UC Berkeley Qualifying Exam

Anya Michaelsen, October 2021

Algebraic Number Theory Study Guide

Major topic: Algebraic Number Theory (Algebra)

References: Neukirch, *Algebraic Number Theory*, Ch I.1-10, II.1-8,
Cassels & Frohlich, *Algebraic Number Theory*, Ch VI, VII

- **Number Fields:** integrality, norm and trace, Dedekind domains, ideal factorization and class group, lattices and Minkowski bound, Dirichlet's unit theorem
- **Local Theory:** p-adic numbers, completions, valuations and absolute values, extensions of valuations, Hensel's lemma, local and global fields, ramification of extensions
- **Class Field Theory:** adeles and ideles, statements of local and global class field theory, statement of Artin reciprocity, statement of Chebotarev density

Additional References:

- Poonen's Summary of the Statements of CFT
- MIT Course Notes on Global CFT and Chebotarev Density Theorem
- Milne's Class Field Theory Notes

Contents

Memorization (– key terms –)

Chapter 1: Algebraic Integers

1.1 Preliminaries/Gaussian Integers

1 units, irreducible elements, prime elements, associated elements

units are invertible, irreducible cannot be written as a product of two non-units, primes $p \mid ab \implies p \mid a$ or $p \mid b$, associated elements differ by a unit

2 $F[\alpha] = F(\alpha)$ for field F and algebraic element α

$F[x]$ is Euclidean Domain, so if f is minimal polynomial for α, then for $g(a) \in F[a]$ with $\deg(g) < \deg(f)$ then $f(x)h(x) + g(x)k(x) = 1$ so then $g(a)k(a) = 1$ and so $g(a)$ has an inverse.

3 Euclidean domain, UFD

Euclidean Domain: There is a $\varphi : R - \{0\} \to \mathfrak{N}$ such that for any α, β, we can find q, r such that $\alpha = q\beta + r$ and either $r = 0$ or $\varphi(r) < \varphi(\beta)$

UFD (unique factorization domain) - every nonzero nonunit element has a unique factorization into prime (equiv to irreducible) elements

4 Noetherian, separable

Noetherian - ideals finiteily generated, ACC on ideals, nonempty collections of ideals have a maximal element,

separable - polynomials when no repeat roots, extensions when all elements have separable min polys

Note: all $K/\mathbb{Q}$ are separable, because repeat root means that $x - \alpha \mid f(x), f'(x)$ so min poly for α divides f' (so its degree is less than f) and divides f (so not irreducible!)

5 primitive element theorem

finite separable extensions are primitive, i.e. $L = K(\alpha)$ for some α.

In particular, all number fields (finite ext over $\mathbb{Q}$) are primitive!

6 structure theorem for finitely generated abelian groups

If G is a finitely generated (or just finite) abelian group then

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_m\mathbb{Z} \oplus \mathbb{Z}^k$$

where $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_m\mathbb{Z}$ is the torsion part and $\mathbb{Z}^k$ is the torsion free part, G has rank k. Can assume that $n_1 \mid n_2 \mid \cdots \mid n_m$.

7 structure theorem for modules over Dedekind Domains/PIDs

R a PID (or DD) and M a finitely generated R-module. Then there are nonzero ideals such that

$$M \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_m \oplus R^k$$

where R^k is the free part of the decomposition.

1.2 Integrality

8 algebraic number field, algebraic numbers and integers

algebraic number field = finite field extension K over $\mathbb{Q}$

algebraic numbers = elements of alg number field (i.e. roots of polynomials over $\mathbb{Q}$)

algebraic integers = zeros of *monic* polynomials over $\mathbb{Q}$

9 integral elements and extensions

setting $A \subset B$ extension of rings

integral element = $b \in B$ is integral over A if b is root of a monic equation degree $n \geq 1$

integral ring = B is integral over A is all elements of B are integral over A.

