite or even if K is the algebraic closure of a finite field, then K has only the trivial absolute value.

Example 2.10.5. Fix a prime $p \in \mathbb{Z}$, and fix $\alpha \in (0, 1)$. The p-adic absolute value on $\mathbb{Q}$ is defined by

$$|x|_p = \left| p^n \frac{a}{b} \right|_p = \alpha^n$$

where n, a, b are uniquely determined by choosing a, b with $\gcd(a, b) = \gcd(b, p) = 1$ and unique factorization of integers. The constant α can be anything in $(0, 1)$ for this to be an absolute value, though typically one uses the value $\alpha = p^{-1}$.

Alternately, this could be defined as follows: recognize that the primes in $\mathbb{Z}$, along with -1, are a generating set for $\mathbb{Q}^\times$, and define $|\cdot|_p$ on a generating set.

$$|x|_p = \begin{cases} 0 & x = 0 \\ 1 & x = q \text{ where } q \text{ is a prime and } q \neq p \\ p^{-1} & x = p \end{cases}$$

Extending this definition by the multiplicative property gives the same as the previous definition.

Definition 2.10.6. Two absolute values $|\cdot|_1, |\cdot|_2$ on K are **equivalent** if they induce the same metric topology on K. Equivalently, $|x|_1 = |x|_2^a$ for some constnat $a \in \mathbb{R}_{>0}$. Also equivalently, they are equivalent if $|x|_1 < 1 \iff |x|_2 < 1$ for all $x \in K$.

Definition 2.10.7. Let K be a field. An equivalence class of absolute values on K is called a **prime** of K. An equivalence class of archimedean absolute values is called an **infinite prime**, and nonarchimedean absolute values a **finite prime**.

2.11 Valuations, relationship with absolute values

Definition 2.11.1. A **valuation** on a field K is a nontrivial group homomorphism $v : K^\times \to (\mathbb{R}, +)$ satisfying

$$v(xy) = v(x) + v(y) \qquad v(x+y) \geq \min(v(x), v(y))$$

(Sometimes it is convenient to formally extend a valuation by setting $v(0) = \infty$.)

Remark 2.11.2. There is a bijective correspondence between nonarchimedean absolute values on K and valuations on K via the isomorphisms

$$\log : (\mathbb{R}_{>0}, \times) \to (\mathbb{R}, +) \qquad \exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, +)$$

To go from a nonarchimedean absolute value to a valuation, compose with log. To go the other way, compose with exp.

Definition 2.11.3. Valuations v, v' on K are **equivalent** if $v' = cv$ for some $c \in \mathbb{R}$. Equivalently, they are equivalent if the corresponding absolute values are equivalent.

Definition 2.11.4. A valuation $v : K^\times \to \mathbb{R}$ is **discrete** if the image is a discrete subgroup. That is to say, the image is isomorphic to $\mathbb{Z}$. If the image is precisely $\mathbb{Z} \subset \mathbb{R}$, then we say v is **normalized**.

Example 2.11.5. Let k be any field, and let $k(t)$ be the field of rational functions in one variable. Let $f \in k[t]$ be an irreducible polynomial. Associated to f, we have a normalized discrete valuation

$$v_f : k(t)^\times \to \mathbb{Z} \qquad v_f\left(\frac{p(t)}{q(t)}\right) = v_f\left(f(t)^n \frac{\widetilde{p}(t)}{\widetilde{q}(t)}\right) = n$$

where $\widetilde{p}, \widetilde{q}$ are uniquely determined since $k[t]$ is a UFD. Geometrically speaking, v_f is almost like counting the order of zeros or poles of a rational function at f. If k is algebraically closed, so that the only irreducible polynomials are linear, then v_f is literally counting zeros/poles at the single root of f. Another discrete valuation on $k(t)$ is the less sophisticated

$$v_\infty : k(t)^\times \to \mathbb{Z} \qquad v_\infty\left(\frac{p}{q}\right) = \deg q - \deg p$$

Another geometric interpretation: suppose k is algebraically closed, then $k(t)$ is the function field of one dimensional projective space $\mathbb{P}^1_k$, and the valuations above correspond to the closed points of $\mathbb{P}^1_k$. We already described how v_f corresponds to the point which is the sole zero of f when f is linear. The valuation v_∞ corresponds to the "point at infinity" of $\mathbb{P}^1_k$.

Definition 2.11.6. Let $v : K^\times \to \mathbb{R}$ be a valuation. The associated **valuation ring** is

$$\mathcal{O}_v = \left\{x \in K^\times : v(x) \geq 0\right\} \cup \{0\} = \left\{x \in K^\times : |x| \leq 1\right\}$$

One may reasonably think of this as the "unit ball" in K, given the metric topology associated to the absolute value associated to the valuation v. Note that $\mathcal{O}_v$ is in fact a subring of K, and the units are

$$U_v = \left\{x \in K^\times : v(x) = 0\right\} = \left\{x \in K^\times : |x| = 1\right\}$$

Think of U_v as the "unit circle" or "unit sphere" in K. It is somewhat dangerous to think of this as the "boundary" of $\mathcal{O}_v$, however, since topologies from nonarchimedean absolute values do not behave at all like one expects, if one is used to the Hausdorff land of real manifolds. The ring $\mathcal{O}_v$ is a local ring with maximal ideal

$$\mathfrak{m}_v = \mathcal{O}_V \setminus U_v = \left\{x \in K^\times : v(x) > 0\right\} = \left\{x \in K^\times : |x| < 1\right\}$$

This functions as the "open unit ball" in K. The **residue field** associated to v is $\mathcal{O}_V/\mathfrak{m}_v$.

2.12 p-adic numbers

Remark 2.12.1. Let K be a field with absolute value and induced metric topology. This comes along with associated notions of Cauchy sequences, convergence, series convergence, and completeness. Generalize the usual definitions using an arbitrary absolute value, and everything works nicely.

Definition 2.12.2. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is denoted $\mathbb{Q}_p$ and called the field of **p-adic** numbers.

Definition 2.12.3. For each nonzero $x \in \mathbb{Q}_p$, there exists $n \in \mathbb{Z}$ such that $|x|_p = p^{-n}$. As a consequence, the normalized discrete valuation $v_p : \mathbb{Q} \to \mathbb{Z}$ extends to $\mathbb{Q}_p$. Hence we may define the **p-adic integers**

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\} = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}$$

as the valuation ring of $\mathbb{Q}_p$. Note that $\mathbb{Z}_p$ is a DVR with maximal ideal $\mathfrak{m} = p\mathbb{Z}_p$. Also note that $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$.

Also note that the neighborhoods $p^n\mathbb{Z}_p$ for $n \in \mathbb{Z}$ give a fundamental system of open neighborhoods of zero in $\mathbb{Q}_p$. That is to say, translates of these neighborhoods give a basis for the metric topology on $\mathbb{Q}_p$.

Remark 2.12.4. An alternate construction of $\mathbb{Z}_p$ is as a profinite group. Let $G_n = \mathbb{Z}/p^n\mathbb{Z}$, and $\pi_m^n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ be the natural quotient map. Ranging over $n \in \mathbb{N}$, this is a directed system (with the usual order on $\mathbb{N}$), and it's inverse limit is $\mathbb{Z}_p$.

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

Example 2.12.5. Another interesting profinite group is the following. Let $H_n = \mathbb{Z}/n\mathbb{Z}$, and for $m|n$ let $\pi_m^n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the natural quotient map. The system (H_n, π_m^n) is a directed system with indexing set $\mathbb{N}$ with partial order given by divisibility. The inverse limit of this system is denote $\widehat{\mathbb{Z}}$. This is an example of a more general construction of the profinite completion of a group.

2.13 Local fields

Definition 2.13.1. A topological space is **locally compact** if every point has a compact neighborhood.

Definition 2.13.2. A topological space X is **totally bounded** if for every $\epsilon > 0$, there is a finite cover of X by ϵ-balls.

Definition 2.13.3. A **local field** is a field K with nontrivial absolute value which is locally compact in its induced metric topology.

Example 2.13.4. $\mathbb{R}$ and $\mathbb{C}$ with the usual Euclidean absolute value/complex norm are local fields.

Example 2.13.5. $\mathbb{Q}_p$ with p-adic absolute value is a local field.

Example 2.13.6. Let $q = p^n$ be a prime power and let $\mathbb{F}_q$ be the (unique up to isomorphism) field with q elements. The field of formal Laurent series $\mathbb{F}_q((t))$ is a local field. The absolute value here is associated with the discrete valuation v_∞ defined by

$$v_\infty\left(a_k t^k + \cdots + a_0 + a_1 t + \cdots\right) = k$$

The associated valuation ring is the ring of formal power series, $\mathcal{O}_V = \mathbb{F}_q[[t]]$.

Remark 2.13.7. Later, we will show that every local field is one of the previous examples or a finite extension of one of them. That is, every local field is one of $\mathbb{R}, \mathbb{C}, \mathbb{Q}_p, \mathbb{F}_q((t))$ for some p or some q, or is a finite extension of $\mathbb{Q}_p$ for some p. (There are no nontrivial finite extension of $\mathbb{C}$, and a finite extension of $\mathbb{F}_q((t))$ is just some other field of the same type, with a different q.)

2.14 p-adic integers

Remark 2.14.1. Let p be a prime. We have a filtration

$$\mathbb{Z}_p^\times \supset 1 + p\mathbb{Z}_p \supset 1 + p^2\mathbb{Z}_p \supset \cdots$$

Definition 2.14.2. The **p-adic logarithm** is defined by

$$\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

Note that by the lim sup convergence test, this converges for $|x|_p < 1$ and diverges for $|x|_p > 1$. In particular, it gives a well defined function on $\mathbb{Z}_p$. It has the usual properties we associate with log.

$$\log(ab) = \log a + \log b$$

Definition 2.14.3. The **p-adic exponential** is defined by

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

By some uninteresting algebra, the lim sup of coefficients for this is $p^{\frac{1}{p-1}}$, so exp converges for x satisfying

$$|x|_p \leq p^{\frac{-1}{p-1}}$$

If $p \neq 2$, exp converges for $x \in p\mathbb{Z}_p$, and for $p = 2$, it converges for $x \in 4\mathbb{Z}_2$. When defined, exp has the usual properties we associated with exp.

$$\exp(a+b) = \exp a + \exp b \qquad \exp\log a = a \qquad \log\exp a = a$$

2.15 Ramified and unramified extensions

Definition 2.15.1. Let K be a complete nonarchimedean discretely valued field, and L/K a finite extension. Let k_K be the associated residue field of K and k_L the associated residue field of L. Note that $\mathcal{O}_K \subset \mathcal{O}_L$ and $\mathfrak{m}_K \subset \mathfrak{m}_L$, hence

$$k_K \hookrightarrow k_L$$

The **residual degree** is

$$f(L|K) = f_K^L = [k_K : k_L]$$

Definition 2.15.2. Let K be a complete nonarchimedean discretely valued field, and L/K a finite extension with $d = [L : K]$. Let $v_K : K^\times \to \mathbb{Z}$ be a normalized discrete valuation. Let $v_L : L^\times \to \mathbb{R}$ be the extension of v_K, and the we know that

$$\operatorname{im} v_L \subset \frac{1}{d}\mathbb{Z}$$

so v_L is also discrete. The **ramification degree** is

$$e(L|K) = e_K^L = e_{L/K} = [v_L(L^\times) : v_K(K^\times)]$$

That is, if π_K is a uniformizer for K and π_L is a uniformizer for L, then

$$(\pi_K) = \left(\pi_L^{e(L|K)}\right)$$

as ideals of $\mathcal{O}_L$.

Definition 2.15.3. Let $L, K, e_{L/K}, f_{L/K}$ be as above. If $e_{L/K} = 1$, then L/K is **unramified**. if $f_{L/K} = 1$, then L/K is **totally ramified**.

Definition 2.15.4. Let p be a prime. A **p-adic field** is a finite extension of $\mathbb{Q}_p$.

3 Theorems

3.1 Integral elements, integral closure, rings of integers

Proposition 3.1.1. *Let K be a number field and let $\alpha \in K$. Then $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial of α over $\mathbb{Q}$ has integer coefficients.*

Proposition 3.1.2. *Let $A \subset B$ be rings, and let $b \in B$. The following are equivalent.*

1. *b is integral over A.*
2. *$A[b]$ is a finitely generated A-module.*
3. *$A[b]$ is contained in a subring C where C is a finitely generated A-module.*
4. *There exists a faithful $A[b]$-module M which is finitely generated as an A-module.*

Proposition 3.1.3. *Let $A \subset B$ be rings, and suppose $b_1, \ldots, b_n \in B$ are integral over A. Then $A[b_1, \ldots, b_n]$ is a finitely generated A-module.*

Proposition 3.1.4. *Let $A \subset B$ be rings. The set of elements of B that are integral over A is a subring of B (containing A). (In particular, for a number field K, the algebraic integers $\mathcal{O}_K$ form a ring.)*

Note: In the following proposition, the hypothesis that α is algebraic is redudant, since L/K is finite (and hence algebraic), but we include it for emphasis.

Proposition 3.1.5. *Let A be an integral domain and $K = \mathrm{Frac}(A)$ be its fraction field, and let L/K be a finite field extension. If $\alpha \in L$ is algebraic over K, then there exists a nonzero $d \in A$ so that $d\alpha$ is integral over A.*

In particular, if L is a number field, then $L = \mathrm{Frac}(\mathcal{O}_L)$ and $L/\mathcal{O}_L$ is a torsion group.

Proof. As α is algebraic, we can write down a monic polynomial relation which is satisfies, with coefficients from K.

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$$

where $a_i \in K$. Let d be a common denominator for the a_i, so that $da_i \in A$, and muliply the equation by d^n.

$$d^n\alpha^n + \ldots + d^n a_1\alpha + d^n a_0 = (d\alpha)^n + \ldots + d^{n-1}a_1(d\alpha) + d^n a_0 = 0$$

Thus $d\alpha$ is integral over A.

For the other remark, we apply this to $A = \mathbb{Z}, K = \mathbb{Q}$, and the proposition says that for $\alpha \in L$, there exists $d \in \mathbb{Z}$ so that $d\alpha \in \mathcal{O}_L$, which is the condition for $L/\mathcal{O}_L$ to be a torsion group. □

Proposition 3.1.6. *A UFD is integrally closed. (In particular, $\mathbb{Z}$ is integrally closed.)*

Proposition 3.1.7. *Let $A_1 \subset A_2 \subset A_3$ be rings with A_2 integral over A_1 and A_3 integral over A_2. Then A_3 is integral over A_1.*

Proposition 3.1.8. *Let A be an integral domain and let $L = \mathrm{Frac}(A)$. Let F/L be a finite extension, and let $B \subset L$ be the integral closure of A. Then B is integrally closed in L.*

In particular, the ring of integers of a number field is integrally closed.

Proposition 3.1.9. *Let A be an integral domain and let $L = \mathrm{Frac}(A)$. Let F/L be a finite extension, and suppose A is integrally closed. Then $\alpha \in F$ is integral over A if and only if the minimal polynomial of α over L has coefficients in A.*

In particular, for a number field $K/\mathbb{Q}$ and $\alpha \in K$, $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial of α has coefficients in $\mathbb{Z}$.

Proposition 3.1.10. *Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer.*

- *If $d \equiv 2, 3 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.*
- *If $d \equiv 1 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.*

3.2 Norm, trace, and discriminant

Proposition 3.2.1 (Trace and norm are homomorphisms)**.** *Let $A \subset B$ be rings so that B is a free A-module of rank n. For $a \in A, b, b' \in B$,*

$$\begin{aligned} \mathrm{Tr}_A^B(b+b') &= \mathrm{Tr}_A^B(b) + \mathrm{Tr}_A^B(b') \\ \mathrm{Tr}_A^B(ab) &= a\,\mathrm{Tr}_A^B(b) \\ \mathrm{Tr}_A^B(a) &= na \\ \mathrm{N}_A^B(bb') &= \mathrm{N}_A^B(b)\,\mathrm{N}_A^B(b') \\ \mathrm{N}_A^B(a) &= a^n \end{aligned}$$

Thus $\mathrm{Tr}_A^B : B \to A$ is an A-module homomorphism, and $\mathrm{N}_A^B : B^\times \to A^\times$ is a group homomorphism.

Proposition 3.2.2 (Trace and norm behave well with towers)**.** *Let $K \subset E \subset L$ be a tower of finite field extensions. Then for $\beta \in L$,*

$$\mathrm{N}_K^L(\beta) = \mathrm{N}_K^E\, N_E^L(\beta) \qquad \mathrm{Tr}_K^L(\beta) = \mathrm{Tr}_K^E\,\mathrm{Tr}_E^L(\beta)$$

Proposition 3.2.3 (Norm and trace in the characteristic polynomial)**.** *Let $T : V \to V$ be a linear transformation, with $\dim V = n$. Then*

$$c_T(x) = x^n - \mathrm{Tr}(T)x^{n-1} + \ldots + (-1)^n \det(T)$$

Proposition 3.2.4. *Let L/K be a finite field extension and let $\alpha \in L$ and let $f \in K[x]$ be the minimal polynomial of α. Then*

$$c_\alpha(x) = f(x)^{[L:K(\alpha)]}$$

Proposition 3.2.5 (Norm and trace in terms of Galois conjugates)**.** *Let L/K be a finite separable field extension and let $\alpha \in L$. Let $\alpha_1, \ldots, \alpha_r$ be the roots of the minimal polynomial of α (in some splitting field containing L). Let $n = [L : K(\alpha)]$. Then*

$$\mathrm{Tr}_K^L(\alpha) = n \sum_{i=1}^{r} \alpha_i \qquad \mathrm{N}_K^L(\alpha) = \left(\prod_{i=1}^{r} \alpha_i \right)^n$$

Proposition 3.2.6. *Let A be an integrally closed domain, and let $K = \mathrm{Frac}(A)$, and let L/K be a finite extension. If $\beta \in L$ is integral over A, then $\mathrm{Tr}_K^L(\beta), \mathrm{N}_K^L(\beta) \in A$.*

Proposition 3.2.7 (Discriminant well defined up to squares)**.** *Let $\phi : V \times V \to K$ be a bilinear form on a finite dimensional K-vector space V. If $\{e_1, \ldots, e_n\}$ and $\{f_1, \ldots, f_n\}$ are bases for V, then*

$$D_\phi(e_1, \ldots, e_n) = \lambda^2 D_\phi(f_1, \ldots, f_n)$$

for some nonzero $\lambda \in K$.

Proposition 3.2.8. *Let $\phi : V \times V \to K$ be a bilinear form on a finite dimensional K-vector space V. The following are equivalent.*

1. *ϕ is nondegenerate.*
2. *ϕ has trivial left kernel (the left kernel is $\{v \in V : \phi(v, u) = 0, \forall u \in V\}$).*
3. *ϕ has trivial right kernel (analogous to left kernel).*
4. *The map $V \to V^*, v \mapsto \big(x \mapsto \phi(v, x)\big)$ is injective.*
5. *The map $V \to V^*, v \mapsto \big(x \mapsto \phi(x, v)\big)$ is injective.*
6. *The map $V \to V^*, v \mapsto \big(x \mapsto \phi(v, x)\big)$ is an isomorphism.*
7. *The map $V \to V^*, v \mapsto \big(x \mapsto \phi(x, v)\big)$ is an isomorphism.*

Proposition 3.2.9. *Let $A \subset B$ be rings, so that B is a free A-module. If $\{\beta_1, \ldots, \beta_n\}$ and $\{\gamma_1, \ldots, \gamma_n\}$ are basis for B over A, and $\gamma_j = \sum_i a_{ij}\beta_i$, then*

$$D(\beta_1, \ldots, \beta_n) = \det(a_{ij})^2 D(\gamma_1, \ldots, \gamma_n)$$

Since $(a_i j)$ is a change of basis matrix, its determinant is a unit in A, so this says that the discriminant is well-defined up to multiplication by squares of units in A, hence there is an equality of ideals

$$\Big(D(\beta_1, \ldots, \beta_n)\Big) = \Big(D(\gamma_1, \ldots, \gamma_n)\Big)$$

Proposition 3.2.10. *Let L/K be a finite field extension. Then L/K is separable if and only if the trace form is nondegenerate.*

Proposition 3.2.11 (Norm and trace in terms of Galois conjugates again)**.** *Let L/K be a finite separable field extension, and set $n = [L : K]$. Fix a separable closure L^{sep} of L, and let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of L into L^{sep} that are the identity when restricted to K. Then for $\beta \in L$,*

$$\mathrm{Tr}_K^L(\beta) = \sum_{i=1}^{n} \sigma_i(\beta) \qquad \mathrm{N}_K^L(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$$

Proposition 3.2.12. *Let L/K be a finite separable field extension and set $n = [L : K]$. Let $\sigma_1, \ldots, \sigma_n : L \to L^{\text{sep}}$ be the distinct embeddings with $\sigma_i|_K = \mathrm{Id}_K$. If $\{\beta_1, \ldots, \beta_n\}$ is a basis of L/K, then*

$$D(\beta_1, \ldots, \beta_n) = \det\Big((\sigma_i(\beta_j)\Big)^2$$

Proof. By definition of the discriminant,

$$D(\beta_1, \ldots, \beta_n) = \det\Big(\mathrm{Tr}_K^L(\beta_i\beta_j)\Big)$$

Using Proposition 3.2.11,

$$\mathrm{Tr}_K^L(\beta_i\beta_j) = \sum_{k=1}^{n} \sigma_k(\beta_i\beta_j) = \sum_{k=1}^{n} \sigma_k(\beta_i)\sigma_k(\beta_j)$$

thus

$$\begin{aligned}
\det\Big(\mathrm{Tr}_K^L(\beta_i\beta_j)\Big) &= \det\left(\sum_{k=1}^{n} \sigma_k(\beta_i)\sigma_k(\beta_j)\right) \\
&= \det\Big(\sigma_k(\beta_i)\Big)\det\Big(\sigma_k(\beta_j)\Big) \\
&= \det\Big(\sigma_k(\beta_j)\Big)^2
\end{aligned}$$

□

Proposition 3.2.13. *Let $L = K(\alpha)$ so that L/K is finite separable of degree n, and let $f(x) \in K[x]$ be the minimal polynomial of α. Then the discriminant of L/K with respect to the basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is*

$$D(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_K^L(f'(\alpha))$$

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings $L \to L^{\text{sep}}$ which fix K, so that $\alpha_i = \sigma_i(\alpha)$ are the distinct roots of $f(x)$. We apply Proposition 3.2.12 with $\beta_j = \alpha^{j-1}$ to get

$$D(1, \alpha, \ldots, \alpha^{n-1}) = \det\Big(\sigma_i(\alpha^{j-1})\Big)^2 = \det(\alpha_i^{j-1})^2$$

This is a Vandermonde determinant (Proposition 1.2.1), so we may compute it as

$$\det(\alpha_i^{j-1})^2 = \left(\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)\right)^2 = (-1)^{\frac{n(n-1)}{2}}\prod_{i\neq j}(\alpha_i-\alpha_j)$$
$$= (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\left(\prod_{j\neq i}(\alpha_i-\alpha_j)\right) = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n} f'(\alpha_i)$$

The last equality comes from the product rule.

$$(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\sigma_i(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} N_K^L(f'(\alpha))$$

□

Remark 3.2.14. We should clarify the relationship between discriminants of number fields and discriminants of polynomials, because they are very closely related. Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n, with roots $\alpha_1, \dots, \alpha_n \in \mathbb{Q}^{\mathrm{al}}$. Let $\alpha = \alpha_1$, and consider the number field $K = \mathbb{Q}(\alpha)/\mathbb{Q}$, with $[K:\mathbb{Q}] = n$. Note that $\alpha \in \mathcal{O}_K$, since f is monic. In the process of the above proof, we showed that

$$D(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}}\prod_{i\neq j}(\alpha_i-\alpha_j)$$

By definition, the discriminant of f is

$$\operatorname{disc}(f) = a_n^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2 = \prod_{i\neq j}(\alpha_i-\alpha_j)$$

where $a_n = 1$ is the leading coefficient of f. By 3.2.19, we have

$$D(1, \alpha, \dots, \alpha^{n-1}) = \left[\mathcal{O}_K : \mathbb{Z}[\alpha]\right]^2 \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$$

Putting this together,

$$\pm\operatorname{disc}(f) = \left[\mathcal{O}_K : \mathbb{Z}[\alpha]\right]^2 \Delta_K$$

That is, the discriminant of a polynomial is "the same" as the discrimiant of the number field determined by one of its roots, up to sign and multiplication by a square (the square is measuring how "far off" the ring of integers $\mathcal{O}_K$ is from being what it "should be", namely $\mathbb{Z}[\alpha]$).

One thing we can notice from this is that $\operatorname{disc}(f)$ is unaffected by a $\mathbb{Q}$-linear change of variables (a substitution $x = ay + b$ with $a, b \in \mathbb{Q}$), since a $\mathbb{Q}$-linear transformation of $\alpha \in K$ does not affect the extension field $K = \mathbb{Q}(\alpha) = \mathbb{Q}(a\alpha + b)$.

Proposition 3.2.15. *Let A be an integrally closed domain. Let $K = \operatorname{Frac}(A)$ and L/K be a finite separable extension of degree n. Let B be the integral closure of A in L. Then B is a submodule of a free A-module of rank n.*

In particular, if A is a PID, then B is a free A-module of rank n. Even more concretely, if $K/\mathbb{Q}$ is a number field, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$.

Proposition 3.2.16. *Let $p \in \mathbb{Z}$ be a prime, and let ζ be a primitive pth root of unity. The ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$, and the discriminant of $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$ is $\pm p^{p-2}$.*

Proposition 3.2.17. *Let $K/\mathbb{Q}$ be a number field with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ is the largest subring of K that is finitely generated as a $\mathbb{Z}$-module.*

Proposition 3.2.18. *Let $A \subset B$ be integral domains, so that B is a free A-module of rank m, and suppose $\operatorname{disc}(B/A) \neq 0$. Then elements $\gamma_1, \ldots, \gamma_m$ form a basis of B over A if and only if we have the following equality of ideals of A.*

$$\Big(D(\gamma_1, \ldots, \gamma_m)\Big) = \Big(\operatorname{disc}(B/A)\Big)$$

Remark 3.2.19. In the previous proposition, with the case $A = \mathbb{Z}$, this says that $\{\gamma_1, \ldots, \gamma_m\}$ is a basis of B if and only if $D(\gamma_1, \ldots, \gamma_m) = \operatorname{disc}(B/\mathbb{Z})$. Thus if $N = \bigoplus_i \mathbb{Z}\gamma_i$, then

$$D(\gamma_1, \ldots, \gamma_m) = [B : N]^2 \operatorname{disc}(B/\mathbb{Z})$$

which gives the following useful criterion.

Proposition 3.2.20. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, with $\alpha \in \mathcal{O}_K$. If $D(1, \alpha, \ldots, \alpha^{n-1})$ is square-free, then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

Proof. In the language of the previous remark 3.2.19, we have $B = \mathcal{O}_K, \gamma_i = \alpha^{i-1}$ and $N = \mathbb{Z}[\alpha]$. Since $D(1, \alpha, \ldots, \alpha^{n-1}) = [\mathcal{O}_K : \mathbb{Z}[\zeta]]^2 \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$ is square free, we get $[\mathcal{O}_K : \mathbb{Z}[\zeta]]^2 = 1$, which says that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. □

3.3 Dedekind domains, unique factorization

Proposition 3.3.1. *Let R be an integral domain. Then R is a DVR if and only if R is Noetherian, integrally closed, and has a unique nonzero prime ideal.*

Proposition 3.3.2. *Let A be a Dedekind domain, and let $K = \operatorname{Frac}(A)$. Let L/K be a finite separable extension, and let B be the integral closure of A in L. Then B is a Dedekind domain.*

In particular, in the case $A = \mathbb{Z}, K = \mathbb{Q}$, we have $B = \mathcal{O}_L$, so the ring of integers of a number field is a Dedekind domain.

Proposition 3.3.3. *Let A be an integral domain, and let $S \subset A$ be a multiplicative subset.*

1. *If A is Noetherian, then $S^{-1}A$ is Noetherian.*
2. *If A is integrally closed, then $S^{-1}A$ is integrally closed.*
3. *If A is a Dedekind domain, then $S^{-1}A$ is a Dedekind domain.*

Proposition 3.3.4. *A Noetherian integral domain A is a Dedekind domain if and only if for every nonzero prime ideal $\mathfrak{p} \subset A$, $A_{\mathfrak{p}}$ is a DVR.*

Proposition 3.3.5 (Unique factorization of ideals in Dedekind domains)**.** *Let A be a Dedekind domain. Then every proper nonzero ideal $\mathfrak{a} \subset A$ can be written uniquely in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_n^{e_n}$$

where $\mathfrak{p}_i$ are distinct prime ideals, and $r_i \in \mathbb{Z}_{>0}$.

Proof. Uses the following three lemmas, and some additional work on top of that. □

Lemma 3.3.6. *Let A be a Noetherian ring. Then every nonzero ideal $\mathfrak{a} \subset A$ contains a product of prime ideals.*

Lemma 3.3.7. *Let A be a ring, and let $\mathfrak{a}, \mathfrak{b} \subset A$ be relatively prime ideals ($\mathfrak{a} + \mathfrak{b} = A$). Then for $m, n \in \mathbb{Z}_{\geq 0}$, $\mathfrak{a}^n, \mathfrak{b}^n$ are relatively prime.*

Lemma 3.3.8. *Let A be an integral domain, and $\mathfrak{p} \subset A$ a maximal ideal. Set $\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$. Then the map*

$$A/\mathfrak{p}^m \to A_\mathfrak{p}/\mathfrak{q}^m \qquad a + \mathfrak{p}^m \mapsto a + \mathfrak{q}^m$$

is an isomorphism for all $m \in \mathbb{N}$.

Proposition 3.3.9. *Let A be a Dedekind domain, and let $\mathfrak{a}, \mathfrak{b} \subset A$ be ideals. Then $\mathfrak{a} \subset \mathfrak{b}$ if and only if $\mathfrak{a}A_\mathfrak{p} \subset \mathfrak{b}A_\mathfrak{p}$ for all nonzero prime ideals $\mathfrak{p} \subset A$.*

Proof. Quick corollary of unique factorization of ideals, and the fact that $A_\mathfrak{p}$ is a DVR. □

Remark 3.3.10. The following proposition isn't very useful, but it gives a nice characterization of how Dedekind domains are not very far from being PIDs. Not every ideal is generated by one element, but every ideal can be generated by two elements.

Proposition 3.3.11. *Let A be a Dedekind domain, and let $\mathfrak{a} \subset \mathfrak{b} \subset A$ be nonzero ideals of A. Then $\mathfrak{a} = \mathfrak{b} + (a)$ for some $a \in A$. In particular, if $\mathfrak{a} \subset A$ is a nonzero ideal and $a \in \mathfrak{a}$ is nonzero, there exists $b \in \mathfrak{a}$ so that $\mathfrak{a} = (a, b)$.*

Proposition 3.3.12. *Let A be a Dedekind domain. Then A is a PID if and only if it is a UFD.*

Proposition 3.3.13. *Let A be a Dedekind domain. Then the set $\mathrm{Id}(A)$ a group with respect to the product operation. More concretely, it is the free abelian group generated by the set of nonzero prime ideals of A.*

Proof. Check that any nonzero integral $\mathfrak{a} \subset A$ is invertible in $\mathrm{Id}(A)$ with inverse

$$\mathfrak{a}^{-1} = \{a \in K : a\mathfrak{a} \subset A\}$$

The rest of the requirements essentially come from unique factorization. □

Proposition 3.3.14. *Let A be a Dedekind domain with $|\mathrm{Cl}(A)| = n$ (in particular, it is finite). Choose representative ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset A$. Let $b \in \bigcap_{i=1}^n \mathfrak{a}_i$, and let $S = \{1, b, b^2, \dots\}$. Then $S^{-1}A$ is a PID.*

Proposition 3.3.15. *Let $\mathfrak{a}, \mathfrak{b}$ be nonzero ideals of a Dedekind domain. Then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.*

3.4 Factorization of primes, ramification

Remark 3.4.1. In the following proposition, $\dim A = 1$ refers to Krull dimension, and $\dim A = 1$ is equivalent to saying that every prime ideal of A is maximal.

Lemma 3.4.2. *Let $A \subset B$ be rings, with $\dim A = 1$, and let $\mathfrak{p} \subset A, \mathfrak{q} \subset B$ be prime ideals. Then*

$$\mathfrak{q} \cap A = \mathfrak{p} \iff \mathfrak{p}B \subset \mathfrak{q}$$

Or in the notation of Atiyah-MacDonald Proposition 1.17,

$$\mathfrak{q}^c = \mathfrak{p} \iff \mathfrak{p}^e \subset \mathfrak{q}$$

Proof. If $\mathfrak{q}^c = \mathfrak{p}$, then $\mathfrak{p}^e = \mathfrak{q}^{ec}$, and $\mathfrak{q}^{ec} \subset \mathfrak{q}$ by Atiyah-MacDonald 1.17(i). For the converse, suppose $\mathfrak{p}^e \subset \mathfrak{q}$. Then $\mathfrak{p} = \mathfrak{p}^{ece} \subset \mathfrak{q}^{ce} \subset \mathfrak{q}$ so $\mathfrak{p} \subset \mathfrak{q}^c = \mathfrak{q} \cap A$. Since $\dim A = 1$, ever prime ideal is maximal, so this forces $\mathfrak{q}^c = \mathfrak{p}$ or $\mathfrak{q}^c = A$. The latter is impossible, since $\mathfrak{q} \subset B$ is proper, thus $\mathfrak{p} = \mathfrak{q}^c$. □

Proposition 3.4.3. *Let A be a Dedekind domain and let $K = \mathrm{Frac}(A)$. Let L/K be a finite separable extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \subset A$ be a prime ideal. A prime ideal $\mathfrak{q} \subset B$ appears in the factorization of $\mathfrak{p}B$ if and only if $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. We know that B is Dedekind, so we have a unique factorization into prime ideals of B,

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

If $\mathfrak{q} = \mathfrak{P}_i$ for some i, then $\mathfrak{p}B \subset \mathfrak{q}$, which by Lemma 3.4.2 implies that $\mathfrak{q} \cap A = \mathfrak{p}$. Conversely, if $\mathfrak{q} \cap A = \mathfrak{p}$, then $\mathfrak{p}B \subset \mathfrak{q}$ by Lemma 3.4.2. By Proposition 1.10(i) of Atiyah-MacDonald,

$$\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} = \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i} \subset \mathfrak{q}$$

and then by Proposition 1.11(i) of Atiyah-MacDonald, $\mathfrak{P}_i^{e_i} \subset \mathfrak{q}$ for some i. Then we have an inclusion of radical ideals $\sqrt{\mathfrak{P}_i^{e_i}} \subset \sqrt{\mathfrak{q}}$, but by Exercise 1.13 of Atiyah-MacDonald, since $\mathfrak{P}_i$ and $\mathfrak{q}$ are prime,

$$\mathfrak{P}_i = \sqrt{\mathfrak{P}_i^{e_i}} \subset \sqrt{\mathfrak{q}} = \mathfrak{q}$$

Then since every prime ideal in B is maximal, the chain of proper nonzero ideals $\mathfrak{P}_i \subset \mathfrak{q}$ forces $\mathfrak{P}_i = \mathfrak{q}$. □

Proposition 3.4.4 (Fundamental Relation)**.** *Let A be a Dedekind domain, and let $K = \mathrm{Frac}(A)$. Let L/K be a finite separable field extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \subset A$ be a prime ideal, and factor $\mathfrak{p}B$ into a product of prime ideals of B,*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

Then

$$\sum_{i=1}^{r} e_i f_i = [L : K] = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B$$

Proposition 3.4.5. *With the same hypotheses as Proposition 3.4.4, also suppose L/K is Galois. Then* $\mathrm{Gal}(L/K)$ *acts transitively on the prime factors of $\mathfrak{p}B$. That is, for any $\mathfrak{p}_i, \mathfrak{P}_j$ appearing in the factorization of $\mathfrak{p}B$, there exists $\sigma \in \mathrm{Gal}(L/K)$ so that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.*

Proposition 3.4.6 (Fundamental Relation for Galois Extensions)**.** *With the same hypotheses as Proposition 3.4.4, also suppose L/K is Galois. Then*

$$e_1 = \ldots = e_r \qquad f_1 = \ldots = f_r$$

Set $e = e_1, f = f_1$. Then

$$efr = [L : K]$$

Proposition 3.4.7. *Let $K \subset L$ be number fields, and let $A \subset K$ be a Dedekind domain, and let B be the integral closure of A in L. Let $\mathfrak{p} \subset A$ be a prime ideal. Then $\mathfrak{p}$ ramifies in L if and only if $\mathfrak{p}$ divides $\mathscr{D}_{B/A}$. In particular, only finitely many primes ramify.*

Remark 3.4.8. As an example of Proposition 3.4.7, consider a quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. If $d \equiv 2, 3 \bmod 4$, then the discriminant is $4d$, so the only primes that ramify are 2 and primes dividing d.

Remark 3.4.9. As an example of Proposition 3.4.7, consider an odd prime $p \in \mathbb{Z}$ and the cyclotomic extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. The discriminant is $\pm p^{p-2}$, so the only prime that ramifies is $p\mathbb{Z}$.

Proposition 3.4.10. *Let A be a Dedekind domain, and $K = \mathrm{Frac}(A)$, and L/K a finite separable extension, and let B be the integral closure of A in L. Suppose $B = A[\alpha]$, and let $f \in A[x]$ be the minimal polynomial of α over K. Let $\mathfrak{p} \subset A$ be a prime ideal, and suppose that*

$$\left(f(x) = \prod_{i=1}^{r} g_i(x)^{e_i} \right) \bmod \mathfrak{p}$$

with $g_1, \ldots, g_r$ distinct and irreducible mod $\mathfrak{p}$. Then $\mathfrak{p}B$ factors as

$$\mathfrak{p}B = \prod_{i=1}^{r} \left(\mathfrak{p}, g_i(\alpha)\right)^{e_i}$$

and

$$B/\left(\mathfrak{p}, g_i(\alpha)\right) \cong \left(A/\mathfrak{p}\right)[x]/\overline{g}_i$$

so $f_i = \deg g_i$.

Proposition 3.4.11. *Let A be a Dedekind domain, and $K = \mathrm{Frac}(A)$, and L/K a finite separable extension, and let B be the integral closure of A in L. Let $\mathfrak{p} \subset A$ be a prime ideal, and suppose $\exists \theta \in L$ such that the integral closure of $A_\mathfrak{p}$ in L is $A_\mathfrak{p}[\theta]$. Let $f \in A_\mathfrak{p}[x]$ be the minimal polynomial of θ over K, and suppose*

$$\left(f = \prod_{i=1}^{r} g_i(x)^{e_i} \right) \bmod p$$

Then

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$$

where $\mathfrak{P}_i = (\mathfrak{p}, g_i(\alpha))$.