10 integrally closed/closure, normalization

integral closure of A in B: $\bar{A} = \{b \in B : b \text{ is integral over } A\}$ (is a ring)

A is integrally closed *in* B: $\bar{A} = A$ in B

normalization of A (A an integral domain): is the integral closure of A in its field of fractions

integrally closed (integral domain): A is integrally closed if it is integrally closed in its field of fractions

11 trace and norm

General formulation:

given L/K extension and $x \in L$, define the map $T_x : \alpha \mapsto x\alpha$ has some matrix representation in the K-vector space

Trace: $Tr_{L/K}(x) = Tr(T_x)$ and Norm $N_{L/K}(x) = \det(T_x)$

Galois formulation: (preferred definition)

L/K is separable (includes all number fields) and $\sigma : L \to \overline{K}$ varies of the K-embeddings of L,

$f_x(t) = \prod_\sigma (t - \sigma x)$ (characteristic poly, has coefficients in K)

Trace: $Tr_{L/K}(x) = \sum_\sigma \sigma x$

Norm: $N_{L/K}(x) = \prod_\sigma \sigma x$

12 basic properties of the trace and norm

$Tr : L \to K$ and $N : L^* \to K^*$

Trace is additive, norm is multiplicative

They stack: Given $K \subset L \subset M$, $Tr_{L/K} \circ Tr_{M/L} = Tr_{M/K}$ and similarly for norm (take galois view)

13 integral basis of a number field

an integral basis of B over A is a set $\omega_1, \ldots, \omega_n$ such that each $b \in B$ can be written *uniquely* as an A-linear combination of the ω_is.

integral basis of B over A makes B a **free A-module**

14 discriminant of a basis/number field

discriminant of a basis $\alpha_1, \ldots, \alpha_n$ of separable ext L/K with σ_i embeddings $L \to \overline{K}$:

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j))^2 = \det(Tr_{L/K}(\alpha_i \alpha_j))$$

discriminant of a number field:

Given $K/\mathbb{Q}$ with integral basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_K$ over $\mathbb{Z}$,

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \ldots, \omega_n)$$

15 $\mathcal{O}_K$, integral basis, and discriminant of $\mathbb{Q}(\sqrt{D})$, D square-free

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}] \\ \mathbb{Z}[\sqrt{D}] \end{cases} \qquad \{\alpha_1, \alpha_2\} = \begin{cases} \{1, \frac{1+\sqrt{D}}{2}\} \\ \{1, \sqrt{D}\} \end{cases} \qquad d_K = \begin{cases} D & D \equiv 1 \mod 4 \\ 4D & D \equiv 2,3 \mod 4 \end{cases}$$

Key example to recall:
$\frac{-1+\sqrt{-3}}{2}$ is a cube root of unity, hence minimal polynomial divides x^3-1 and is in $\mathcal{O}_K$ for $\mathbb{Q}(\sqrt{-3})$. Hence -3 has half integers and gives the $1 \mod 4$ condition.

1.3 Ideals

16 Dedekind domain

Noetherian, integrally closed domain where every (nonzero) prime ideal is maximal

17 ideal operations

$\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a}$

$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ =smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b})$

$\mathfrak{a} \cap \mathfrak{b} = \operatorname{lcm}(\mathfrak{a}, \mathfrak{b})$

$\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$

18 Chinese Remainder Theorem

Given ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ in a Dedekind domain $\mathcal{O}$, pairwise coprime ($\mathfrak{a}_i + \mathfrak{a}_j = \gcd(\mathfrak{a}_i, \mathfrak{a}_j) = (1) = \mathcal{O}$).

$$\mathfrak{a} := \cap \mathfrak{a}_i \qquad \mathcal{O}/\mathfrak{a} \cong \bigoplus_i \mathcal{O}/\mathfrak{a}_i$$

19 fractional ideals, integral ideals, and ideal inverses

fractional ideal is finitely generated $\mathcal{O}$-submodule of K (field of fractions) (i.e. gen'd by finitely many elements from K with coefficients in $\mathcal{O}_K$)

integral ideals of K are the usual ring ideals of $\mathcal{O}$

$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathcal{O}\}$ inverse ideal

fractional ideals are quotients of 2 integral ideals

20 ideal group, J_K

the abelian group of fractional ideals of K, with (1) identity and ideal inverses.

by unique factorization of fractional ideals (from integral ideals) J_K is freely generated by prime ideals.

21 ideal class group, Cl_K

P_K is the subgroup of fractional principal ideals

$Cl_K = J_K/P_K$

1.4 Lattices

22 lattice

subgroup of an n dimensional $\mathbb{R}$-vector space of the form $\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ with linearly independent v_i's in V.

23 complete lattice, fundamental region

a lattice is complete if it has the same dimension as the vector space it lives in, i.e. $|\{v_1, \ldots, v_m\}| = \dim V$.

fundamental region/mesh = coeffs in $[0, 1)$ = $\{x_1v_1 + \cdots x_mv_m \mid 0 \leq x_i < 1\} = \Phi$

24 discrete subgroup

a subgroup of a vector space is discrete if every point is isolated, i.e. has a neighborhood in V where it is the only point in the subgroup in that neighborhood.

subgroup = lattice $\iff$ subgroup is discrete

25 volume of a lattice

given a lattice spanned by $v_1, \ldots, v_n$

$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi) = |\det(\langle v_i, v_j\rangle)|^{1/2}$

Example : $\Gamma = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$

$$\mathrm{vol}(\Gamma) = \left|\det\begin{pmatrix}\langle 1,1\rangle & \langle 1,i\rangle \\ \langle i,1\rangle & \langle i,i\rangle\end{pmatrix}\right|^{1/2} = \left|\det\begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}\right|^{1/2} = |-1|^{1/2} = 1$$

26 centrally symmetric

defn: if $x \in X$ then $-x \in X$

examples and nonexamples :

examples: unit circle

$\{(x, y) \mid x \in [-1, 1]\}$ strip is centrally symmetric, $\{(x, y) \mid x \in [0, 1]\}$ off-center strip is not

27 convex subset

defn: if $x, y \in X$ then $(x + y)/2 \in X$ (their midpoint)

examples and nonexamples

example: unit circle, squares, rectangles, circles, triangles.

non-example: things that fold in on themselves or have gaps, like the union of two strips

28 Minkowski Lattice Point Theorem

Theorem Let Γ be a complete lattice in the Euclidean vector space X and X a centrally symmetric, convex, subset of V. Suppose

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma)$$

then X contains at least one nonzero lattice point $\gamma \in \Gamma$.

1.5 Minkowski Theory

29 Minkowski Space

$K/\mathbb{Q}$ number field, with n embeddings $\tau : K \hookrightarrow \mathbb{C}$

$K_{\mathbb{C}} = \prod_\tau \mathbb{C}$ (with $K \xrightarrow{j} K_{\mathbb{C}}$ by $\alpha \mapsto (\tau(\alpha))_\tau$)

Then complex conjugation acts on the indices $\tau \mapsto \overline{\tau}$ as well as the elements, call this F

$K_{\mathbb{R}} \subseteq K_{\mathbb{C}}$, **the Minkowski Space** is the fixed subspace under F

If ρ's are the r real embeddings and σ's are fixed representatives of the complex embedding pairs:

$$K_{\mathbb{R}} = \left\{ (z_\tau) \in \prod_\tau \mathbb{C} \mid z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z}_\sigma \right\}$$

$K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{\sigma,\text{ real}} \mathbb{R} \times \prod_{\tau,\text{ imag}} \mathbb{C} \cong \mathbb{R}^{r+2s}$ ($r =$ real embeddings, $2s =$complex embeddings)

30 volume of an ideal

$\mathfrak{a}$ lattice in $\mathcal{O}_K$ has volume $\sqrt{|d_k|}(\mathcal{O}_K : \mathfrak{a})$ where d_K is discriminant of the field and $(\mathcal{O}_K : \mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$

31 Minkowski Lattice Theorem for Ideals

If $\mathfrak{a} \neq 0$ is an integral ideal of $K/\mathbb{Q}$ and $c_\tau > 0$ for $\tau \in \mathrm{Hom}(K, \mathbb{C})$ be real numbers with $c_\tau = c_{\overline{\tau}}$ and

$$\prod_\tau c_\tau > (2/\pi)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}) \qquad (\approx\text{volume of } c_\tau \text{ rectangle } > 2^n \text{ vol of } \mathfrak{a} \text{ lattice })$$

then there exists some $a \in \mathfrak{a}$ ($a \neq 0$) such that

$$|\tau a| < c_\tau \quad \text{for all } \tau \in \mathrm{Hom}(K, \mathbb{C}) \qquad (\text{there exists a nontrivial pt in the lattice} \cap \text{rectangle })$$

Idea: Basically c_τ's form a rectangle (centally sym and convex) in $K_{\mathbb{R}}$ that intersects the lattice.