Proof. See Janusz Chapter 1, Theorem 7.4. □

Proposition 3.4.12. *Let A be a Dedekind domain, and $K = \mathrm{Frac}(A)$, and L/K a finite separable extension, and let B be the integral closure of A in L. Suppose $\exists \theta \in B$ such that $L = K(\theta)$, and let*

$$D = D(1, \theta, \ldots, \theta^{n-1}) = \mathrm{disc}(L/K)$$

Then for $\mathfrak{p} \subset A$ prime so that $D \notin \mathfrak{p}$, we have $S^{-1}B = A_{\mathfrak{p}}[\theta]$. (In particular, the previous theorem can be used to factor any such prime.)

Proof. See Janusz Chapter 1, Theorem 7.5. □

Proposition 3.4.13. *Let $p \in \mathbb{Z}$ be an odd prime. The following are equivalent.*

1. $p \equiv 1 \bmod 4$.
2. *p splits completely in $\mathbb{Z}[i]$.*
3. *p is a sum of two squares.*

3.5 Quadratic extensions

In this section, we summarize all the various theory applied in the relatively concrete case of quadratic number fields.

Proposition 3.5.1. *Let $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. If $d \equiv 2, 3 \bmod 4$, then*

1. $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$
2. $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = 4d$
3. *Primes that ramify are 2 and divisors of d.*
4. *The minimal polynomial of $\sqrt{d}$ is $f(x) = x^2 - d$.*
5. *Let $p \in \mathbb{Z}$ be a prime. Then*

$$p\mathcal{O}_K = \begin{cases} \mathfrak{P}_1^2 & p = 2 \text{ or } p|d \\ \mathfrak{P}_1\mathfrak{P}_2 & p \neq 2 \text{ and } p \nmid d \end{cases}$$

6. *In the first case above, $e = f = 1, r = 2$. In the second case, $e = 2, f = r = 1$.*

If $d \equiv 1 \bmod 4$, then

1. $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$
2. $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = d$
3. *Primes that ramify are divisors of d.*
4. *The minimal polynomial of $\sqrt{d}$ is $f(x) = x^2 - x + \frac{1-d}{2}$.*

5. *Let $p \in \mathbb{Z}$ be a prime. Then*

$$p\mathcal{O}_K = \begin{cases} \mathfrak{P}_1^2 & p|d \\ \mathfrak{P}_1\mathfrak{P}_2 & p \nmid d \end{cases}$$

6. *In the first case above, $e = f = 1, r = 2$. In the second case, $e = 2, f = r = 1$.*

3.6 Lagrange's theorem on sum of four squares

Definition 3.6.1. Let A be a commutative ring. The **quaternion algebra** over A is the four-dimensional A-algebra $\mathbb{H}(A)$ with basis $1, i, j, ij$ and relations

$$i^2 = j^2 = -1 \qquad ij = -ji$$

Note that $\mathbb{H}(A)$ is an associative algebra. For $q = a + bi + cj + dij \in \mathbb{H}(A)$, the **conjugate** of q is

$$\overline{q} = a - bi - cj - dij$$

The **reduced norm** of q is $N(z) = q\overline{q}$.

Lemma 3.6.2 (Properties of conjugation)**.** *Conjugation is an involution of $\mathbb{H}(A)$. That is, it is an anti-homomorphism of order 2. Explicitly, this means*

$$\overline{z + z'} = \overline{z} + \overline{z'} \qquad \overline{zz'} = \overline{z}\overline{z'} \qquad \overline{\overline{z}} = z$$

Lemma 3.6.3 (Properties of norm)**.** *Norm has the following properties.*

1. *$N(a + bi + cj + dij) = a^2 + b^2 + c^2 + d^2$*
2. *For $q, z \in \mathbb{H}(A)$, $N(qz) = N(q)N(z)$.*
3. *$z \in \mathbb{H}(A)$ is a unit if and only if $N(z)$ is a unit in A.*

Definition 3.6.4. The **Hurwitz quaternions** are

$$H = \left\{ a + bi + cj + dij | a, b, cd \in \mathbb{Z} \text{ or } a, b, c, d \in \frac{1}{2}\mathbb{Z} \right\}$$

Note that $\mathbb{H}(\mathbb{Z}) \subset H \subset \mathbb{H}(\mathbb{Q})$.

Lemma 3.6.5. *The Hurwitz quaternions have the following properties, as a subalgebra of $\mathbb{H}(\mathbb{Q})$.*

1. *H is closed under conjugation.*
2. *For $z \in H$, $z + \overline{z} \in \mathbb{Z}$ and $N(z) \in \mathbb{Z}$.*
3. *$z \in H$ is a unit if and only if $N(z) = 1$.*
4. *Every left or right ideal of H is principal.*

Lemma 3.6.6. *Let $\mathbb{F}_q$ be the finite field with q elements. Any $\alpha \in \mathbb{F}_q$ can be written as a sum of two squares in $\mathbb{F}_q$.*

Theorem 3.6.7 (Lagrange)**.** *Every natural number is a sum of four squares.*

Proof. Covered in class. Note that the proof does not really utilize techniques and concepts developed in this class. □

3.7 Discrete valuations

Proposition 3.7.1. *Let $v : K^\times \to \mathbb{Z}$ be a discrete valuation.*

1. *If $c \in K^\times$ is an element of finite order, then $v(c) = 0$. Consequently, $v(a) = v(-a)$ for all $a \in K^\times$.*
2. *If $a, b \in K^\times$ with $v(a) > v(b)$, then $v(a + b) = v(b)$.*
3. *If $a_1, \ldots, a_n \in K^\times$ with $a_1 + \ldots + a_n = 0$, then the minimal value of $v(a_i)$ is attained for at least two indices i.*

Proposition 3.7.2. *Let A be a Dedekind domain, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset A$ be nonzero distinct prime ideals. Let $v_{\mathfrak{p}_1}, \ldots, v_{\mathfrak{p}_n}$ be the corresponding discrete valuations on $\mathrm{Frac}(A)$. Let $x_1, \ldots, x_n \in A$. Then for every integer m, there exists $x \in A$ so that $v_{\mathfrak{p}_i}(x - x_i) > n$ for $1 \leq i \leq n$.*

Proof. This is just a restatement of the Chinese Remainder Theorem in terms of discrete valuations. □

3.8 Eisenstein extensions

We generalize Eisenstein's criterion to a more general setting. First, recall the original statement.

Proposition 3.8.1 (Eisenstein's criterion, original version)**.** *Let p be a prime. If*

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

satisifes $p | a_i$ for $i = 0, \ldots, m-1$ and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Z}[x]$

Proposition 3.8.2 (Generalized Eisenstein's criterion)**.** *Let A be a Dedekind domain, and let $K = \mathrm{Frac}(A)$. Let $f \in A[x]$ be Eisenstein at a prime ideal $\mathfrak{p}$. Then $f \in K[x]$ is irreducible, and if $\alpha \in K^{\mathrm{sep}}$ is a root of f, then $\mathfrak{p}$ is totally ramified in $K(\alpha)$, and $v_{\mathfrak{p}}(\alpha) = 1$.*

Furthermore, if L/K is a separable extension, and B is the integral closure of A in L, then $\mathfrak{p}B$ factors into prime ideals as

$$\mathfrak{p}B = (p, \alpha)^{\deg f}$$

Note that the original verion is the case where $A = \mathbb{Z}$.

3.9 Finiteness of the class group, lattice theory

Lemma 3.9.1. *Let K be a number field, and let $n \in \mathbb{Z}_{\geq 1}$. There are only finitely many ideals in $\mathcal{O}_K$ with norm n.*

Proof. Let $\mathfrak{a} \subset \mathcal{O}_K$, with $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| = n$. Then $n \in \mathbb{Z} \subset \mathcal{O}_K$, so viewing the class of n as element of $|\mathcal{O}_K/\mathfrak{a}|$, we have $\overline{n} = 0$, since it is a group of order n. Thus $n \in \mathfrak{a}$, so $(n) \subset \mathfrak{a}$. Thus $\mathfrak{a}$ corresponds to an ideal of the finite ring $|\mathcal{O}_K/(n)|$. Since this ring is finite, it has only finitely many ideals, so there can be only finitely many such $\mathfrak{a}$. □

Proposition 3.9.2. *Let V be a finite dimensional real vector space, and $\Lambda \subset V$ be a subgroup. The following are equivalent.*

1. *Λ is a lattice.*
2. *Λ is a discrete subgroup.*
3. *There is an open subset $U \subset V$ such that $U \cap \Lambda = \{0\}$.*
4. *Each compact subset of V intersects Λ in a finite set.*
5. *Each bounded subset of V intersects Λ in a finite set.*

Proposition 3.9.3. *Let $\Lambda \subset \mathbb{R}^n$ be a full lattice, and $S \subset \mathbb{R}^n$ be a measureable subset such that $\mu(S) > V(\Lambda)$. Then there exist distinct $x, y \in S$ so that $x - y \in \Lambda$.*

Theorem 3.9.4 (Minkowski Convex Body Theorem)**.** *Let $\Lambda \subset \mathbb{R}^n$ be a full lattice, and $S \subset \mathbb{R}^n$ be a measurable subset, which is convex and symmetric about the origin. If*

$$\mu(S) > 2^n V(\Lambda)$$

or

$$\mu(S) \geq 2^n V(\Lambda) \text{ and } S \text{ is compact}$$

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

Proposition 3.9.5. *Let $r_1, r_2 \in \mathbb{N}, n = n_1 + 2r_2$. For $t \in \mathbb{R}_{\geq 0}$, set*

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

Let μ denote Lebesgue measure on $\mathbb{R}^n \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Then

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

Proof. See Milne [**?**] Lemma 4.22, or Janusz Chapter 1, Proposition 12.4. Professor Rapinchuk noted that in the case $r_1 = r_2 = 1$, we can actually visualize B_t as two cones glued at their circular ends, and in this case the measure computation is immediate. □

Proposition 3.9.6. *Let K be a number field with canonical embeddings σ. If $M \subset K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ with basis $\{x_1, \ldots, x_n\}$, then $\sigma(M)$ is a lattice in $\mathbb{R}^n$ whose volume is*

$$V(\sigma(M)) = 2^{-r_2} |\det(\sigma_j(x_i))|$$

Recall that $\Delta_K = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$.

Proposition 3.9.7. *Let $K/\mathbb{Q}$ be a number field with canonical embedding σ, and let $n = [K : \mathbb{Q}]$. Let $\mathfrak{a} \subset \mathcal{O}_K$ be a nonzero ideal. Then $\sigma(\mathcal{O}_K)$ and $\sigma(\mathfrak{a})$ are full lattices in $\mathbb{R}^n$, with volumes*

$$V(\sigma(\mathcal{O}_K)) = 2^{-r_2} |\Delta_K|^{1/2}$$
$$V(\sigma(\mathfrak{a})) = 2^{-r_2} |\Delta_K|^{1/2} N(\mathfrak{a})$$

Proposition 3.9.8. *Let $K/\mathbb{Q}$ be a number field, and let $\mathfrak{a} \subset \mathcal{O}_K$ be a nonzero ideal. Then there exists a nonzero $x \in \mathfrak{a}$ so that*

$$|N(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\Delta_K|^{1/2} N(\mathfrak{a})$$

Lemma 3.9.9 (Arithmetic mean-geometric mean inequality)**.** *If $a_1, \ldots, a_n \in \mathbb{R}_{\geq 0}$, then the geometric mean is less than or equal to the arithmetic mean. Symbolically,*

$$\left(\prod_{i=1}^{n} a_i\right)^{1/n} \leq \frac{1}{n} \sum_{i=1}^{n} a_i$$

Proposition 3.9.10 (Hermite-Minkowski bound)**.** *Let K be a number field. Every class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an integral ideal $\mathfrak{b}$ satisfying*

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|}$$

Theorem 3.9.11. *Let K be a number field. The class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

Theorem 3.9.12. *Let K be a number field, with $K \neq \mathbb{Q}$. The discriminant Δ_K is not ± 1.*

Theorem 3.9.13 (Hermite-Minkowski)**.** *There does not exist a number field K which is unramified over $\mathbb{Q}$. (Note that this fails if we replace $\mathbb{Q}$ with another number field.)*

Corollary 3.9.14. *There does not exist an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ with $\deg f > 1$ so that the discriminant of f is ± 1.*

Theorem 3.9.15 (Hermite-Minkowski)**.** *There are only finitely many number fields with a given discriminant.*

3.10 Class groups of quadratic number fields

Remark 3.10.1. Let K be any field, and let $K(\alpha)$ be a Galois extension with primitive element α. Then for $\sigma \in \mathrm{Gal}(K(\alpha)/K)$, $\sigma\alpha$ is also a primitive element, that is, $K(\alpha) = K(\sigma\alpha)$. Viewing σ as an automorphism $K(\alpha) \to K(\alpha)$ note that the image is also $K(\sigma\alpha)$, so it must be that they are equal.

Proposition 3.10.2. *If $K/\mathbb{Q}$ is Galois, then K is either totally real or totally imaginary.*

Proof. Let K be the splitting field of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. If f has no real roots, then K is totally imaginary. By the previous remark, if any root of f is real, then it is a primitive element, so all other roots can be written in terms of it and elements of $\mathbb{Q}$, so all roots are real, and K is totally real. □

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with d square-free. Let r_1, r_2 be the number of real embeddings and complex embeddings, respectively. Since every quadratic extension is Galois, by 4.3.3 $K/\mathbb{Q}$ is totally real or totally imaginary, so there are two possibilities:

1. $r_1 = 2, r_2 = 0$. In this case the Minkowski bound is $N(\mathfrak{a}) \leq \frac{1}{2}\sqrt{|\Delta_K|}$

2. $r_1 = 0, r_2 = 1$. In this case the Minkowski bound is $N(\mathfrak{a}) \leq \frac{2}{\pi}\sqrt{|\Delta_K|}$

If the Minkowski bound is < 2, then $\mathrm{Cl}(K)$ is trivial, since nontrivial elements of $\mathrm{Id}(\mathcal{O}_K)$ have norm at least 2. Thus the following result.

Proposition 3.10.3. *Let K be a quadratic number field, with r_1 real embeddings and r_2 complex embeddings.*

1. *If $r_1 = 2, r_2 = 0$ and $|\Delta_K| < 16$, then $\mathrm{Cl}(K)$ is trivial.*

2. *If $r_1 = 0, r_2 = 1$ and $|\Delta_K| < \pi^2$, then $\mathrm{Cl}(K)$ is trivial.*

Recall that if $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer, then

$$\Delta_K = \begin{cases} 4d & d \equiv 2, 3 \bmod 4 \\ d & d \equiv 1 \bmod 4 \end{cases}$$

Using this, we can give refine the previous result to 4 separate cases.

Proposition 3.10.4. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, with r_1 real embeddings and r_2 complex embeddings.*

1. *If $d \equiv 2, 3 \bmod 4$ and $r_1 = 2, r_2 = 0$ and $|d| < 4$, then $\mathrm{Cl}(K)$ is trivial.*

2. *If $d \equiv 1 \bmod 4$ and $r_1 = 2, r_2 = 0$ and $|d| < 16$, then $\mathrm{Cl}(K)$ is trivial.*

3. *If $d \equiv 2, 3 \bmod 4$ and $r_1 = 0, r_2 = 1$ and $|d| < \frac{\pi^2}{4}$, then $\mathrm{Cl}(K)$ is trivial.*

4. *If $d \equiv 1 \bmod 4$ and $r_1 = 0, r_2 = 1$ and $|d| < \pi^2$, then $\mathrm{Cl}(K)$ is trivial.*

Note that $\pi^2 \approx 9.8$ and $\frac{\pi^2}{4} \approx 2.4$. Concrete examples include the following.

1. $d = -1, K = \mathbb{Q}(i), d \equiv 3 \bmod 4, r_1 = 0, r_2 = 1, \Delta_K = -4$. Since $|d| < \pi^2$, the class group is trivial.

2. $d = 3, K = \mathbb{Q}(\sqrt{3}), d \equiv 3 \bmod 4, r_1 = 2, r_2 = 0, \Delta_K = 12$. Since $|3 * 4| < 16$, the class group is trivial.

Example 3.10.5. In the case $d = -5, K = \mathbb{Q}(\sqrt{-5}), \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}], \Delta_K = -20$, the Minkowski bound is not sufficient to conclude using the methods above that the class group is trivial. In fact, we can exhibit by example that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, and we know that $\mathcal{O}_K$ is a UFD if and only if the class group is trivial, so $\mathrm{Cl}(K)$ must be nontrivial. However, the Minkowski bound is still useful for computing $\mathrm{Cl}(K)$, see the following proposition.

Proposition 3.10.6. *Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathrm{Cl}(K)$ is cyclic of order 2, generated by the class of the ideal $(2, \sqrt{-5} + 1)$.*

Proof. The Minkowski bound is

$$N(\mathfrak{a}) \leq \frac{2}{\pi}\sqrt{20} \approx 2.847 < 3$$

Thus $\mathrm{Cl}(K)$ is generated by prime ideals of $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ of norm at most 2. The only prime of norm 1 the the whole ring, so $\mathrm{Cl}(K)$ is generated by prime ideals of norm 2. Let $\mathfrak{p} \subset \mathbb{Z}[\sqrt{-5}]$ be a prime ideal of norm 2. Then $\mathfrak{p}|2\mathcal{O}_K$, so we want to factor $2\mathcal{O}_K$. By Kummer's theorem, this is controlled by the factorization of the minimal polynomial of $\sqrt{-5}$ (x^2+5) reduced modulo 2.

$$x^2 + 5 \equiv (x+1)^2 \bmod 2 \implies 2\mathcal{O}_K = (2, \sqrt{-5}+1)^2$$

Let $\mathfrak{p}_2 = (2, \sqrt{-5}+1)^2$. The fundamental relation gives $2 = ef$. By the above factorization, $e = 2$, so $f = 1$, that is,

$$\dim_{\mathbb{F}_2} \mathcal{O}_K/\mathfrak{p}_2 = 1 \implies N(\mathfrak{p}_2) = |\mathcal{O}_K/\mathfrak{p}_2| = 2$$

Recall that $\mathrm{Cl}(K)$ is generated by primes of norm 2, and we just showed that a prime of norm 2 divides $2\mathcal{O}_K$, and by unique factorization it must be $\mathfrak{p}_2$. Thus $\mathrm{Cl}(K)$ is generated by $\mathfrak{p}_2$. The relation $\mathfrak{p}_2^2 = 2\mathcal{O}_K$ implies that $\mathfrak{p}_2$ has order dividing 2, since principal ideals are trivial in $\mathrm{Cl}(K)$. Since we know that $\mathrm{Cl}(K)$ is a nontrivial group, the generator can't be trivial, so $\mathfrak{p}_2$ is nontrivial, and hence has order exactly 2. Thus $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}\langle\mathfrak{p}_2\rangle$.

Alternatively, one can argue directly that $\mathfrak{p}_2$ is nontrivial in $\mathrm{Cl}(K)$ by showing that it is not a principal ideal. Suppose $\mathfrak{p}_2 = (\alpha)$, with $\alpha = m + n\sqrt{-5}$. Then

$$N(\mathfrak{p}_2) = 2 = N(\alpha) = m^2 + 5n^2$$

but this clearly has no solutions for $m, n \in \mathbb{Z}$, so we conclude that $\mathfrak{p}_2$ is not principal. □

Proposition 3.10.7. *Let $K = \mathbb{Q}(\sqrt{82})$. Then $\mathrm{Cl}(K)$ is cyclic of order 4.*

Proof. Similar to previous computation of the class group for $\mathbb{Q}(\sqrt{-5})$, but more complicated. We know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{82}]$ and $\Delta_K = 2^3 \cdot 41$, so the Minkowski bound gives $N(\mathfrak{a}) \leq 9$, so $\mathrm{Cl}(K)$ is generated by primes of norm ≤ 9. Consider the factorizations of $x^2 + 82$ modulo the primes $2, 3, 5, 7$.