32 Minkowski Bound

Every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ has a nonzero element a with

$$|N_{K/\mathbb{Q}}(a)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

where s is the number of complex embedding pairs and d_K is discriminant of the field

1.6 The Class Number

33 absolute (ideal) norm

$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$ and when $\mathfrak{a} = (\alpha)$ then $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$ (hence the name 'norm')

34 basic properties of ideal absolute norm

multiplicative, so suffices to compute on prime ideals (shown by chinese remainder theorem on $\mathcal{O}_K/\mathfrak{a}$)
extend to fractional ideals to get homomorphism $\mathfrak{N} : J_K \to \mathbb{R}_+^*$ (postive reals with multiplication)

35 class number

$J_K =$ fractional ideals, and $P_K =$ principal fractional ideals, $Cl_K = J_K/P_K$
class number , $h_k = |Cl_K| = (J_K : P_K)$
class number is finite!

36 example number field with class number 1 (trivial class group, PID)

$\mathbb{Q}(\sqrt{-3})$ ($d_K = -3$)or $\mathbb{Q}(\sqrt{5})$ ($d_K = 5$) [both are $1 \mod 4$]
all ideals are principal

37 example number field with class number > 1, (nontrivial class group)

$K = \mathbb{Q}(\sqrt{-5})$ has class number 2 with the prime 2 ramifying as $\mathfrak{p}_2^2$ where $\mathfrak{p}$ is not principal (ramifies because divides $d_K = -20$ and not principal because no $a^2 + 5b^2 = 2$)

38 Minkowski Bound on Ideal Norms in Class Group

Every class $[\mathfrak{a}] \in Cl_K$ has an ideal with absolute norm

$$\mathfrak{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

in particular focus on powers of primes less than the bound.

39 Minkowski Lower Bound for Discriminant

$K/\mathbb{Q}$ with $[K:\mathbb{Q}] = n$ and s is the number of complex embedding *pairs*

$$\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \leq \sqrt{|d_K|}$$

1.7 Dirichlet's Unit Theorem

40 Dirichlet's Unit Theorem

$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}$ where $\mu(K)$ is the roots of unity in K (finite group) and r is the number of real embeddings, s is number of complex embeddings pairs.

41 fundamental units

The $r+s-1$ units in K that generate the unit group of $\mathcal{O}_K$.

42 Multiplicative Minkowski set up

Hyperplane in $\prod_\tau \mathbb{R}$ is the kernel of the trace map

$$\begin{tikzcd}
K^* \arrow[r, "j:a\mapsto(\tau a)_\tau"'] \arrow[d, "N_{K/\mathbb{Q}}"'] & K_\mathbb{C}^* = \prod_\tau \mathbb{C}^* \arrow[r, "\ell:(a_\tau)_\tau\mapsto(\log|a_\tau|)_\tau"'] \arrow[d, "N"] & \prod_\tau \mathbb{R} \arrow[d, "Tr"] \\
\mathbb{Q}^* \arrow[r] & \mathbb{C}^* \arrow[r, "\log|\cdot|"] & \mathbb{R}
\end{tikzcd}$$

1.8 Extensions of Dedekind Domains

43 Dedekind Kummer Theorem

Dedekind Kummer Theorem: *If $K = \mathbb{Q}(\alpha)$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$ (or general L/K) with $f(x)$ the minimal polynomial of α. Then however $f(x)$ factors mod p is how p splits in $\mathcal{O}_K$.*

Note: Generalizes when $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ as long as $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$

44 ramification index and inertia degree

Given L/K and $\mathcal{O}_L$ over $\mathcal{O}_K$ with $\mathfrak{p}$ a prime in $\mathcal{O}_L$ that splits as $\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$

e_i is the **ramification index** of $\mathfrak{q}_i$ and $f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$ is the **inertia degree.**

45 split (completey), ramified/unramified, inert

split - multiple primes lying over (completely - n distinct primes lying over)

ramified - at least one dividing prime divides to a power, unramified - all primes divide only once

inert - remains prime (maximal inertia degree)

46 State Quadratic Reciprocity.

Quadratc Reciprocity: Given two distinct odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}$$

Proof Idea:

Work in the field $\mathbb{Q}(\zeta_p)$ and look at quadratic gauss sums, use these to express a quantity in two ways, where equating gives the desired expression.

47 Legendre Symbol Formulas

For odd primes:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Also in general

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

1.9 Hilbert's Ramification Theory

48 Proof that $\mathrm{Gal}(L/K)$ acts transitively on the primes

If not,take $\mathfrak{p}$ a prime lying over $\mathfrak{q}$, and suppose $\mathfrak{p} \neq \sigma\mathfrak{p}'$ for all $\sigma \in \mathrm{Gal}(L/K)$ then by CRT choose $x \in \mathfrak{p}$ but not in $\sigma\mathfrak{p}'$ for all $\sigma \in \mathrm{Gal}(L/K)$ (hence $\sigma(x) \notin \mathfrak{p}'$ for all σ)

Taking norm of x, $N_{L/K}(x) = \prod_\sigma \sigma(x)$. Since $x \in \mathfrak{p}$ and $N(x) \in \mathcal{O}_K$, $x \in \mathfrak{p} \cap \mathcal{O}_K = \mathfrak{q}$.

But $\mathfrak{p}' \cap \mathcal{O}_K = \mathfrak{p} \cap \mathcal{O}_K = \mathfrak{q}$ and none of $\sigma(x) \in \mathfrak{p}'$ which is prime, contradiction!

49 ramification degree/inertia index in Galois extensions

since $\mathrm{Gal}(L/K)$ acts transitively on the primes, they have the same inertia index and ramification degrees, so $e_i = e$ and $f_i = f$ and $n = efr$ where r is the number of primes lying over $\mathfrak{p}$.

50 decomposition group

Given a prime $\mathfrak{p} \in \mathcal{O}_L$ and $G = \mathrm{Gal}(L/K)$,

$$G_\mathfrak{p} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

Properties: $|G_\mathfrak{p}| = ef$ and $G_{\sigma\mathfrak{p}} = \sigma G_\mathfrak{p} \sigma^{-1}$

51 inertia group

$I_\mathfrak{p} = \ker(G_\mathfrak{p} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{p})/(\mathcal{O}_K/\mathfrak{p}))$

$|I_\mathfrak{p}| = e$

52 decomposition and inertia subfields

L/K Galois extension, with L^D the decomposition subfield and L^I the inertia subfield

$$[L : L^I] = e \qquad [L^I : L^D] = f \qquad [L^D : K] = r$$

$K \to L^D$ the prime splits completely

$L^D \to L^I$ the prime is inert

$L^I \to L$ the prime is totally ramified

1.10 Cyclotomic Fields

53 (primitive) nth roots of unity

$\zeta_n = e^{2\pi i/n}$, a root of $x^n - 1$ that generates *all* other roots (i.e. isnt a root of some $f(x) \mid x^n - 1$)

54 cyclotomic polynomials

$$\boxed{\text{the min poly for } \zeta_n = e^{2\pi i/n}} \iff \boxed{f \mid x^n - 1 \ \& \ f \nmid x^d - 1 \ \forall d < n} \iff \boxed{\prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - e^{2\pi i k/n})}$$

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

When $n = p$ is prime, $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$

$\deg(\Phi_n(x)) = \varphi(n) = \#\{1 \le d \le n : \gcd(d, n) = 1\}$ Euler Totient Function

Special case: $\varphi(p^k) = p^{k-1}(p-1)$ and is multiplicative on relatively prime pieces.