The primes $5, 7$ are inert (they remain prime in $\mathcal{O}_K$), but $2\mathcal{O}_K$ is a square and $3\mathcal{O}_K$ splits as a product of two distinct primes. Thus $\mathrm{Cl}(K)$ is generated by the three primes dividing $2\mathcal{O}_k, 3\mathcal{O}_K$. By working with these even further one can conclude that $\mathrm{Cl}(K)$ is generated by an element of order dividing 4. Then using the Dirichlet Unit Theorem (a later result), one can show that the element has order 4. □

3.11 A cubic extension with trivial class group

Proposition 3.11.1. *Let $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$, and let α be a root of f, and let $K = \mathbb{Q}(\alpha)$. Then*

1. *The discriminant of f is 49.*

2. *All three roots of f (in $\mathbb{C}$) are real, that is, $r_1 = 3, r_2 = 0$ for $K = \mathbb{Q}(\alpha)$.*

3. $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

4. $\mathrm{Cl}(K)$ *is trivial.*

Proof. (1) Recall that a $\mathbb{Q}$-linear change of variables does not affect the discriminant, and make the substitution $y = x + \frac{1}{3}$. Then

$$f(x) = f\left(y - \frac{1}{3}\right) = y^3 - \frac{7}{3}y - \frac{7}{27}$$

Using the formula from 4.1.2, the discriminant of this polynomial in y is 49.

(2) Just graph the function. Alternately, note that

$$f(-3) < 0 \qquad f(-1) > 0 \qquad f(0) = -1 < 0 \qquad f(2) > 0$$

so there are three sign changes.

(3) Let $A = \mathbb{Z}[\alpha]$. It is clear that $A \subset \mathcal{O}_K$. A has the $\mathbb{Z}$-basis $1, \alpha, \alpha^2$, with discriminant

$$\mathrm{disc}(A/\mathbb{Z}) = \mathrm{disc}(f) = 49$$

We know that

$$49 = \mathrm{disc}(A/\mathbb{Z}) = \mathrm{disc}(\mathcal{O}_K/\mathbb{Z})[\mathcal{O}_K : A]^2$$

If $A \neq \mathcal{O}_K$, then $[\mathcal{O}_K : A] = 7$ by the above relation, so $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = 1$. Then by the Hermite-Minkowski inequality unless $K = \mathbb{Q}$, which we know is false, so $A = \mathcal{O}_K$.

(4) By the Minkowski bound,

$$\left(\frac{4}{\pi}\right)^{r_2} \left(\frac{n!}{n^n}\right) \sqrt{|\Delta_K|} = \frac{3!}{3^3}(7) = \frac{42}{27} < 2$$

since $r_2 = 0$. Since the Hermite-Minkowski bound is less than 2, all elements of $\mathrm{Cl}(K)$ are trivial. □

3.12 Dirichlet unit theorem

Theorem 3.12.1 (Dirichlet unit theorem)**.** *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $U_K = \mathcal{O}_K^\times$. Let r_1 be the number of real embeddings of K, and r_2 be the number of complex embeddings of K. Let $\mu(K)$ be the group of roots of unity in K. Then*

$$U_K \cong \mu(K) \times \mathbb{Z}^{r_1 + r_2 - 1}$$

In particular, U_K is a finitely generated abelian group.

The results that follow are used to build up the proof of the preceding theorem.

Proposition 3.12.2. *Let $x \in \mathcal{O}_K$. Then x is a unit if and only if $N_{\mathbb{Q}}^K(x) = \pm 1$.*

Proposition 3.12.3. *Let K be a number field, with associated r_1, r_2. Let $\sigma_1, \ldots, \sigma_{r_1+r_2}$ be the emeddings of K into $\mathbb{C}$. Let*

$$L : K^\times \to \mathbb{R}^{r_1+r_2} \qquad x \mapsto \Big(\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)| \Big)$$

be the logarithmic canonical "embedding" (not actually injective, but traditionally called an embedding nonetheless). (Note that $L(xy) = L(x) + L(y)$.) Let $C \subset \mathbb{R}^{r_1+r_2}$ be a bounded set. Then

$$L^{-1}(C) \cap U_K$$

is finite. Consequently, $L(U_K)$ is a discrete subgroup (lattice) in $\mathbb{R}^{r_1+r_2}$, that is, $L(U_K) \cong \mathbb{Z}^r$ for some $r \leq r_1 + r_2$.

Remark 3.12.4. In the language of the previous proposition, it is not hard to obtain the refined estimate $r_1 + r_2 - 1$ for the rank of $L(U_K)$, since the image of L lies in the hyperplane $W \subset \mathbb{R}^{r_1+r_2}$ defined by

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_2} y_j = 0$$

Since W is defined by one equation,

$$\dim_{\mathbb{R}} W = r_1 + r_2 - 1$$

and as previously noted, $L(U_K) \subset W$, so the rank of $L(U_K)$ is bounded above by $r_1 + r_2 - 1$. This is the value we want for Dirichlet's unit theorem, so we just need to verify that this bound is attained, which is to say, we want $L(U_K)$ to be a full lattice in W.

Proposition 3.12.5. *Let K be a number field, and let L be the log canonical embedding. Then*

$$\ker L|_{U_K} = \mu(K)$$

Proof. Let $\sigma_1, \ldots, \sigma_{r_1+r_2}$ be the distinct embeddings of K into $\mathbb{C}$. Let $x \in \mu(K)$, with $x^n = 1$. Then $|\sigma_i(x)|^n = 1$, so $|\sigma_i(x)| = 1$, so $L(x) = (0, \ldots, 0)$, hence $x \in \ker L$.

Conversely, we apply Proposition 3.12.3 to $C = \{0\}$, we get that $\ker L|_{U_K}$ is finite, which is to say, it is a finite subgroup of $K^\times$, which is to say it is a subset of $\mu(K)$. □

Remark 3.12.6. Using the previous result, we have an exact sequence of abelian groups

$$1 \to \mu(K) \to U_K \to L(U_K) \to 1$$

Since $L(U_K)$ is free abelian, it is projective, so this sequence splits. Hence

$$U_K \cong \mu(K) \times L(U_K) \cong \mu(K) \cong \mathbb{Z}^r$$

for some r satisfying $r \leq r_1 + r_2 - 1$. Now we really just need to show that $L(U_K)$ has the maximum possible rank, and the unit theorem is proved.

Proposition 3.12.7. *Let V be a finite dimensional real vector space. A discrete subgroup $\Lambda \subset V$ is a full lattice if and only if there exists a bounded subset $M \subset V$ such that translations of Λ by M cover V.*

Proposition 3.12.8. *Let K be a number field. For each $n \in \mathbb{Z}_{>0}$, only finitely many $a \in \mathcal{O}_K$ satisfy*

$$|N_{\mathbb{Q}}^K(a)| = n$$

up to multiplication by units. More precisely, there exist $a_1, \ldots, a_k$ with k depending on n, such that

$$|N_{\mathbb{Q}}^K(a_i)| = n$$

and any $a \in \mathcal{O}_K$ satisfying $|N(a)| = n$ differs from some a_i by a unit $u \in U_K$.

Proof. If $|N(a)| = n$, then

$$[\mathcal{O}_K : (a)] = N((a)) = |N(a)| = n$$

hence $(n) \subset (a) \subset \mathcal{O}_K$. By a standard correspondence, such ideals (a) correspond to ideals of the quotient ring $\mathcal{O}_K/(n)$. Since $\mathcal{O}_K/(n)$ is a finite ring, there are only finitely many such ideals. Hence there are only finitely many such a up to multiplication by units. □

Proposition 3.12.9. *Let K be a number field, with associated r_1, r_2, such that $r_1 + 2r_2 = [K : \mathbb{Q}]$. Set $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Let $\sigma : K \to V$ be the canonical embedding, and let*

$$N : V \to \mathbb{R} \qquad N(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) = y_1 \cdots y_r |z_1|^2 \cdots |z_{r_2}|^2$$

(Note that $N(\sigma x) = N_{\mathbb{Q}}^K(x)$.) Let $V^\times \subset V$ be the subset with nonzero entries in each component, viewed as a group with componentwise multiplication. Set

$$G = \left\{ v \in V^\times : |N(v)| = 1 \right\}$$

Then

1. *G is a closed subgroup of $V^\times$.*
2. *$\sigma(U_K)$ is a discrete subgroup of G (and since G is abelian, it is normal).*
3. *The quotient group $G/\sigma(U_K)$ is compact in the quotient topology.*

Remark 3.12.10. With the previous proposition, we can finish the proof of the Dirichlet unit theorem by showing that $L(U_K)$ is a lattice of rank $r_1 + r_2 - 1$. Continuing the notation of Proposition 3.12.9, define

$$\widetilde{L} : V^\times \to \mathbb{R}^{r_1+r_2} \qquad (y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \mapsto \Big(\log|\sigma_1 y_1|, \ldots, \log|\sigma_{r_2} z_{r_2}| \Big)$$

and consider the composition

$$K^\times \xrightarrow{\ \sigma\ } V^\times \xrightarrow{\ \widetilde{L}\ } \mathbb{R}^{r_1+r_2}$$

Note that $\widetilde{L} \circ \sigma$ is the same as the map L from Proposition 3.12.3. As before, let $W \subset \mathbb{R}^{r_1+r_2}$ be the hyperplane defined by

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_2} y_j = 0$$

Now set $\Lambda = L(U_K) \subset W$. Note that $\widetilde{L}$ is continuous and surjective, and that $\widetilde{L}(G) = W$. Thus we obtain an induced map $\widetilde{L} : G \to W$, which induce a map on the quotients $G/\sigma(U_K) \to W/L(U_K) = W/\Lambda$. Since $\widetilde{L}$ is continuous and surjective, this induced map is also continuous and surjective.

Since G/U is compact by 3.12.9, so is W/Λ. Thus W/Λ is bounded, so Λ is a full lattice in W. Thus the rank of $\Lambda = L(U_K)$ is $r_1 + r_2 - 1$.

3.13 Applications of the Dirichlet unit theorem

3.13.1 Quadratic number fields

Proposition 3.13.1. *Let K be an imaginary quadratic number field. Then $U_k \cong \mu(K)$.*

Proof. We have $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ and square free. Thus $r_1 = 0, r_2 = 1$, so $r_1 + r_2 - 1 = 0$. Thus by the unit theorem, the free part of $\mu(K)$ has rank zero. The torsion part is $\mu(K)$. □

Proposition 3.13.2. *Let K be a real quadratic number field. Then*

$$U_K \cong \{\pm 1\} \times \mathbb{Z}$$

In particular, the positive units (> 0 after embedding $K \hookrightarrow \mathbb{R}$) form a subgroup of K isomorphic to $\mathbb{Z}$, so there is a generator ϵ which is unique if we require $\epsilon > 1$.

Proof. We have $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$ and square free. Thus $r_1 = 2, r_2 = 0$, so the free part of U_K has rank $2 + 0 - 1 = 1$. Since K has a real embedding, $\mu(K) \cong \{\pm 1\}$. □

Remark 3.13.3. Let K be a real quadratic number field. What can we say about the fundamental unit ϵ? Suppose $x = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$ is a unit in $\mathcal{O}_K$. Then $x, x^{-1}, -x, -x^{-1}$ are also units, and $N(x) = a^2 - b^2 d = \pm 1$. For $x \neq \pm 1$, only on of $\pm a \pm b\sqrt{d}$ is bigger than 1, so we can assume $a, b > 0$ in our search for ϵ. Past this point, we need to consider the cases $d \equiv 2, 3 \bmod 4$ and $d \equiv 1 \bmod 4$ separately, since $\mathcal{O}_K$ depends on these cases.

We start by considering $d \equiv 2, 3 \bmod 4$, in which case $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Hence a unit $x = a + b\sqrt{d}$ has $a, b \in \mathbb{Z}$ satisfying $a^2 - b^d d = \pm 1$. Suppose $\epsilon = a_1 + b_1\sqrt{d}$ is the fundamental unit, $\epsilon > 1$, so $a_1, b_1 > 0$. Define a_n, b_n by

$$a_n + b_n\sqrt{d} = \epsilon^n = (a_1 + b_1\sqrt{d})^n$$

A bit of algebraic manipulation shows $b_n = a_1 b_{n-1} + a_{n-1} b_1$, so $b_1, b_2, \ldots$ is a strictly increasing sequence. To calculate $a_1 + b_1\sqrt{d}$, just compute

$$d, 4d, 9d, 16d, \ldots$$

until one of these differs by a square from ± 1. When $b^2 d = a^2 \pm 1$, we set $\epsilon = a + b\sqrt{d}$, and we know that this is the fundamental unit.

Example 3.13.4. Let $K = \mathbb{Q}(\sqrt{7})$. This fits in the case $d \equiv 2, 3 \bmod 4$. The sequence $b^2 d$ is

$$7, 28, 63, \ldots$$

and $63 = 64 - 1$, so the fundamental unit is $b_1 = 3, a_1 = 8$.

$$\epsilon = 8 + 3\sqrt{7}$$

Example 3.13.5. Let $K = \mathbb{Q}(\sqrt{82})$. This fits in the case $d = \equiv 2, 3 \bmod 4$. The sequence $b^2 d$ starts with 82 which already differs from a square by ± 1, so the fundamental unit is

$$\epsilon = 9 + \sqrt{82}$$

Remark 3.13.6. Now we continue the general discussion of finding a fundamental unit for a real quadratic number field in the case where $d \equiv 1 \bmod 4$. In this case, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, so if $\frac{1}{2}\left(a + b\sqrt{d}\right)$ is a unit, then

$$a^2 - db^2 = \pm 4$$

If $\frac{1}{2}\left(a_1 + b_1\sqrt{d}\right)$ is a fundamental unit ($a_1, b_1 > 0$), then the solutions to the equation above are given by the sequence

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^2 2^{1-n}$$

Similar to the previous case, to find a_1, a_2, consider the sequence $d, 4d, 9d, \ldots$ and stop when $b^2 d$ differs from a square by ± 4. The first b when you stop is b_1, and a_1 is the square root of the square which $b^2 d$ is ± 4 away from.

Example 3.13.7. Let $K = \mathbb{Q}(\sqrt{5})$. The first term of the sequence $b^2 d$ is 5 which already differs from the sqaure 1 by 4, so $a_1 = b_1 = 1$ and the fundamental unit is

$$\frac{1}{2}\left(1 + \sqrt{5}\right)$$

3.13.2 A higher degree example

Example 3.13.8. Let $f(x) = x^3 + x^2 - 2x - 1$ and let α be a root of f. Let $K = \mathbb{Q}(\alpha)$. Earlier, we showed that f has three real roots, so there are three real embeddings, so $r_1 = 3, r_2 = 0$. Since K is totally real, $\mu(K) \cong \{\pm 1\}$. Thus

$$U_K \cong \{\pm 1\} \times \mathbb{Z}^2$$

3.14 Generalization of unit theorem for S-units

Remark 3.14.1. The following generalization of Dirichlet's unit theorem is not usually phrased in this way; it is usually phrased in the language of ideles, but we aren't covering that in this class.

Proposition 3.14.2. *Let K be a number field, and let $S \subset \operatorname{spec} \mathcal{O}_K$ be a finite set. Then*

$$U_K(S) \cong \mu(K) \times \mathbb{Z}^{r_1 + r_2 + |S| - 1}$$

Proof. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$, and consider

$$\phi : U_K(S) \to \mathbb{Z}^t \qquad u \mapsto \left(v_{\mathfrak{p}_1}(u), \ldots, v_{\mathfrak{p}_t}(u)\right)$$

Note that ϕ is a group homomorphism, and that $\ker \phi = U_K$. Let $h_K = |\operatorname{Cl}(K)|$. Then for any i, $\mathfrak{p}_i^{h_K}$ is a principal ideal, say generated by the element $\pi_i \in \mathcal{O}_K$.

$$\mathfrak{p}_i^{h_K} = (\pi_i)$$

By unique factorization of ideals,

$$\phi(\pi_i) = (0, \ldots, 0, h_K, 0, \ldots, 0)$$

with the h_K occuring the the ith index. Thus $\phi(\pi_1), \ldots, \phi(\pi_t)$ generate a subgroup of $\mathbb{Z}^t$ of rank t, and we have a short exact sequence

$$1 \longrightarrow U_K \hookrightarrow U_K(S) \xrightarrow{\phi} \mathbb{Z}^t \longrightarrow 1$$

Since $\mathbb{Z}^t$ is projective, this splits, so we obtain

$$U_K(S) \cong U_K \times \mathbb{Z}^t \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1} \times \mathbb{Z}^{|S|} \cong \mu(K) \times \mathbb{Z}^{r_1+r_2+|S|-1}$$

□

3.15 Cyclotomic fields

Proposition 3.15.1. *Let $n \in \mathbb{Z}_{\geq 1}$ and let ζ be a primitive nth root of unity. Let $K = \mathbb{Q}(\zeta)$. Then*

1. *The minimal polynomial of ζ is the nth cyclotomic polynomial*

$$\Phi_n(x) = \prod_{m \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (x - \zeta^m) \qquad \in \mathbb{Z}[x]$$

   and K is the splitting field of Φ_n.

2. *$[K : \mathbb{Q}] = \phi(n)$, where ϕ is the Euler totient function.*

3. *$K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proposition 3.15.2. *Let p be a prime and $r \in \mathbb{Z}_{\geq 1}$. Let ζ be a primitive p^rth root of unity, and let $K = \mathbb{Q}(\zeta)$. Then*

1. *If ζ' is another primitive p^rth root of unity, then $\frac{1-\zeta'}{1-\zeta}$ is a unit in $\mathbb{Z}[\zeta]$, hence also a unit in $\mathcal{O}_K$.*

2. *$\mathcal{O}_K = \mathbb{Z}[\zeta]$*

3. *The element $1 - \zeta$ generates a prime ideal of $\mathcal{O}_K$, and*

$$(p) = (1 - \zeta)^e$$

   where $e = [K : \mathbb{Q}] = \phi(p^r) = (p-1)p^{r-1}$. That is, p is totally ramified.

4. *The discriminant is $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \pm p^c$, where*

$$c = p^{r-1}(pr - r - 1)$$

   Hence p is the only prime that ramifies.

Proposition 3.15.3. *Let $n, m \in \mathbb{Z}_{\geq 1}$ and let ζ_n, ζ_m be primitive nth, mth roots of unity respectively. If $\gcd(n, m) = 1$, then ζ_{mn} is a primitive mnth root of unity, and consequently*

$$\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n, \zeta_m)$$

where the middle term is the compositum in $\mathbb{Q}^{\text{al}}$ (or $\mathbb{C}$, if you prefer), and

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$$

Proposition 3.15.4 (from Neukirch)**.** *Let $L/\mathbb{Q}, L'\mathbb{Q}$ be Galois of degrees n, n' respectively, such that $L \cap L' = \mathbb{Q}$. Suppose $w_1, \ldots, w_n$ and $w'_1, \ldots, w'_n$ are $\mathbb{Z}$-bases for $\mathcal{O}_L, \mathcal{O}_{L'}$ respectively. Suppose*

$$D = D(w_1, \ldots, w_n) \qquad D' = D(w'_1, \ldots, w'_n)$$

are relatively prime. Then $\left\{w_i w'_j : 1 \leq i \leq n, 1 \leq j \leq n'\right\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{LL'}$ with

$$D(w_i w'_j) = D^{n'}(D')^n$$

Proposition 3.15.5. *Let ζ be a primitive nth root of unity and let $K = \mathbb{Q}(\zeta)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta]$. In particular, $1, \zeta, \ldots, \zeta^{\phi(n)-1}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.*

Proof. Write n as a product of primes $n = p_1^{t_1} \ldots p_r^{t_r}$, and let $\zeta_i = \zeta^{n/\left(p_i^{t_i}\right)}$. Then

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1) \cdots \mathbb{Q}(\zeta_r)$$

with

$$\mathbb{Q}(\zeta_1) \cdots \mathbb{Q}(\zeta_{i-1}) \cap \mathbb{Q}(\zeta_i) = \mathbb{Q}$$

Since $1, \zeta_i, \ldots, \zeta_i^{\phi(p_i)}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{Q}(\zeta_i)}$ by previous work, and the discriminant for $\mathbb{Q}(\zeta_i)$ is a power of p_i, by the Neukirch result, we can induct and conclude that the products of various powers of ζ_i give a $\mathbb{Z}$-basis for $\mathcal{O}_K$. □

Proposition 3.15.6. *Let $n \in \mathbb{Z}_{\geq 1}$ and let ζ be a primitive nth root of unity and let $K = \mathbb{Q}(\zeta)$. Let $n \in \mathbb{Z}$, written as a product of primes $n = \prod_p p^{t_p}$. For a prime p, let f_p be the smallest positive integer such that*

$$p^{f_p} \equiv 1 \bmod \left(\frac{n}{p^{t_p}}\right)$$

Then (p) factors in $\mathcal{O}_K$ as

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\phi(p)^{t_p}}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct primes of $\mathcal{O}_K$, all of residual degree f_p.