55 ring of integers and Galois group of $\mathbb{Q}(\zeta_n)$

$\mathcal{O}_K = \mathbb{Z}[\zeta_n] \qquad \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

56 basic cyclotomic field facts

$\zeta_n = e^{2\pi i/n}$, a root of $x^n - 1$ that generates *all* other roots (i.e. isnt a root of some $f(x) \mid x^n - 1$)

$\mathcal{O}_K = \mathbb{Z}[\zeta_n] \qquad \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$\mathrm{Disc}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = p^\ell$ and more generally for ζ_n the discriminant is a product of primes in n.

Chapter 2: The Theory of Valuations

2.1 The p-adic Numbers

57 p-adic expansion for integers and rationals

for integers, $\sum_{k=0}^\infty a_k p^k$ for $a_k \in \mathbb{Z}/p\mathbb{Z}$ (can use finite sums for positive integers)

for fractions $1/h$ with $(h, p) = 1$ then $1 = hx + yp$ for some x, y so (up to adjusting to be in $[0, p-1]$)

$$\tfrac{1}{h} = x + \tfrac{1}{h}yp = x + (x + \tfrac{1}{h}yp)yp = x + xyp + xy^2\tfrac{1}{h}p^2 = x\sum_{k=0}^\infty (yp)^k$$

for a general fraction write as $\frac{g}{h}p^{-m}$ for $(g, p) = (h, p) = 1$ then get expansion of g/h and shift by p^-m.

58 p-adic integers, p-adic numbers

$\mathbb{Z}_p = \{\sum_{k=0}^\infty a_k p^k : a_k = 0, 1, 2, \ldots, p-1\}$

$\mathbb{Q}_p = \{\sum_{k=-m}^\infty a_k p^k : a_k = 0, 1, 2, \ldots, p-1\}$

59 $\mathbb{Z}_p$ as a projective limit (ring structure)

$\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ by truncation $\sum_{k=0}^\infty a_k p^k \mapsto \sum_{k=0}^{n-1} a_k p^k$

and $\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \cdots \leftarrow \mathbb{Z}/p^n\mathbb{Z} \leftarrow \cdots$

yields a projective limit $\lim_{\leftarrow k} \mathbb{Z}/p^k\mathbb{Z}$ with $\mathbb{Z}_p \xrightarrow{\sim} \lim_{\leftarrow k} \mathbb{Z}/p^k\mathbb{Z}$ by uniqueness of representations.

In $\mathbb{Z}_p$ multiplication is messy foiling of infinite sums, but in the limit multiplication is pointwise!

2.2 The p-adic Absolute Value

60 p-adic valuation and absolute value

$v_p(a) = v_p(p^m \frac{b}{c}) = m$ where $(bc, p) = 1$ $\qquad$ $|a|_p = \frac{1}{p^{v_p(a)}} = \frac{1}{p^m}$

61 product formula for $\mathbb{Q}$

For any $a \in \mathbb{Q}^*$ (nonzero) $\prod_p |a|_p = 1$ where $p = \infty, 2, 3, 5, 7, \ldots$ (all primes plus infinity)

2.3 Valuations

62 (multiplicative) valuation (properties and equivalence)

$|\cdot| : K \to \mathbb{R}$ satisfying

i $|x| \geq 0$ and $|x| = 0 \iff x = 0$

ii $|xy| = |x||y|$

iii $|x+y| \leq |x| + |y|$

Equivalent: $|\cdot|_1, |\cdot|_2$ give same topology ($d(x,y) = |x-y|$) $\iff$ $|x|_1 = |x|_2^s$ for some $s > 0$.

63 Approximation Theorem

Given $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ be pairwise inequivalent valuations on a field K
and $a_1, a_2, \ldots, a_n \in K$
Idea: We can approximate these arbitrarily well with respsect to each valuation
for all $\varepsilon > 0$ there exists some $x \in K$ such that $|x - a_i|_i < \varepsilon$ for all $i = 1, 2, \ldots, n$

64 nonarchimedean and archimedean valuations

nonarchimedean: $|n|$ is bounded for all $n \in \mathbb{Z}$
(should be bounded by 1, since $|1y| = |1||y|$ so $|1| = 1$ and $|n| = |1 + \cdots + 1| \leq \max\{|1|\} = 1$)
archimedean: $|n|$ is not bounded for all $n \in \mathbb{Z}$