3.16 Special case of Fermat's last theorem

Definition 3.16.1. Let p be an odd prime, and let ζ be a primitive pth root of unity, and let $K = \mathbb{Q}(\zeta)$. The prime p is **regular** if p does not divide $h_K = |\operatorname{Cl}(K)|$.

Definition 3.16.2. Then nth **Bernoulli number** B_n is defined by the equation

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

Note that $B_n \in \mathbb{Q}$.

Proposition 3.16.3 (Kummer's criterion)**.** *An odd prime p is not regular if and only if p divides the numerator of some Bernoulli number B_k for $k = 2, 4, \ldots, p-3$.*

Proposition 3.16.4 (Fermat's last theorem for regular primes, due to Kummer)**.** *Let p be a regular prime. Then*

$$x^p + y^p = z^p$$

has no nontrivial solutions for $x, y, z \in \mathbb{Z}$ with $p|xyz$.

3.17 Local fields

Proposition 3.17.1. *An absolute value is nonarchimedean if and only if the values $|n1|$ are bounded for all $n \in \mathbb{Z}$. (In particular, if a field has positive characteristic, this is a finite set so there are only nonarchimedean absolute values.)*

Theorem 3.17.2 (Ostrowski)**.** *Any nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ or to $|\cdot|_p$ for some prime p. (This has a nice generalization to number fields as well.)*

Proposition 3.17.3 (Product formula)**.** *Let $x \in \mathbb{Q}^\times$. Then*

$$\prod_{\alpha} |x|_\alpha = 1$$

where α ranges over $\{\infty, 2, 3, 5, \ldots\}$. Another way to write this is

$$\prod_{p \text{ prime}} |x|_p = \frac{1}{|x|_\infty}$$

Proposition 3.17.4 (Some properties of nonarchimedean analysis)**.** *Let K be a field with nonarchimedean absolute value and associated metric topology.*

1. *If a sequence (x_n) converges to $x \in K$, then $|x_n| = |x|$ for $n \gg 0$. (This does NOT say that the sequence eventually stabilizes, but the sequence of absolute values does eventually stabilize.)*
2. *A sequence (x_n) is Cauchy if and only if $|x_{n+1} - x_n| \to 0$ as $n \to \infty$.*
3. *If a sequence (x_n) is Cauchy and not limiting to zero, then $|x_n| = |x_m|$ for $n, m \gg 0$.*

4. *Suppose K is complete. A series converges if and only if the nth term tends to zero.*

Proposition 3.17.5. *Let K be a field with nonarchimedean absolute value and associated metric topology. Let*

$$B(a,r) = \{x \in K : |x-a| < r\}$$
$$\overline{B}(a,r) = \{x \in K : |x-a| \leq r\}$$

(Don't be tricked by the notation: $\overline{B}(a,r)$ is not necessarily the closure of $B(a,r)$. Or maybe it is and this is obvious, I'm not sure. Just don't assume it without thinking it through, just a warning.)

1. *If $b \in B(a,r)$, then $B(a,r) = B(b,r)$. That is, every point inside an open ball is a center for that ball.*
2. *If $b \in \overline{B}(a,r)$, then $\overline{B}(a,r) = \overline{B}(b,r)$.*
3. *$B(a,r)$ is both open and closed.*
4. *Two balls in K have non-empty intersection if and only if one contains the other. More precisely, if $a, b \in K$ and $r, s \in \mathbb{R}_{>0}$, then*

$$B(a,r) \cap B(r,s) = \emptyset$$

   if and only if one ball contains the other.

5. *The topology on K is totally disconnected.*

Proposition 3.17.6. *$\mathbb{Q}$ is not complete with respect to any p-adict absolute value.*

Proposition 3.17.7 (Completions)**.** *Let K be a field with absolute value. There exists a field $\widehat{K}$ with an absolute value such that $K \hookrightarrow \widehat{K}$, and the absolute value extends, and $\widehat{K}$ is complete. Furthermore, the image of K is dense in $\widehat{K}$.*

Also, $\widehat{K}$ has the following universal property. Any isometry $K \to E$ of metric fields extends uniquely to $\widehat{K}$, making the following diagram commute. Consequently, $\widehat{K}$ is unique up to isometry.

$$\begin{array}{ccc} \widehat{K} & \xrightarrow{\widehat{\phi}} & \widehat{E} \\ \uparrow & & \uparrow \\ K & \xrightarrow{\phi} & E \end{array}$$

Example 3.17.8. $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$. $\mathbb{Q}_p$ is (by definition) the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. By Ostrowski's theorem, there are no other complete fields containing $\mathbb{Q}$.

Proposition 3.17.9. *For each nonzero $x \in \mathbb{Q}_p$, there exists $n \in \mathbb{Z}$ such that $|x|_p = p^{-n}$. As a consequence, the normalized discrete valuation $v_p : \mathbb{Q} \to \mathbb{Z}$ extends to $\mathbb{Q}_p$.*

Proposition 3.17.10. *The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ has dense image. More precisely, if $x \in \mathbb{Z}_p$ and $n \geq 1$, there exists a unique $\alpha \in \mathbb{Z}$ with $0 \leq \alpha \leq p^n - 1$ such that $|x - \alpha|_p \leq p^{-n}$.*

Consequently, for $x \in \mathbb{Z}_p$, there exists a unique Cauchy sequence (α_n) with $\alpha_n \to x$, with $\alpha_n \in \mathbb{Z}, 0 \leq \alpha_n \leq p^n - 1$ and $\alpha_n \equiv \alpha_{n-1} \bmod p^{n-1}$.

As a further consequence, for any $n \geq 1$, we have an exact sequence

$$0 \to \mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

which implies

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

Proposition 3.17.11. *Every $x \in \mathbb{Q}_p$ can be written as a "Taylor series in p with integer coefficients". More precisely, x can be written as*

$$x = b_{-m}p^{-m} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots$$

If we reduce each b_i modulo p, so that $0 \leq b_i \leq p - 1$, then this expansion is unique. Note that the first nonzero coefficient gives the valuation of x, that is,

$$v_p(x) = -m$$

Consequently $x \in \mathbb{Q}_p$ is in $\mathbb{Z}_p$ if and only if the series corresponding to x starts with $i \geq 0$.

Example 3.17.12. Let p be any prime and $x = -1$. In $\mathbb{Q}_p$, we have

$$-1 = \sum_{i=0}^{\infty}(p-1)p^i = (p-1) + (p-1)p + (p-1)p^2 + \cdot$$

Example 3.17.13. Let $p = 3$ and $x = \frac{1}{2}$. In $\mathbb{Q}_3$, we have

$$-\frac{1}{2} = \frac{1}{1-3} = 1 + 3 + 3^2 + 3^3 + \cdots$$

so

$$\frac{1}{2} = 1 - \frac{1}{2} = 2 + 3 + 3^2 + \cdots$$

Proposition 3.17.14. *Let (X, d) be a metric space. Then X is compact if and only if X is complete and totally bounded.*

Proposition 3.17.15. *$\mathbb{Z}_p$ is compact, and hence $\mathbb{Q}_p$ is locally compact.*

Proposition 3.17.16. *A topological group of profinite if and only if it is compact, Hausdorff, and totally disconnected.*

Proposition 3.17.17. *Let K be a field with nontrivial absolute value. The following are equivalent.*

1. *K is a local field.*
2. *There exists at least one compact closed ball in K.*

3. *Every closed ball in K is compact. That is, every set of the form*

$$\overline{B}(a,r) = \{x \in K : |x-a| \leq r\}$$

for $a \in K, r \in \mathbb{R}_{\geq 0}$ is compact.

Proof. (3) $\implies$ (1) $\implies$ (2) is obvious, so we just need to show (2) $\implies$ (3). By (2), we can choose a, r so that $\overline{B}(a,r)$ is compact. Note that the translation $x \mapsto x+a$ is a homeomorphism $K \to K$, so $\overline{B}(0,r)$ is compact.

Since the absolute value is nontrivial, there exists $a \in K$ with $|a| > 1$. The map $x \mapsto ax$ is a homeomorphism $K \to K$ which takes $\overline{B}(0,\delta)$ to $\overline{B}(0,\delta|a|)$, so

$$\overline{B}(0,\delta r|a|), \overline{B}(0,\delta r|a|^2), \ldots, \overline{B}(0,r|a|^n), \ldots$$

are compact for all n. Thus, closed balls of arbitrarily large radius centered at zero are compact. Any closed ball centered at zero is contained in one of these, so it is also compact. Thus all closed balls centered at zero (or any radius) are compact. By translation again, all balls are compact. □

Proposition 3.17.18. *A local field is complete.*

Proof. We prove the contrapositive (not complete $\implies$ not local). Let K be a field with nontrivial absolute value which is not complete. Let $\widehat{K}$ be the completion of K, and choose $x \in \widehat{K} \setminus K$, and a Cauchy sequence x_n in K converging to x. Since the sequence is Cauchy, we can choose a closed ball $B \subset K$ containing all x_n for $n \gg 0$. Set

$$U_n = \left\{ y \in K : |y-x| > \frac{1}{n} \right\} = K \setminus B\left(x, \frac{1}{n}\right)$$

Note that the sets U_n cover K; in particular, they are an open cover of B. However, there is no finite subcover, since the sequence x_n eventually escapes U_n and B contains the sequence x_n. Thus K is not local. □

Proposition 3.17.19. *Let K be a nonarchimedean valued field with associated valuation v. The following are equivalent.*

1. *K is local.*
2. *The valuation ring $\mathcal{O}_v$ is compact.*
3. *K is complete, v is discrete, and the residue field $\mathcal{O}_v/\mathfrak{m}_v$ is finite.*

Remark 3.17.20. For an arbitrary nonarchimedean field K with valuation ring $\mathcal{O}_v$, we can write down power series expressions for elements of $\mathcal{O}_v$ and Laurent series expressions for elements of K.

Proposition 3.17.21. *Let p, q be primes. Then $\mathbb{Q}_p \cong \mathbb{Q}_q$ as abstract fields if and only if $p = q$.*

Remark 3.17.22. The reverse direction is obvious. The forward direction is obvious IF we require the isomorphism to preserve the absolute value, since in that case the isomorphism of valued fields would induce an isomorphism of residue fields $\mathbb{F}_p \cong \mathbb{F}_q$, which is only possible if $p = q$. However, we want to see that even if they are just isomorphic as fields, then $p = q$.

Proposition 3.17.23. *Let p be a prime. Then*

1. *$\sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$ is a unit if and only if a_0 is a unit, if and only if $a_0 \neq 0$ (since $a_0 \in \mathbb{Z}/p\mathbb{Z}$.*
2. *For $p \neq 2$, the units of $\mathbb{Z}_p$ are*
$$\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times$$
(isomorphism of groups).
3. *For $p = 2$,*
$$\mathbb{Z}_2^\times \cong \mathbb{Z}_2 \times \{\pm 1\}$$
(isomorphism of groups).
4. *For any prime p,*
$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$$
Since $\mathbb{Z}, \mathbb{Z}_p$ are torsion free, the only roots of unit of $\mathbb{Q}_p$ are ± 1 and $(p-1)$st roots of unity if $p \geq 3$, and ± 1 if $p = 2$.

Remark 3.17.24. As a consequence of the above discussion of roots of unity in $\mathbb{Q}_p$, we can say that $\mathbb{Q}_p$ for $p \geq 3$ is not isomorphic to $\mathbb{R}$ as abstract fields, since $\mathbb{R}$ only contains ± 1 as roots of unity. Obviously, $\mathbb{Q}_p$ is not isomorphic to $\mathbb{C}$ as a field, by similar reasoning, as $\mathbb{C}$ contains all roots of unity.

Proposition 3.17.25. *If p is an odd prime and $n \geq 1$, then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.*

Proposition 3.17.26. *Let*
$$f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$$
Define
$$r_f = \frac{1}{\limsup |a_n|_p^{1/n}}$$
Then $f(x)$ converges for x such that $|x|_p < r_f$ and diverges if $|x|_p > r_f$. (If $|x|_p = r_f$, it may or may not converge.)

Proposition 3.17.27. *The domain of convergence of a power series $f \in \mathbb{Q}_p[[x]]$ is either a point, a ball, or all of $\mathbb{Q}_p$, and convergence on that domain is uniform.*

Proposition 3.17.28. *For a prime $p \geq 3$,*
$$\exp : p\mathbb{Z}_p \to (1 + p\mathbb{Z}_p) \cong \mathbb{Z}_p$$
with inverse given by the p-adic logarithm. If $p = 2$, the same maps give an isomorphism (of topological gropus)
$$2\mathbb{Z}_2 \to 1 + 4\mathbb{Z}_2$$

3.17.1 Hensel's Lemma

Proposition 3.17.29 (Hensel's lemma, version 1)**.** *Let K be a complete nonarchimedean discretely valued field, and let*

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\}$$

be the associated local ring with maximal ideal

$$\mathfrak{m} = \{x \in K : |x| < 1\}$$

Let $f(t) \in \mathcal{O}_K[t]$ be monic, and suppose $x_1 \in \mathcal{O}_K$ such that $|f'(x_1)| = 1$ and $f'(x_1) \not\equiv 0 \bmod \mathfrak{m}$. Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $|x - x_1| < |f(x_1)|$.

Proposition 3.17.30 (Hensel's lemma, version 2)**.** *Let K be a complete nonarchimedean discretely valued field, with associated local ring $(\mathcal{O}_K, \mathfrak{m})$. Let $f(x) \in \mathcal{O}_K[x]$ be monic. Suppose $x_1 \in \mathcal{O}_K$ such that*

$$f'(x_1) \neq 0 \qquad |f(x_1)| < |f'(x_1)|^2$$

Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and

$$|x - x_1| \leq \left| \frac{f(x_1)}{f'(x_1)} \right|$$

Proposition 3.17.31 (Hensel's lemma, version 3)**.** *Let K be a complete nonarchimedean discretely valued field, with associated local ring $(\mathcal{O}_K, \mathfrak{m})$, and residue field $k = \mathcal{O}_K/\mathfrak{m}$. Let $f \in \mathcal{O}_K[x]$, and suppose there exist $g_1, h_1 \in \mathcal{O}_K[x]$ with g_1 monic and $\gcd(g_1, h_1) = 1$ such that*

$$\overline{f} = \overline{g_1 h_1} \in k[x] \qquad (\text{equivalently } f \equiv g_1 h_1 \bmod \mathfrak{m})$$

Then there exist $g, h \in \mathcal{O}_K[x]$ such that g is monic, $\overline{g} = \overline{g}_1, \overline{h} = \overline{h}_1$, and $f = gh$. That is, factorizations of polynomials over k lift to factorizations over $\mathcal{O}_K$, provided there are no common factors and one is monic.

3.17.2 Applications of Hensel's lemma

Proposition 3.17.32. *Let p be an odd prime. Then $u \in \mathbb{Z}_p^\times$ is a square if and only if $u \bmod p$ is a square in $\mathbb{F}_p^\times$.*

Proof. Clearly if $u = a^2$ is a square in $\mathbb{Z}_p$, then $u = a^2 \bmod p$ so $u \bmod p$ is a square in $\mathbb{F}_p^\times$. For the converse, we apply Hensel's lemma, version 3 in the case $K = \mathbb{Q}_p, \mathcal{O}_K = \mathbb{Z}_p, \mathfrak{m} = p\mathbb{Z}_p, k = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ to the polynomial $f(x) = x^2 - u \in \mathbb{Z}_p[x]$. Suppose $u \bmod p$ is a square in $\mathbb{F}_p$,

$$u \equiv a^2 \pmod{p}$$

for some $a \in \mathbb{Z}_p^\times$. Then f splits as

$$f(x) \equiv x^2 - u \equiv x^2 - a^2 \equiv (x - a)(x + a) \pmod{p}$$

Since $p \neq 2$, $a \neq -a$ so $\gcd(x+a, x-a) = 1$. Then by Hensel's lemma, there exist $g, h \in \mathbb{Z}_p[x]$ such that

$$\begin{aligned} g &\equiv x + a \pmod{p} \\ h &\equiv x - a \pmod{p} \\ f &= gh \in \mathbb{Z}_p[x] \end{aligned}$$

That is, there are $b, c \in \mathbb{Z}_p$ such that

$$g(x) = x + b \qquad h(x) = x - c \qquad b \equiv c \equiv a \pmod{p}$$

Then

$$f(x) = x^2 - u = g(x)h(x) = (x + b)(x - c) = x^2 + (b - c)x - bc$$

which implies $b = c$, and then $b^2 = u$. □

Remark 3.17.33. Let $p = 2$. The analogous version of the previous proposition says that $u \in \mathbb{Z}_2^\times$ is a square if and only if $u \equiv 1 \bmod 8$. As above, one direction is immediate. The converse requires version 2 of Hensel's lemma, applied to the same polynomial $x^2 - u$.

Lemma 3.17.34. *Let $x \in \mathbb{Q}_p^\times$. The following are equivalent.*

1. *$x \in \mathbb{Z}_p^\times$.*
2. *x^{p-1} has nth roots for infinitely many $n \in \mathbb{Z}_{\geq 1}$.*

Proposition 3.17.35. *The only field automorphism of $\mathbb{Q}_p$ is the identity.*

Proof. Let $\phi : \mathbb{Q}_p \to \mathbb{Q}_p$ be a field automorphism. Then $\phi|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$, and by the previous lemma, if $u \in \mathbb{Z}_p^\times$ then $\phi(u) \in \mathbb{Z}_p^\times$, since having nth roots is preserved by a field automorphism. Since $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$, we can write any $x \in \mathbb{Q}_p^\times$ as

$$x = p^n u \qquad u \in \mathbb{Z}_p^\times$$

Then

$$\phi(x) = \phi(p^n u) = p^n \phi(u)$$

with $\phi(u) \in \mathbb{Z}_p^\times$ as noted previously, hence

$$v_p(\phi(x)) = n = v_p(x)$$

that is, ϕ preserves the p-adic valuation. Equivalently, ϕ preserves the p-adic absolute value, which implies that ϕ is continuous. Since $\mathbb{Q} \subset \mathbb{Q}_p$ is dense, ϕ is determined by its values on $\mathbb{Q}$, hence $\phi = \mathrm{Id}_{\mathbb{Q}_p}$. □

Proposition 3.17.36. *Let K be a complete local field.*

1. *If K is archimedean, then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.*
2. *If K is nonarchimedean and $\operatorname{char} K = p$, then $K \cong \mathbb{F}_q((t))$ for some $q = p^n$, and the residue field is $k_K \cong \mathbb{F}_q$. (This case is called "equal characteristic".)*
3. *If K is nonarchimedean and $\operatorname{char} K = 0$, then K is a finite extension of $\mathbb{Q}_p$ for some p, and the residue field is $k_K \cong \mathbb{F}_p$. (This case is called "mixed characteristic.")*

3.17.3 Extending absolute values

Lemma 3.17.37. *Let K be a complete nonarchimedean discretely valued field. Let $f \in K[t]$ be monic irreducible with $f(0) \in \mathcal{O}_K$. Then $f \in \mathcal{O}_K[t]$.*

Proposition 3.17.38. *Let K be a complete nonarchimedean discretely valued field, and let L/K be a finite extension, with $n = [L : K]$. Then there is a unique absolute value on L extending the absolute value on K, such that L is complete with respect to the absolue value. Explicitly,*

$$|x|_L = \left|N_K^L(x)\right|_K^{1/n}$$

Furthermore, the valuation ring $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Remark 3.17.39. By the above, if L/K is Galois and $\alpha, \alpha' \in L$ are Galois conjugates, then $|\alpha|_L = |\alpha'|_L$, since α, α' have the same norm.