65 strong triangle inequality

Normal Triangle Inequality: $|x+y| \leq |x| + |y|$
Strong Triangle Inequality: $|x+y| \leq \max\{|x|, |y|\}$
Consequence: $|x| \neq |y|$ then $|x+y| = \max\{|x|, |y|\}$
Valuation is nonarchimedean $\iff$ satisfies strong triangle inequality

66 Valuations on $\mathbb{Q}$

The only (nontrivial) valuations are $|\cdot|_p$ and $|\cdot|_\infty$.
Proof Sketch:
<u>Case:</u> Nonarchimedean (will yield $|\cdot|_p$)
$|n| \leq 1$ for all $n \in \mathbb{Z}$, and for some prime p, $|p| < 1$ (otherwise trivial valuation)
Then $p\mathbb{Z} \subset \{x \in \mathbb{Z} : |x| < 1\}$ but $p\mathbb{Z}$ maximal, so equality holds.
$|a| = |p^m b| = |p^m||b| = |p|^m = |a|_p^s$ for some s.
<u>Case:</u> Archimedean (will yield $|\cdot|_\infty$)

Claim $|m|^{1/\log(m)} = |n|^{1/\log(n)}$ for all $n, m > 1$.
So $C = |n|^{1/\log(n)} = e^s$ implies $|n| = C^{\log(n)} = e^{s\log(n)} = |n|_\infty^s$ and extend to all positive rationals.

67 exponential (additive) valuations (properties and equivalence)

$v : K \to \mathbb{R} \cup \{\infty\}$ such that

i $v(x) = \infty \iff x = 0$

ii $v(xy) = v(x) + v(y)$ (is additive)

iii $v(x + y) \geq \min\{v(x), v(y)\}$

two valuations are equivalent if there is some $s > 0$ such that $v(x) = su(x)$ for all x.

68 relationship between additive/multiplicative valuations

$v(x) \implies |x| = q^{-v(x)}$ for some $q > 1$
$|x| \implies v(x) = -\log|x|$

69 valuation ring

$\mathcal{O}$ in K is valuation ring if for all $x \in K$ either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$
maximal ideal is $\{x \in \mathcal{O} : x^{-1} \notin \mathcal{O}\}$

70 discrete valuation, normalized valuation

discrete if there is a smallest positive value s, that is $v(K^*) = s\mathbb{Z}$. normalized if $s = 1$

71 prime elements (w.r.t. normalized additive valuation)

if $v(K^*) = \mathbb{Z}$ then $\pi \in \mathcal{O} = \{x \in K : v(x) \geq 0\}$ is prime if $v(\pi) = 1$

72 principal units and nth higher unit groups

$U^{(1)} = 1 + \mathfrak{p}$ are the principal units, $U^{(n)} = 1 + \mathfrak{p}^n$ nth higher unit group
$U^{(n+1)}/U^{(n)} \cong \mathcal{O}/\mathfrak{p}$.

2.4 Completions

73 complete valued field

$(K, |\ |)$ complete if every cauchy sequence (with respect to $d(x, y) = |x - y|$) converges to an element in K.

74 completion w.r.t. a valuation

Given K with valuation $|\ |$, take R to be the ring of cauchy sequences in K with respect to $|\ |$, and the maximal ideal $\mathfrak{m}$ of nullsequences (converges to 0) then $\widehat{K} = R/\mathfrak{m}$
$K \to \widehat{K}$ by $a \mapsto (a, a, a, \ldots)$
extend the valuation $|\ |$ to $\widehat{K}$ by defining $|(x_n)| = \lim_{n\to\infty} |x_n|$.
completions are unique (up to isomorphism)

75 Ostrowski's Theorem

The only complete fields with respect to archimedean valuations are $\mathbb{R}$ and $\mathbb{C}$ (up to isomorphism)

76 Hensel's Lemma

Hensel's Lemma *If $f \in \mathbb{Z}_p[x]$ with some $a_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(a_0) \equiv 0 \mod p$ but $f'(a_0) \neq 0 \mod p$ then there is a lift $\alpha \in \mathbb{Z}_p$ of a_0 such that $f(\alpha) = 0$.*