Remark 3.17.40. Let K be a complete valued field as in the previous theorem. Since the algebraic closure of K is the union over all finite extensions of K, using the previous theorem, we can extend the absolute value on K uniquely to the algebraic closure. (This can also be done for the separable closure if that is desirable.) However, this does not tell us that the algebraic closure is complete with respect to the extended value, and usually it is not. We now have processes

$$K \rightsquigarrow \widehat{K} \qquad K \rightsquigarrow K^{\text{alg}}$$

both with unique extensions of the absolute value. So we can do things like

$$K \rightsquigarrow \widehat{K} \rightsquigarrow \widehat{K}^{\text{alg}} \rightsquigarrow \widehat{\widehat{K}^{\text{alg}}} \rightsquigarrow \widehat{\widehat{K}^{\text{alg}}}^{\text{alg}} \rightsquigarrow \cdots$$

which in principle may never terminate, since after taking the completion, we may not have an algebraically closed field, and after taking the algebraic closure, we may not have a complete field.

For example, the algebraic closure of $\mathbb{Q}_p$ is not complete with respect to to the extended absolute value (assertion without proof here, not obvious). It is a theorem (beyond this class) that if you form the completion of $\mathbb{Q}_p^{\text{alg}}$ with respect to its absolute value that the resulting field is algebraically closed in addition to being complete. That is, starting with $\mathbb{Q}$ with p-adic absolute value, the above process terminates after

$$\mathbb{Q} \rightsquigarrow \mathbb{Q}_p \rightsquigarrow \mathbb{Q}_p^{\text{alg}} \rightsquigarrow \widehat{\mathbb{Q}_p^{\text{alg}}}$$

since this completion is algebraically closed, taking the algebraic closure does nothing.

Proposition 3.17.41. *Let K be a complete nonarchimedean discretely valued field, and let L/K be a finite separable extension, with extended absolute value, such that the valuation on L is also discrete. Then $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $[L : K]$.*

Proposition 3.17.42. *Let K be a comlpete nonarchimedean discretely valued field, and L/K a finite extension, with extended absolute value. Assume that the residue fields k_K, k_L are perfect. Then*

$$[L : K] = e_{L/K} f_{L/K}$$

Proof. Let $d = [L : K]$. By the previous result, $\mathcal{O}_L \cong \mathcal{O}_K^d$ as an $\mathcal{O}_K$-module. Let π_K, π_L be uniformizers, that is,

$$(\pi_K) = \pi_K \mathcal{O}_K = \mathfrak{m}_K \qquad (\pi_L) = \pi_L \mathcal{O}_L = \mathfrak{m}_L$$

Then

$$\mathcal{O}_L/\pi_K\mathcal{O}_L \cong \mathcal{O}_K^d/\pi_k\mathcal{O}_K^d \cong (\mathcal{O}_K/\pi_K\mathcal{O}_K)^d \cong (k_K)^d$$

Recall that by definition of $e = e_{L/K}$, $(\pi_K) = (\pi_L^e)$. Consider the filtration

$$\begin{array}{ccccccccc} \mathcal{O}_L & \supset & \pi_L\mathcal{O}_L & \supset & \pi_L^2\mathcal{O}_L & \supset & \cdots & \supset & \pi_L^e\mathcal{O}_L = \pi_k\mathcal{O}_L \\ & & (\pi_L) & & (\pi_L^2) & & & & (\pi_L^e) = (\pi_k) \end{array}$$

Recall that by definition of $f = f_{L/K}$, we have $k_L \cong k_K^f$. At each step of the filtration, we have

$$\pi_L^i\mathcal{O}_K/\pi_L^{i+1}\mathcal{O}_L \cong \mathcal{O}_L/\pi_L\mathcal{O}_L \cong k_L \cong k_K^f$$

Since there are e steps in the filtration, and each step has successive quotient k_k^f, in total we have

$$\mathcal{O}_L/\pi_K\mathcal{O}_L \cong \left(k_K^f\right)^e = k_K^{ef}$$

Since this quotient is also k_K^d, we get $d = ef$ as desired. □

Proposition 3.17.43. *The indices e, f are "multiplicative in towers." More precisely, let K be a complete nonarchimedean discretely valued field, and let $K \subset L \subset M$ be a tower of finite extensions. Then*

$$e_K^M = e_L^M e_K^L \qquad f_K^M = f_L^M f_K^L$$

Proof. For f, this just follows from the tower law for field extensions.

$$f_K^M = [k_M : k_K] = [k_M : k_L][k_L : k_K] = f_L^M f_M^L$$

The result for e could probably be proved directly, but it also follows using the tower law for f, the tower law for $K \subset L \subset M$, and the previous result $[L : K] = e_K^L f_K^L$.

$$e_K^M = \frac{[M : K]}{f_K^M} = \frac{[M : L][L : K]}{f_L^M f_K^L} = \left(\frac{[M : L]}{f_L^M}\right)\left(\frac{[L : K]}{f_K^L}\right) = e_L^M e_K^L$$

□

Example 3.17.44. Let $K = \mathbb{Q}_5$ and $L = \mathbb{Q}_5(\sqrt{2})$, so $[L : K] = 2$. Normalize the discrete valuation on K so that $v_K(K^\times) = \mathbb{Z}$ and $v_L(L^\times) = \frac{1}{e}\mathbb{Z}$. Note that

$$N_K^L(\sqrt{2}) = \sqrt{2}(-\sqrt{2}) = 2$$

so

$$|\sqrt{2}|_L = |2|_K^{1/2} = 1$$

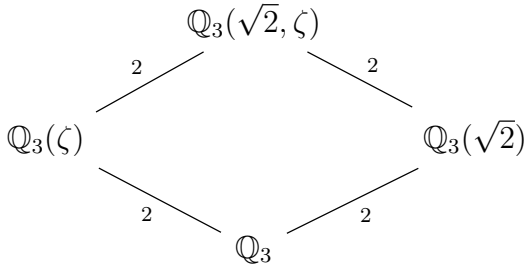
so $\sqrt{2} \in \mathcal{O}_L$. Thus there is an element of the residue field $k_L = \mathcal{O}_L/\mathfrak{m}_L$ which is a root of $x^2 - 2$. Since $x^2 - 2$ is irreducible over $k_K \cong \mathbb{F}_5$, the extension k_L/k_K has degree greater than 1, that is, $f > 1$. Since $ef = 2$, this forces $f = 2, e = 1$. Hence $\mathbb{Q}_5(\sqrt{2})$ is totally unramified over $\mathbb{Q}_5$.

Example 3.17.45. Let $K = \mathbb{Q}_5$ and $L = \mathbb{Q}_5(\sqrt{5})$, so $[L : K] = 2$. Normalize the discrete valuation on K so that $v_K(K^\times) = \mathbb{Z}$ and $v_L(L^\times) = \frac{1}{e}\mathbb{Z}$. Then

$$1 = v_L(5) = 2v_L(\sqrt{5}) \implies v_L(\sqrt{5}) = \frac{1}{2}$$

Thus $e \geq 2$, so $f = 1, e = 2$, and $\sqrt{5}$ is a uniformizer.

Example 3.17.46. Let $K = \mathbb{Q}_3$ and $L = \mathbb{Q}_3(\sqrt{2}, \zeta)$ where ζ is a primitive 3rd root of unity. Note that $[L : K] = 4$.



Note that ζ is a root of $x^2 + x + 1$ over $\mathbb{Q}_3$. By a similar argument as in Example 3.17.44,

$$e_{\mathbb{Q}_3}^{\mathbb{Q}_3(\sqrt{2})} = 1 \qquad f_{\mathbb{Q}_3}^{\mathbb{Q}_3(\sqrt{2})} = 2$$

Regarding $\mathbb{Q}_3(\zeta)$, we observe that

$$\begin{aligned} x^2 + x + 1 = (x - \zeta)(x - \zeta^2) &\implies 3 = (\zeta - 1)(\zeta^2 - 1) \\ &\implies v_{\mathbb{Q}_3(\zeta)}(3) = 1 = v_L(\zeta - 1) + v_L(\zeta^2 - 1) \end{aligned}$$

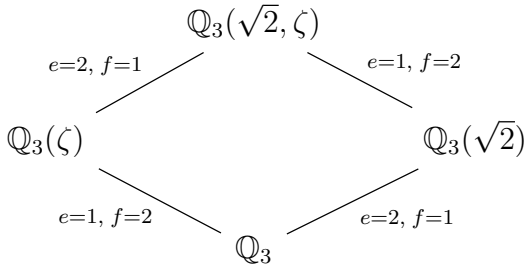
Since $\zeta - 1, \zeta^2 - 1$ are Galois conjugates, they have equal valuation. Hence

$$v_L(\zeta - 1) = \frac{1}{2}$$

so

$$e^{\mathbb{Q}_3(\zeta)}\mathbb{Q}_3 = 2 \qquad f_{\mathbb{Q}_3}^{\mathbb{Q}_3(\zeta)} = 1$$

Returning to our original diagram, we can write in the ramification and residual degrees we computed. Since all the extensions are degree 2, we can also deduce ramification and residual degrees for the upper extensions and the total extension L/K by multiplicativity in towers.



By multiplicativity in towers,

$$e_K^L = f_K^L = 2$$

3.17.4 Unramified extensions

Proposition 3.17.47. *Let K be a complete nonarchimedean discretely valued field, with perfect residue field k_K. For a finite unramified extension L/K, by the primitive element theorem we can write L as $L = K(\alpha)$ for some $\alpha \in L$. Define*

$$k_L = k_K(\overline{\alpha})$$

This gives a bijection

$$\begin{aligned}\Psi : \{\text{finite unramified extensions of } K\} &\to \{\text{finite extensions of } k_K\} \\ L = K(\alpha) &\mapsto k_L = k_K(\overline{\alpha})\end{aligned}$$

Furthermore, if L/K and L'/K are finite unramified extensions, there is an isomorphism

$$\begin{aligned}\mathrm{Hom}_K(L, L') &\to \mathrm{Hom}_{k_K}(k_L, k_{L'}) \\ \phi &\mapsto \phi|_{\mathcal{O}_L} \bmod \mathfrak{m}_K\end{aligned}$$

That is, the bijection Ψ is actually an equivalence of categories.

Proposition 3.17.48. *Let K be as above, and let L/K be a finite unramified extension. Then*

$$\mathrm{Aut}(L/K) \cong \mathrm{Aut}(k_L/k_K)$$

Thus L/K is Galois if and only if k_L/k_K is Galois and in this case,

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K)$$

In particular, if k_K is finite, then any unramified finite extension L/K is cyclic Galois. (Since any finite extension of a finite field is cyclic Galois.)

Proof. A finite extension L/K is Galois if and only if K is the fixed field of $\mathrm{Aut}(L/K)$. By the equivalence of categories above, $\mathrm{Aut}(L/K) \cong \mathrm{Aut}(k_L/k_k)$, and K is the fixed field of $\mathrm{Aut}(L/K)$ if and only k_K is the fixed field of $\mathrm{Aut}(k_L/k_K)$. □

Example 3.17.49. Let $K = \mathbb{Q}_p$. The residue field is $k_K = \mathbb{F}_p$. Since k_K has a unique finite extension of degree n for each $n \in \mathbb{Z}_{\geq 1}$, $\mathbb{Q}_p$ has a unique unramified extension L_n of degree n for each $n \in \mathbb{Z}_{\geq 1}$. Concretely,

$$L_n = \mathbb{Q}_p(\mu_{p^n-1})$$

where μ_{p^n-1} is the group of $p^n - 1$ roots of unity. To point out the blatantly obvious, L_n corresponds to the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$, and

$$\mathrm{Gal}(L_n/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

Proposition 3.17.50. *Let K be a complete nonarchimedean discretely valued field, with perfect residue field k_K, and let L/K be a finite separable extension. There exists a unique*

subextension K' such that L/K' is totally ramified and K'/K is unramified.

$$\begin{array}{c} L \\ {\scriptstyle f=1}\,\Big|\,{\scriptstyle \text{totally ramified}} \\ K' \\ {\scriptstyle e=1}\,\Big|\,{\scriptstyle \text{unramified}} \\ K \end{array}$$

*(K' is called the **maximal unramified extension** of K in L.)*

Proof. Since k_L/k_K is a finite extension, by the Proposition 3.17.47, there exists a unique unramified extension K'/K such that $k_L \cong k_{K'}$. By multiplicativity in towers, $f^L_{K'} = 1$. □

Example 3.17.51. Let $K = \mathbb{Q}_3, L = \mathbb{Q}_3(\sqrt{2}, \zeta)$ where ζ is a primitive 3rd root of unity. We considered this example previously, and saw that $\mathbb{Q}_3(\sqrt{2})$ is the maximal unramified subextension.

3.17.5 Totally ramified extensions

Proposition 3.17.52. *Let K be a complete nonarchimedean discretely valued field, and let L/K be a totally unramified extension, and set $e = [L : K]$. Let π_L be a uniformizer for L, and assume the discrete valuation v_L is normalized so that $v_L(\pi_L) = 1$. Then π_L satsifies an Eistenstein polynomial of degree e over $\mathcal{O}_K$, and*

$$\mathcal{O}_L = \mathcal{O}_K[\pi_L] \qquad L = K(\pi_L)$$

Conversely, if $f \in \mathcal{O}_K[x]$ is Eisenstein, then $K[x]/(f)$ is a totally ramified extension of K and if α is a root of f, then $v_{K(\alpha)}(\alpha) = 1$, so roots of f give uniformizers for $K(\alpha)$.

Example 3.17.53. Let ζ be a primitive 3rd root of unity. Then $\mathbb{Q}_3(\zeta)\mathbb{Q}$ is totally ramified of degree 2, with uniformizer $\zeta - 1$, since the minimal polynomial of ζ is $x^2 + x + 1$ and the minimal polynomial of $\zeta - 1$ is $x^2 + 3x + 3$, which is Eisenstein.

Proposition 3.17.54 (Krasner's lemma)**.** *Let K be a complete nonarchimedean discretely valued field. Let $f \in K[x]$ be monic irreducible with $d = \deg f$, and factor f over an algebraic closure K^{alg} as*

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

Suppose $\beta \in K^{\text{alg}}$ such that

$$|\beta - \alpha_1| < |\beta - \alpha_i| \qquad i = 2, 3, \ldots, d$$

Then $\alpha_1 \in K(\beta)$, hence $K(\alpha_1) \subset K(\beta)$.

Proof. The inequalities $|\beta - \alpha_1| < |\beta - \alpha_i|$ imply that α_1 is not equal to any other α_i, that is, α_1 is a simple root. Since the Galois group of f acts transitively on the roots, all the other roots must also be simple; that is, f has d distinct roots. Let

$$L = K(\beta) \qquad L' = K(\beta, \alpha_1, \ldots, \alpha_d)$$

Then L'/L is Galois, since it is the splitting field of f over L. For $\sigma \in \mathrm{Gal}(L'/L)$, we have $\sigma\beta = \beta$, hence

$$|\beta - \sigma\alpha_1| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1| < |\beta - \alpha_i|$$

That is, $\sigma\alpha_1$ is not equal to any of $\alpha_2, \ldots, \alpha_d$. Since the Galois group acts transitively on the roots, we must ahve $\sigma\alpha_1 = \alpha_1$, which is to say, α_1 is in the fixed field of $\mathrm{Gal}(L'/L)$, which is precisely $L = K(\beta)$. □

Definition 3.17.55. Let K be a complete nonarchimedean discretely valued field. We define a norm on $\mathcal{O}_K[x]$ by

$$\left\| \sum_i a_i x^i \right\| = \max_i |a_i|$$

This naturally induces a metric via

$$d(f, g) = \|f - g\|$$

Proposition 3.17.56 (Corollary of Krasner's lemma)**.** *Let K be a complete nonarchimedean discretely valued field. Let $f \in \mathcal{O}_K[x]$ be monic irreducible. Let $\alpha \in K^{\mathrm{alg}}$ be a root of f. There exists $\epsilon > 0$ such that for all $g \in \mathcal{O}_K[x]$ with $\|g - f\| < \epsilon$, g is irreducible and separable, and $K(\alpha) = K(\beta)$ for some root β of g.*

That is to say, in a sufficiently small neighborhood of a monic irreducible polynomial $f \in \mathcal{O}_K[x]$ under the norm defined above, every polynomial is separable and irreducible and defines the same extensions of K.

Proposition 3.17.57. *Let K be a p-adic field. For any $n \in \mathbb{Z}_{\geq 1}$, K has only finitely many extensions of degree n (up to K-isomorphism).*

Proof. Since $\mathrm{char}\, K = 0$, any finite extension is separable, and any separable extension of K factors as a tower of a totally ramified extension and an unramified extension.

By the equivalence of unramified extensions of K with extensions of the residue field $k_K \cong \mathbb{F}_p$, there is a unique (up to isomorphism) unramified extension of K of a given degree. So this reduces to showing there are finitely many totally ramified extensions of a given degree.

We know that totally ramified extensions are generated by roots of Eisenstein polynomials. Since K is local, $\mathcal{O}_K, \mathcal{O}_K^\times$ are compact. An Eisenstein polynomial has the form

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \qquad a_{n-1}, \ldots, a_1 \in \pi_K \mathcal{O}_K, \qquad a_0 \in \pi_K \mathcal{O}_K^\times$$

Thus the Eisenstein polynomials over $\mathcal{O}_K$ are parametrized by the set $S = (\pi_K \mathcal{O}_K)^{n-2} \times \pi_K \mathcal{O}_K^\times$, which is a compact subset of K^{n-1}. By the previous corollary, for $f \in S$, we can choose $\epsilon_f > 0$ such that for any polynomial in the open neighborhood of f with radius ϵ_f,

the roots of that polynomial generate the same extension as roots of f. Hence we have an open cover S by

$$S = \bigcup_{f \in S} B(f, \epsilon_f)$$

By compactness of S, we can choose a finite subcover. That is, all totally ramified extensions of K are generated by roots from a fintie list of Eisenstein polynomials. Since each Eisenstein polynomial has finitely many roots, this says that all the totally ramified extensions of K are generated by a finite list of elements, hence there are only finitely many totally ramified extensions of K. □

3.18 Results beyond our class

Theorem 3.18.1. *Let $p \in \mathbb{Z}$ be prime and ζ be a primitive pth root of unity. $\mathbb{Z}[\zeta]$ is a UFD if and only if $p \leq 19$. Equivalently, the class group of $\mathbb{Q}(\zeta)$ is trivial if and only if $p \leq 19$.*

Theorem 3.18.2. *Let $p \in \mathbb{Z}$ be prime and ζ be a primitive pth root of unity. $\mathbb{Z}[\zeta]$ has infinitely many units for $p \geq 5$.*

Theorem 3.18.3 (Class number formula)**.** *Let K be a number field. For $s \in \mathbb{C}$ with $\Re(s) > 1$, define the Dedekind zeta function of K,*

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^2}$$

(The sum is over all nonzero ideals $\mathfrak{a}$.) Note that ζ_K has analytic continuation to all of $\mathbb{C}$ which is meromorphic and has a simple pol at $s = 1$. The residue at $s = 1$ is given by

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} \operatorname{Reg}(K) h_K}{w_K \sqrt{|\Delta_K|}}$$

where $h_K = |\operatorname{Cl}(\mathcal{O}_K)|, w_K = |\mu(K)|, \Delta_K = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$.

4 Exercises

4.1 Informal exercises from lectures

4.1.1 Discriminants

Proposition 4.1.1. *Let $f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$. Note that f is irreducible by the rational root test. Let α be a root of f in a splitting field $\mathbb{Q}(\alpha)/\mathbb{Q}$. With respect to the basis $\{1, \alpha, \alpha^2\}$ of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, the discriminant is*

$$D(1, \alpha, \alpha^2) = -N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(f'(\alpha)) = -23$$

(The first equality is given, the content of this is the second equality.) Thus by Proposition 3.2.20, $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Proof. Note that $f'(\alpha) = 3\alpha^2 - 1$. Recall that by definition, $N(3\alpha^2 - 1)$ is the determinant of the matrix of $3\alpha^2 - 1$ as a $\mathbb{Q}$-linear transformation $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$. We compute

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

$$(3\alpha^2 - 1)(\alpha) = 3\alpha^3 - \alpha = 3(\alpha + 1) - \alpha = 2\alpha + 3 = \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}$$

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

Thus, with respect to the basis $\{1, \alpha, \alpha^2\}$, the matrix of $3\alpha^2 - 1$ is

$$\begin{pmatrix} -1 & 3 & 0 \\ 0 & 2 & 3 \\ 3 & 0 & 2 \end{pmatrix} = 23$$

Thus $D(1, \alpha, \alpha^2) = -23$. □

Proposition 4.1.2. *Let K be a field and suppose $f(x) = x^n + ax + b \in K[x]$ is irreducible and separable over K. Let β be a root of f, and let $L = K(\beta)$. Then the discriminant of L/K with respect to the basis $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ is*

$$D(1, \beta, \ldots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_K^L(f'(\beta)) = (-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n \right)$$

Proof. We may assume that $n \geq 3$, since we already computed the discriminant in the case $k = 2$ in Example 2.2.11. Note that $N_K^L(\beta) = (-1)^n b$, and since $n \geq 3$, $\mathrm{Tr}_K^L(\beta) = 0$. By Proposition 3.2.13, it suffices to prove that

$$\mathrm{N}_K^L(f'(\beta)) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n$$

Set

$$\gamma = f'(\beta) = n\alpha^{n-1} + a = -(n-1)a - nb\beta^{-1}$$

so then

$$\beta = \frac{-nb}{\gamma + (n-1)a}$$

Thus $K(\beta) = K(\gamma)$, so the minimal polynomial of γ over K also has degree n. We want to find the minimal polynomial of γ. To that end, let $P(x), Q(x) \in K[x]$ so that

$$f\left(\frac{-nb}{x + (n-1)a}\right) = \frac{P(x)}{Q(x)}$$

so that when we substitute $\gamma = x$, we get

$$f\left(\frac{-nb}{\gamma + (n-1)a}\right) = f(\beta) = 0 \implies P(\gamma) = 0$$

Thus P divides the minimal polynomial of γ. If we can show that $\deg P = n$, then (a monic version of) P is the minimal polynomial of γ. Now we compute $P(x)$.

$$\begin{aligned} f\left(\frac{-nb}{x + (n-1)a}\right) &= \left(\frac{-nb}{x + (n-1)a}\right)^n + \left(\frac{-nb}{x + (n-1)a}\right) a + b \\ &= \frac{(-nb)^n - nba(x + (n-1)a)^{n-1} + b(x + (n-1)a)^n}{(x + (n-1)a)^n} \end{aligned}$$

thus

$$P(x) = (-nb)^n - nba(x + (n-1)a)^{n-1} + b(x + (n-1)a)^n$$

which has degree n (as a polynomial in x), so P is an irreducible polynomial for which γ is a root. To make it monic, we multiply by b^{-1}, so $b^{-1}P(x)$ is the minimal polynomial of γ. Then we can compute the norm of γ by looking at the constant term of of $b^{-1}P(x)$ (up to sign), so

$$\begin{aligned} N_K^L(\gamma) &= (-1)^n\Big(\text{ constant term of } b^{-1}P(x)\Big) \\ &= b^{-1}(-1)^n\Big((-nb)^n - nba((n-1)a)^{n-1} + b((n-1)a)^n\Big) \\ &= n^n b^{n-1} - (-1)^n n(n-1)^{n-1}a^n + (-1)^n(n-1)^n a^n \\ &= n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n\Big(n - (n-1)\Big) \\ &= n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n \end{aligned}$$

□

4.1.2 Class groups

Proposition 4.1.3. *Let A be a Dedekind domain.* $\mathrm{Cl}(A)$ *is trivial if and only if A is a PID.*

Proof. If A is a PID, then since $\mathrm{Id}(A)$ is generated by principal ideals, $P(A) = \mathrm{Id}(A)$ so the class group is trivial. Conversely, if $\mathrm{Cl}(A)$ is trivial, then $\mathrm{Id}(A) = P(A)$, so every fractional ideal of A is principal, so every ideal of A is principal. □

Proposition 4.1.4. *Let A be a Dedekind domain, and let $S \subset A$ be a multiplicative subset. Then the canonical embedding $A \to S^{-1}A, a \mapsto \frac{a}{1}$ induces an isomorphism between $\mathrm{Id}(S^{-1}A)$ and the subgroup of $\mathrm{Id}(A)$ generated by primes of A that do not intersect S.*

Proof. This is just a consequence of the ideal correspondence for localization, which says that primes of $S^{-1}A$ are in bijection with primes of A that do not intersect S. We know that $S^{-1}A$ is a Dedekind domain, so by unique factorization of ideals on both sides, the $\mathrm{Id}(S^{-1}A)$ and $\mathrm{Id}(A)$ are both free abelian on sets of generators which are in bijection, so they are isomorphic. □

4.1.3 $\mathbb{Q}_p$

Lemma 4.1.5. *Let p be a prime, and let*

$$x = \sum_{i \geq v_p(x)} b_i p^i \in \mathbb{Q}_p$$

If x has only finitely many nonzero terms, then $x \in \mathbb{Q}$.

Proof. Obvious. □

Remark 4.1.6. Let p be a prime and $k \in \mathbb{Z}, k \neq 0$. Then in $\mathbb{Q}_p$, we have

$$\frac{1}{1-p^k} = 1 + p^k + p^{2k} + \cdots$$

Proposition 4.1.7. *Let p be a prime, and let*

$$x = \sum_{i \geq v_p(x)} b_i p^i \in \mathbb{Q}_p$$

Then $x \in \mathbb{Q}$ if and only if the sequence (b_i) is eventually periodic.

Proof. Let $x \in \mathbb{Q}$ and write $x = \frac{a}{b}$ with $\gcd(a, b) = 1$. Let n be the highest power of p dividing $1 - b$, so we can write $p^n y = 1 - b$ for some $y \in \mathbb{Z}$, with $\gcd(y, p) = 1$. Then in $\mathbb{Q}_p$, we have the equality

$$\frac{a}{b} = \frac{a}{1-(1-b)} = \frac{a}{1-p^n y} = a + ayp^n + ay^2 p^{2n} + \cdots$$

To get our unique representative of x, we need to reduce the coefficients $a, ay, ay^2, \ldots$ mod p. Since $a, y \in \mathbb{Z}$, this sequence is eventually periodic, since there are only finitely many residues mod p. (There are also $n-1$ terms with coefficient zero between each of these nonzero coefficient, but these do not affect the periodicity.) Thus the sequence of (b_i) corresponding to x is eventually periodic.

For the converse, suppose $x = \sum b_i p^i \in \mathbb{Q}_p$ with (b_i) eventually periodic. Write $x = y + z$ where z is the periodic tail, and y has only finitely many nonzero terms. By Lemma 4.1.5, $y \in \mathbb{Q}$, so $x \in \mathbb{Q} \iff z \in \mathbb{Q}$. So we have reduced to showing that z is rational. Let $z = \sum a_i p^i$, and we know that $a_{i+k} = a_i$ for some k and all i. We can rearrange the terms of the series freely since it converges absolutely, so we gather the terms with matching coefficients.

$$\begin{aligned} z &= a_{-m}p^{-m} + a_{-m+1}p^{-m} + \cdots + a_{-m}p^{-m+k} + a_{-m+1}p^{-m+k+1} + \cdots \\ &= a_{-m}\Big(p^{-m} + p^{-m+k} + p^{-m+2k} + \cdots\Big) \\ &\quad + a_{-m+1}\Big(p^{-m+1} + p^{-m+1+k} + p^{-m+1+2k} + \cdots\Big) \\ &\quad\quad \vdots \\ &\quad + a_{-m+k-1}\Big(p^{-m+k-1} + p^{-m+2k-1} + p^{-m+3k-1} + \cdots\Big) \end{aligned}$$

Then we factor p^{-m+k-j} out of the power series in p next to each a_{-m+j}, and get

$$\begin{aligned} z &= \sum_{j=0}^{k-1} a_{-m+j}p^{-m+j}\Big(1 + p^k + p^{2k} + \cdots\Big) \\ &= \sum_{j=0}^{k-1} a_{-m+j}p^{-m+j}\left(\frac{1}{1-p^k}\right) \end{aligned}$$

This is now a finite sum of rational numbers, hence $z \in \mathbb{Q}$. □

4.2 Homework set 1

Proposition 4.2.1. *Let $K/\mathbb{Q}$ be a number field, and let $N_{\mathbb{Q}}^K : K^\times \to \mathbb{Q}^\times$ be the norm map. Then*

1. *$N_{\mathbb{Q}}^K$ maps $\mathcal{O}_K^\times$ to $\{\pm 1\}$.*
2. *Conversely, if $a \in \mathcal{O}_K$ satisfies $N_{\mathbb{Q}}^K(a) = \pm 1$, then $a \in \mathcal{O}_K^\times$.*

Proof. Let $a \in \mathcal{O}_K^\times$, with inverse $a^{-1} \in \mathcal{O}_K^\times$. Then

$$1 = N_{\mathbb{Q}}^K(1) = N_{\mathbb{Q}}^K(aa^{-1}) = N_{\mathbb{Q}}^K(a)N_{\mathbb{Q}}^K(a^{-1})$$

Since we know that $N_{\mathbb{Q}}^K$ maps $\mathcal{O}_K$ to $\mathbb{Z}$ (Corollary 2.21 of Milne [**?**]), this says that $N_{\mathbb{Q}}^K(a)$ is a unit in $\mathbb{Z}$, hence $N_{\mathbb{Q}}^K(a) = \pm 1$. For the converse, we know that a^{-1} exists in $K^\times$, we just need to show $a^{-1} \in \mathcal{O}_K^\times$. Suppose $N_{\mathbb{Q}}^K(a) = \pm 1$, so the minimal polynomial of a in $\mathbb{Z}[x]$ is

$$a^n + b_{n-1}a^{n-1} + \ldots + b_1 a + (\pm 1) = 0$$

We multiply this equation by a^{-n}, and obtain

$$1 + b_{n-1}a^{-1} + \ldots + b_1\left(a^{-1}\right)^{n-1} + (\pm 1)\,a^{-n} = 0$$

Up to sign, this is a monic polynomial in $\mathbb{Z}[x]$, so $a^{-1} \in \mathcal{O}_K^\times$. □

For the next proposition, recall that the ring of integers of a quadratic extension $K = \mathbb{Q}\left(\sqrt{-D}\right)$ is $\mathbb{Z}[\sqrt{-D}]$ if $-D \equiv 2, 3 \bmod 4$, and $\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$ if $-D \equiv 1 \bmod 4$.

Proposition 4.2.2. *Let $K = \mathbb{Q}(\sqrt{-D})$ where $D \geq 1$ is a square free integer. Then*

1. $\mathcal{O}_K^\times = \{\pm 1\}$ *if* $D \neq 1, D \neq 3$.
2. $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$ *if* $D = 1$.
3. $\mathcal{O}_K^\times = \left(\pm 1, \pm\frac{1+\sqrt{-3}}{2}, 1 - \frac{1+\sqrt{-3}}{2}, -1 + \frac{1+\sqrt{-3}}{2}\right)$ *if* $D = 3$.

Proof. When $-D \equiv 2, 3 \bmod 4$, the norm map is given by

$$N_{\mathbb{Q}}^K\left(a + b\sqrt{-D}\right) = \left(a + b\sqrt{-D}\right)\left(a - b\sqrt{-D}\right) = a^2 + Db^2$$

When $-D \equiv 1 \bmod 4$, the norm map is given by

$$N_{\mathbb{Q}}^K\left(a + b\frac{1+\sqrt{-D}}{2}\right) = \left(a + b\frac{1+\sqrt{-D}}{2}\right)\left(a + b\frac{1-\sqrt{-D}}{2}\right) = a^2 + ab + b^2\left(\frac{1+D}{4}\right)$$

By Proposition 4.2.1, $a \in \mathcal{O}_K$ is a unit if and only if $N_{\mathbb{Q}}^K(a) = \pm 1$.

First, we consider the case $D = 1$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The norm of $a + bi \in \mathbb{Z}[i]$ is $a^2 + b^2$, which is ± 1 only if one of a, b is zero and the other is ± 1 (since $a, b \in \mathbb{Z}$). Thus units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Now consider $D = 3$, so $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, and the norm of $a + b\left(\frac{1+\sqrt{-3}}{2}\right)$ is $a^2 + ab + b^2$, so we analyze integral solutions to this. If one of a, b is zero, the other must be ± 1, and one checks that $(\pm 1, 0), (0, \pm 1)$ are solutions. If one of a, b is ± 1, say $a = \pm 1$, then b satisfies one of the four equations

$$b(b \pm 1) = -1 \pm 1$$

Two of these have no solutions, and the other two give the solutions $(1, -1), (-1, 1)$. The six solutions mentioned give rise to the listed units. We claim there are no other solutions.

Suppose (a, b) is a solution not already listed, with $|a|, |b| \geq 2$. Note that a, b must have opposite signs. Taking absolute values, we obtain

$$1 = |\pm 1| = |a^2 + ab + b^2| \geq |a^2| + |b^2| - |ab|$$

Without loss of generality, suppose $|a| \leq |b|$. Note that $a \neq 0$ implies $|a| \geq 2$, so

$$|ab| \leq |b^2| \implies |b^2| - |ab| \geq 0 \implies |a^2| + |b^2| - |ab| \geq 2$$

Combining our two strings of inequalities, we obtain $1 \geq 2$, which is false, so no such solution exists.

Now we consider more generally $D \neq 1, 3$. If $-D \equiv 2, 3 \bmod 4$, units are $a + b\sqrt{-D}$ so that $a^2 + Db^2 = 1$. Since $D > 1$, we must have $b = 0$, and then the only solutions are $a = \pm 1$. If $-D \equiv 1 \bmod 4$, units are $a + b\left(\frac{1+\sqrt{-D}}{2}\right)$ satisfying $a^2 + ab + b^2\left(\frac{1+D}{4}\right) = \pm 1$. Since $D \neq 3$, $\left|\frac{1+D}{4}\right| > 1$, so the same chain of absolute values as in the case $D = 3$ prohibits any units with $|a|, |b| \geq 2$. Then one may tediously check the possibilities with $a, b \in \{0, \pm 1\}$ to conclude that only $a = \pm 1, b = 0$ are solutions. $\square$

Exercise 3. For each of the following irreducible polynomials, we let α be a root and $K = \mathbb{Q}(\alpha)$. Then we compute $\mathcal{O}_K, \operatorname{disc}(K/\mathbb{Q})$, and factorizations of $2, 3, 5, 7$ in $\mathcal{O}_K$.

(a) $f(x) = x^2 + 31$

(b) $f(x) = x^2 + 39$

(c) $f(x) = x^2 - 29$

(d) $f(x) = x^3 + x - 1$

Solution. (a) In this case, $\alpha = \sqrt{-31}$ and $K = \mathbb{Q}(\sqrt{-31})$. Since $-31 \equiv 1 \bmod 4$, the ring of integers is $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-31}}{2}\right]$. Let $\beta = \frac{1+\sqrt{-31}}{2}$. We compute the discriminant using the basis $1, \beta$. Note that $\beta^2 = \frac{1}{2}(\alpha - 15)$, so

$$\operatorname{Tr}\beta = \frac{1}{2}\operatorname{Tr}\alpha - \frac{1}{2}\operatorname{Tr}15 = 0 - 15 = -15$$

$$D(1,\beta) = \det\begin{pmatrix} \operatorname{Tr}1 & \operatorname{Tr}\beta \\ \operatorname{Tr}\beta & \operatorname{Tr}\beta^2 \end{pmatrix} = \det\begin{pmatrix} 2 & 1 \\ 1 & -15 \end{pmatrix} = -31$$

To factor $2, 3, 5, 7$ in $\mathcal{O}_K$, we use Kummer's theorem which says that a factorization of the minimal polynomial of β mod p gives a factorization of p in $\mathcal{O}_K$. The minimal polynomial of β is $x^2 - x + 8$.

$$\begin{aligned} &x^2 - x + 8 \equiv x^2 + x = x(x+1) \bmod 2 \\ &x^2 - x + 8 \equiv x^2 - x + 2 \text{ is irreducible mod } 3 \\ &x^2 - x + 8 \equiv (x-2)(x-4) \bmod 5 \\ &x^2 - x + 8(x-3)(x-5) \bmod 7 \end{aligned}$$

Thus

$$\begin{aligned} &(2)\mathcal{O}_K = (2,\beta)\,(2,\beta+1) \\ &(3)\mathcal{O}_K \text{ is prime} \\ &(5)\mathcal{O}_K = (5,\beta-2)(5,\beta-4) \\ &(7)\mathcal{O}_K = (7,\beta-3)(7,\beta-5) \end{aligned}$$

(b) In this case $\alpha = \sqrt{-39}$. Since $-39 \equiv 1 \bmod 4$, the ring of integers is $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-39}}{2}\right]$. Let $\beta = \frac{1+\sqrt{-39}}{2}$. Note that $\beta^2 = \frac{1}{2}(\alpha - 19)$.Using the basis $1, \beta$, the discriminant is

$$\operatorname{Tr}\beta^2 = \frac{1}{2}\operatorname{Tr}\alpha - \frac{1}{2}\operatorname{Tr}(19) = -19$$

$$D(1,\beta) = \det\begin{pmatrix} \operatorname{Tr}1 & \operatorname{Tr}\beta \\ \operatorname{Tr}\beta & \operatorname{Tr}\beta^2 \end{pmatrix} = \det\begin{pmatrix} 2 & 1 \\ 1 & -19 \end{pmatrix} = -39$$

To factor $2, 3, 5, 7$ in $\mathcal{O}_K$, we factor the minimal polynomial of β modulo the prime in question. The minimal polynomial of β is $x^2 - x + 10$.

$$\begin{aligned} x^2 - x + 10 &\equiv x(x+1) \bmod 2 \\ x^2 - x + 10 &\equiv (x-2)^2 \bmod 3 \\ x^2 - x + 10 &\equiv x(x-1) \bmod 5 \\ x^2 - x + 10 &\text{ is irreducible mod } 7 \end{aligned}$$

Thus

$$\begin{aligned} 2\mathcal{O}_K &= (2, \beta)(2\beta + 1) \\ 3\mathcal{O}_K &= (3, \beta - 2)^2 \\ 5\mathcal{O}_K &= (5, \beta)(5, \beta - 1) \\ 7\mathcal{O}_K &\text{ is prime} \end{aligned}$$

(c) In this case $\alpha = \sqrt{29}$ and $K = \mathbb{Q}(\sqrt{29})$. Since $29 \equiv 2 \bmod 3$, the ring of integers is $\mathbb{Z}[\sqrt{29}]$. Using the basis $1, \alpha$, the discriminant is

$$D(1, \alpha) = \det \begin{pmatrix} \operatorname{Tr} 1 & \operatorname{Tr} \alpha \\ \operatorname{Tr} \alpha & \operatorname{Tr} \alpha^2 \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2(29) \end{pmatrix} = 4(29)$$

We factor $x^2 + 29$ modulo the primes $2, 3, 5, 7$ to calculate their factorizations in $\mathcal{O}_K$.

$$\begin{aligned} x^2 + 29 &\equiv (x+1)^2 \bmod 2 \\ x^2 + 29 &\equiv (x+1)(x+2) \bmod 3 \\ x^2 + 29 &\equiv (x-1)(x-4) \bmod 5 \\ x^2 + 29 &\text{ is irreducible mod } 7 \end{aligned}$$

Thus

$$\begin{aligned} 2\mathcal{O}_K &= (2, \alpha + 1)^2 \\ 3\mathcal{O}_K &= (3, \alpha + 1)(3, \alpha + 2) \\ 5\mathcal{O}_K &= (5, \alpha - 1)(5, \alpha - 4) \\ 7\mathcal{O}_K &\text{ is prime} \end{aligned}$$

(d) Let $f(x) = x^3 + x - 1$ and let α be a root of f, and let $K = \mathbb{Q}(\alpha)$. Let $N = \mathbb{Z}[\alpha] \subset \mathcal{O}_K$. In class we showed that

$$D(1, \alpha, \alpha^2) = [\mathcal{O}_K : N]^2 \operatorname{disc}(\mathcal{O}_K / \mathbb{Z})$$

so if $D(1, \alpha, \alpha^2)$ is square-free, we can conclude that $\mathcal{O}_K = N$. Denote $\operatorname{Tr}_{\mathbb{Q}}^K$ by Tr. Since f is the minimal polynomial of α, we can read off $\operatorname{Tr} \alpha = 0$. Using a CAS, the minimal polynomial of α^2 is $x^3 + 2x^2 + x - 1$, so $\operatorname{Tr} \alpha^2 = -2$. Since $\alpha^3 = 1 - \alpha$, we have

$$\operatorname{Tr}(1 - \alpha) = \operatorname{Tr} 1 - \operatorname{Tr} \alpha = 3 \qquad \operatorname{Tr} \alpha^4 = \operatorname{Tr}(\alpha - \alpha^2) = \operatorname{Tr} \alpha - \operatorname{Tr} \alpha^2 = 2$$

$$D(1,\alpha,\alpha^2) = \det \begin{pmatrix} \operatorname{Tr} 1 & \operatorname{Tr}\alpha & \operatorname{Tr}\alpha^2 \\ \operatorname{Tr}\alpha & \operatorname{Tr}\alpha^2 & \operatorname{Tr}\alpha^3 \\ \operatorname{Tr}\alpha^2 & \operatorname{Tr}\alpha^3 & \operatorname{Tr}\alpha^4 \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & -2 \\ 0 & -2 & 3 \\ -2 & 3 & 2 \end{pmatrix} = -31$$

Since -31 is a square-free integer, we conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. By the calculation we just did, $\operatorname{disc}(K/\mathbb{Q}) = -31$, since $1, \alpha, \alpha^2$ is a basis for $\mathcal{O}_K$ over $\mathbb{Z}$. To factor $2, 3, 5, 7$ in $\mathbb{Z}[\alpha]$, we use Kummer's theorem.

$$\begin{aligned} &x^3 + x - 1 \text{ is irreducible mod } 2 \\ &x^3 + x - 1 \equiv (x-2)(x^2+2x+2) \bmod 3 \\ &x^3 + x - 1 \text{ is irreducible mod } 5 \\ &x^3 + x - 1 \text{ is irreducible mod } 7 \end{aligned}$$

and note that $x^2 + 2x + 2$ is irreducible mod 3. Thus $2\mathcal{O}_K, 5\mathcal{O}_K, 7\mathcal{O}_K$ are prime, and

$$3\mathcal{O}_K = (3, \alpha - 2)(3, \alpha^2 + 2\alpha + 2)$$

Remark 4.2.3. We clarify the statement of the next proposition. Let K be a number field with ring of integers $\mathcal{O}_K$, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a (nonzero, proper) prime ideal. Since $\mathcal{O}_K$ is a Dedekind domain, $\mathfrak{p}$ is maximal, so $\mathcal{O}_K/\mathfrak{p}$ is a field. We also know that $\mathcal{O}_K/\mathfrak{p}$ is finite.

Proposition 4.2.4 (Exercise 4)**.** *Let K be a number field, with ring of integers $\mathcal{O}_K$, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal, and let $p = \operatorname{char} \mathcal{O}_K/\mathfrak{p}$. Then there exists $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} = (p, \alpha)$.*

Proof. The fact that $\mathcal{O}_K/\mathfrak{p}$ has characteristic p says that $p \equiv 0 \bmod \mathfrak{p}$, which is to say, $p \in \mathfrak{p}$. Since $\mathcal{O}_K$ is a Dedekind domain, by Corollary 3.16 of Milne [**?**], there exists $\alpha \in \mathfrak{p}$ so that $\mathfrak{p} = (p, \alpha)$. □

Proposition 4.2.5 (Exercise 5)**.** *Let p, q be distinct primes in $\mathbb{Z}$, and let n be the order of q in $\mathbb{F}_p^\times$. Let ζ_p be a primitive pth root of unity, and $K = \mathbb{Q}(\zeta_p)$. Then*

(a) q is unramified in K.

(b) If q factors as

$$q\mathcal{O}_K = \mathfrak{P}_1 \dots \mathfrak{P}_r$$

then $r = \frac{p-1}{n}$.

Proof. (a) We computed in class that the discriminant of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is $\pm p^{p-2}$, and we know that the only primes that ramify are ones dividing the discriminant. Thus p is the only prime that ramifies, and since $q \neq p$, q is unramified.

(b) By part (a), we know that $q\mathcal{O}_K$ factors as $\mathfrak{P}_1 \dots \mathfrak{P}_r$ with $\mathfrak{P}_i$ distinct primes of $\mathcal{O}_K$. We computed in class that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Since $K/\mathbb{Q}$ is Galois and $[K : \mathbb{Q}] = p - 1$, by the fundamental relation, we have $efr = fr = p - 1$, where $f = \dim_{\mathbb{F}_q} \mathbb{Z}[\zeta_p]/\mathfrak{P}_1$. To finish the proof, it suffices to show that $f = n$.

Since $\mathcal{O}_K$ is a Dedekind domain, $\mathfrak{P}_1$ is maximal, so $\mathbb{Z}[\zeta_p]/\mathfrak{P}_1$ is a field, and by the classification of finite fields, it must be $\mathbb{F}_{q^f}$. Since $\mathbb{Z}[\zeta_p]$ is generated over $\mathbb{Z}$ by ζ_p, $\mathbb{Z}[\zeta_p]/\mathfrak{P}_1$ is generated over $\mathbb{F}_q$ by ζ_p, so $\mathbb{Z}[\zeta_p]/\mathfrak{P}_1 \cong \mathbb{F}_q(\zeta_p) \cong \mathbb{F}_{q^f}$. INCOMPLETE

Another approach: The minimal polynomial of ζ_p over $\mathbb{Z}$ is $\phi_p(x) = 1+x+\ldots+x^{p-1}$. By a theorem of Kummer from class, the factorization of $q\mathbb{Z}[\zeta_p]$ is determined by the factorization of ϕ_p modulo q, so it suffices to factor $1 + x + \ldots + x^{p-1}$ modulo q. If what we want is true, then ϕ_p should split into $\frac{p-1}{n}$ irreducible factors. INCOMPLETE

□

Proposition 4.2.6 (Exercise 6)**.** *Let $K \subset L \subset M$ be a tower of number fields, with respective rings of integers $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_M$. Let $\mathfrak{p}_K \subset_{\mathcal{K}}$ be a prime ideal, and let $\mathfrak{p}_L \subset \mathcal{O}_L, \mathfrak{p}_M \subset \mathcal{O}_M$ be prime ideals such that*

$$\mathfrak{p}_L \cap \mathcal{O}_K = \mathfrak{p}_K \qquad \mathfrak{p}_M \cap \mathcal{O}_K = \mathfrak{p}_K$$

Then

$$e(\mathfrak{p}_M/\mathfrak{p}_K) = e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K) \qquad f(\mathfrak{p}_M/\mathfrak{p}_K) = f(\mathfrak{p}_M/\mathfrak{p}_L)f(\mathfrak{p}_L/\mathfrak{p}_K)$$

Proof. Recall that $\mathfrak{p}_L \cap \mathcal{O}_K\mathfrak{p}_K$ is equivalent to saying that $\mathfrak{p}_L$ appears in the (unique) factorization of $\mathfrak{p}_K\mathcal{O}_L$, and that $e(\mathfrak{p}_L/\mathfrak{p}_K)$ is, by definition, the power of $\mathfrak{p}_L$ in that factorization. We use $(\cdots)$ to denote the irrelevant part of the factorization.

$$\begin{aligned}
\mathfrak{p}_K\mathcal{O}_L &= \mathfrak{p}_L^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots) \\
\mathfrak{p}_K\mathcal{O}_M &= \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_K)}(\cdots) \\
\mathfrak{p}_L\mathcal{O}_M &= \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_L)}(\cdots)
\end{aligned}$$

Putting these together, we obtain

$$\begin{aligned}
\mathfrak{p}_K\mathcal{O}_M &= (\mathfrak{p}_K\mathcal{O}_L)\mathcal{O}_M \\
&= \left(\mathfrak{p}_L^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots)\right)\mathcal{O}_M \\
&= (\mathfrak{p}_L\mathcal{O}_M)^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots) \\
&= \left(\mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_L)}(\cdots)\right)^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots) \\
&= \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots)
\end{aligned}$$

Note that in each step, the unwritten parts of the factorization $(\cdots)$ do not include any factors of $\mathfrak{p}_M$. Comparing this with the factorization $\mathfrak{p}_K\mathcal{O}_M = \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_K)}(\cdots)$, by uniqueness we conclude that the powers of $\mathfrak{p}_M$ are equal, that is,

$$e(\mathfrak{p}_M/\mathfrak{p}_K) = e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K)$$

The statement for f is simpler to prove. Since $\mathfrak{p}_K \subset \mathfrak{p}_L \subset \mathfrak{p}_M$, we have a tower of fields $\mathcal{O}_K/\mathfrak{p}_K \subset \mathcal{O}_L/\mathfrak{p}_L \subset \mathcal{O}_M/\mathfrak{p}_M$, and then from multiplicativity of field degrees in towers, we get

$$\begin{aligned}
f(\mathfrak{p}_M/\mathfrak{p}_K) &= [\mathcal{O}_M/\mathfrak{p}_M : \mathcal{O}_K/\mathfrak{p}_K] \\
&= [\mathcal{O}_M/\mathfrak{p}_M : \mathcal{O}_L/\mathfrak{p}_L][\mathcal{O}_L/\mathfrak{p}_L : \mathcal{O}_K/\mathfrak{p}_K] \\
&= f(\mathfrak{p}_M/\mathfrak{p}_L)f(\mathfrak{p}_L/\mathfrak{p}_K)
\end{aligned}$$

□

Proposition 4.2.7 (Exercise 7)**.** *Let $K = \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{11})$. Then*

$$7\mathcal{O}_K = \mathfrak{P}_1^2\mathfrak{P}_2^2$$

for some prime ideals $\mathfrak{P}_1, \mathfrak{P}_2 \subset \mathcal{O}_K$.

Proof. First, note that $K/\mathbb{Q}$ is the splitting field of $(x^2-5)(x^2-7)(x^2-11)$, so it is Galois. By Galois theory, $[K : \mathbb{Q}] = 8$ [1]. We can write $7\mathcal{O}_K = \mathfrak{P}_1^e \dots \mathfrak{P}_r^e$, and the fundamental relation gives $efr = 8$. Now we just need to show $e = f = r = 2$. As a first step, consider the tower $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{7}) \subset K$. From our study of quadratic extensions, we know that 7 ramifies, that is,

$$7\mathcal{O}_L = \mathfrak{P}^2$$

so $e(7\mathcal{O}_L/7\mathbb{Z}) = 2$, with $f = r = 1$ here. By Exercise 6 (multiplicativity in towers), this tower gives a lower bound $e(7\mathcal{O}_K/7\mathbb{Z}) \geq 2$. Now consider the tower

$$\mathbb{Q} \subset M = \mathbb{Q}(\sqrt{5}, \sqrt{11}) = \mathbb{Q}(\sqrt{5} + \sqrt{11}) \subset K$$

Using a computer algebra system, the minimal polynomial of $\mathbb{Q}(\sqrt{5}+\sqrt{11})$ is $x^4 - 32x^2 + 36$, which factors into two irreducible quadratics modulo 7.

$$x^4 - 32x^2 + 36 \equiv (x^2 + 3x + 6)(x^2 + 4x + 6) \bmod 7$$

Thus by a theorem of Kummer, $7\mathcal{O}_M = \mathfrak{P}_1\mathfrak{P}_2$, so

$$e(7\mathcal{O}_M/7\mathbb{Z}) = 1 \qquad r(7\mathcal{O}_M/7\mathbb{Z}) = 2 \qquad f(7\mathcal{O}_M/7\mathbb{Z}) = 2$$

By mutliplicativity in towers, we get lower bounds $f(7\mathcal{O}_K/7\mathbb{Z}) \geq 2$ and $r(7\mathcal{O}_K/7\mathbb{Z}) \geq 2$. Now we have $e, f, r \geq 2$, and $efr = 8$, so the only possibility is $e = f = r = 2$. □

Proposition 4.2.8 (Exercise 8)**.** *Let A be an integral domain, and $K = \mathrm{Frac}(A)$, and L/K a finite extension. Let B be the integral closure of A in L, and $S \subset A$ a multiplicative subset. Then $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.*

Proof. First we show that every element of $S^{-1}B$ is integral over $S^{-1}A$. Let $x = \frac{b}{s} \in S^{-1}B$. Since B is integral over A, b satisfies a monic polynomial in $A[x]$, so we have a relation in B of the form

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

Since B is an integral domain, the canonical map $B \to S^{-1}B$ is injective, so may view this as a relation in $S^{-1}B$. Then we multiply by s^{-n} to obtain

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_0}{s^n} = 0$$

[1] In fact, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$. For a general computation, see Proposition 0.18 of `http://users.math.msu.edu/users/ruiterj2/Math/Documents/Spring%202017/Algebra/Homework_4.pdf`

which says that $\frac{b}{s}$ satisfies a monic polynomial in $S^{-1}A$, hence $\frac{b}{s}$ is integral over $S^{-1}A$. To finish the proof, we need to show that every integral element of L over $S^{-1}A$ lies in $S^{-1}B$. Let $\alpha \in L$ be integral over $S^{-1}A$, so there is a relation in $S^{-1}A$ of the form

$$\alpha^n + \left(\frac{a_{n-1}}{s_{n-1}}\right)\alpha^{n-1} + \ldots + \frac{a_0}{s_0} = 0$$

with $a_i \in A, s_i \in S$. Clearing denominators, there exists $s \in S$ so that αs is integral over A, so $s\alpha \in B$, so $\alpha \in S^{-1}B$. □

Proposition 4.2.9. *Let $v : K^\times \to \mathbb{Z}$ be a discrete valuation.*

1. *If $x \in K^\times$ is an element of finite order, then $v(x) = 0$. In particular, $v(a) = v(-a)$.*
2. *If $a, b \in K^\times$ and $v(a) > v(b)$, then $v(a + b) = v(b)$.*
3. *Suppose there are $a_1, \ldots, a_n \in K^\times$ with*

$$a_1 + \ldots + a_n = 0$$

Then the minimal value of $v(a_i)$ is attained for at least two indices i.

Proof. (1) If $x^n = 1$, then $0 = v(1) = v(x^n) = nv(x)$ so $v(x) = 0$. Consequently,

$$v(-a) = v(-1) + v(a) = 0 + v(a) = v(a)$$

(2) Suppose $v(a) > v(b)$. Then

$$v(a + b) \geq \min\Big(v(a), v(b)\Big) = v(b)$$

On the other hand,

$$v(b) = v(a + b - a) \geq \min\Big(v(a + b), v(-a)\Big) = \min\Big(v(a + b), v(a)\Big)$$

Since $v(b) < v(a)$, this min can't be $v(a)$, so it is $v(a + b)$. Thus $v(b) \geq v(a + b)$. Since we have inequality both ways, $v(b) = v(a+b)$. (3) Suppose $a_1 + \ldots + a_n = 0$ with $a_i \in K^\times$. Fix j so that $v(a_j)$ is minimal. Then rearrange the equation to

$$-a_j = a_1 + \ldots + \widehat{a_j} + \ldots + a_n$$

Applying v to this, we obtain

$$v(-a_j) = v(a_j) = v\Big(a_1 + \ldots + \widehat{a_j} + \ldots + a_n\Big) \geq \min\Big(v(a_1), \ldots, \widehat{v(a_j)}, \ldots, v(a_n)\Big)$$

Since j was chosen so that $v(a_j)$ is minimal among $v(a_i)$, we also get

$$\min\Big(v(a_1), \ldots, \widehat{v(a_j)}, \ldots, v(a_n)\Big) \geq v(a_j)$$

Thus we get equality. Thus there is another index k so that $v(a_k) = v(a_j)$. □

4.3 Homework set 2

Proposition 4.3.1 (Exercise 1)**.** *There does not exist an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 with discriminant ± 1.*

Proof. Let $n = \deg f$, and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\mathbb{Q}^{\mathrm{al}}$. Let $K = \mathbb{Q}(\alpha_1)$. Since $\deg f > 1$ and f is irreducible, $K \neq \mathbb{Q}$. By Proposition 2.34 of Milne [**?**],

$$\mathrm{disc}(f) = D(1, \alpha, \ldots, \alpha^{n-1})$$

From Remark 2.25 of Milne [**?**], we have

$$D(1, \alpha, \ldots, \alpha^{n-1}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \Delta_K$$

Combining these, if $\mathrm{disc}(f) = \pm 1$, then

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \Delta_K = \pm 1$$

which implies $|\Delta_K| = 1$, since the other factor is an integer. Since $K \neq \mathbb{Q}$, by the Hermite-Minkowski theorem, $|\Delta_K| \neq 1$, so this is a contradiction. Thus $\mathrm{disc}(f) \neq \pm 1$. □

Remark 4.3.2. Let K be any field, and let $K(\alpha)$ be a Galois extension with primitive element α. Then for $\sigma \in \mathrm{Gal}(K(\alpha)/K)$, $\sigma\alpha$ is also a primitive element, that is, $K(\alpha) = K(\sigma\alpha)$. Viewing σ as an automorphism $K(\alpha) \to K(\alpha)$ note that the image is also $K(\sigma\alpha)$, so it must be that they are equal.

Proposition 4.3.3 (Exercise 3, repeat of Proposition 4.3.3)**.** *If $K/\mathbb{Q}$ is Galois, then K is either totally real or totally imaginary.*

Proof. Let K be the splitting field of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. If f has no real roots, then K is totally imaginary. By the previous remark, if any root of f is real, then it is a primitive element, so all other roots can be written in terms of it and elements of $\mathbb{Q}$, so all roots are real, and K is totally real. □