Generalizations

Hensel's Lemma V2 *If $f \in \mathbb{Z}_p[x]$ with some $a_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $|f(a_0)|_p < |f'(a_0)|_p^2$ then there is a lift $\alpha \in \mathbb{Z}_p$ of a_0 such that $f(\alpha) = 0$.*

Hensel's Lemma V3 *If $f \in \mathbb{Z}_p[x]$ (with $f \not\equiv 0 \mod p$) with $\bar{f} = \bar{g}\bar{h} \mod p$, for relatively prime polynomials $\bar{g}, \bar{h}$ then there is a degree preserving lift $g = \bar{g} \mod p$ and $h = \bar{h} \mod p$ such that $f = gh$.*

77 extension of valuation of complete field

If K is complete w.r.t. $|\ |$ and L/K a finite algebraic extension, then $|\ |$ extends uniquely to a valuation on L and L is complete.

$$|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|_K}$$

2.5 Local Fields

78 multiplicative group decomposition K^*

Given $\mathbb{Q}_p$ we have the multiplicative group

$$\mathbb{Q}_p^* = (p) \times \mu_{p-1} \times (1 + (p)) \cong \mathbb{Z} \oplus \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}$$

where $(p) = \{p^k : k \in \mathbb{Z}\}$ and $(1 + (p))$ are the principal units. More generally $K/\mathbb{Q}_p$

$$K^* = (\pi) \times \mu_{q-1} \times (1 + (\pi)) \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$$

where π is a prime element ($v(\pi) = 1$) and q is the number of elements in the residue field ($q = p^f$)

2.7 Unramified and Tamely Ramified Extensions

79 unramified extension

ramification of the unique prime ideal is 1

$[L : K] = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$ (can be expressed in terms of decom and inertia subgroups to show that $|I_\mathfrak{p}| = e = 1$)

80 maximal unramified subextension

composite of all unramified subextenstions (composite of unramified extensions is again unramified)

81 tamely ramified extension

the ramification index is coprime to p, the size of the residue field

82 maximal tamely ramified subextension

composite of all tamely ramified subextenstions (composite of tamely ramified extensions is again tamely ramified)

2.8 Extensions of Valuations

83 extensions of valuations

L/K with valuation v on K, w is an extension of v if $w(\alpha) = v(\alpha)$ for all $\alpha \in K$.

each embedding $\tau : L \to \overline{K_v}$ gives a valuation by $w = v \circ \tau$ that is $|x|_w = |\tau x|_v$.

These valuations are the same for τ and τ' if there is an automorphism $\sigma : \overline{K_v} \to \overline{K_v}$ taking τ to τ'.

84 valuation extensions from minimal polynomial

If $L = K(\alpha)$ where α has minimal polynomial $f \in K[x]$ then extension w_i of v correspond to irreducible factors of f in K_v (e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$)

85 fundamental identity for valuations

$[L : K] = \sum_{w|v} [L_w : K_v]$ where $w \mid v$ ranges over all valuations w extending v.

For $K_v = \mathbb{Q}_p$ (v is discrete), $[L : K] = \sum_{w|v} e_w f_w$ with $e_w = (w(L^*) : v(K^*))$ and $f_w = [\lambda_w : \kappa]$

86 tame inertia

tame inertia is cyclic, that is when $p \nmid |I_\mathfrak{q}|$ in extension $K/\mathbb{Q}_p$, then $I_\mathfrak{q}$ is cyclic with order e.

Class Field Theory

87 Local Class Field Theory Statements

Let K be a local field. Then there is a local artin map ϕ_K that is a continuous surjection (K^* with topology induced by valuation and $\mathrm{Gal}(\cdot/\cdot)$ with Krull topology)

$$K^* \xrightarrow{\phi_K} \mathrm{Gal}(K^{ab}/K)$$

where K^{ab} is the maximal abelian extension of K. For any finite abelian extension L/K, the quotient map $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$ composes to get a surjective map $\phi_{L/K} : K^* \to \mathrm{Gal}(L/K)$. If L/K is unramified and π is any uniformizer for K, then $\phi_{L/K}(\pi) = \mathrm{Frob}_p \in \mathrm{Gal}(L/K)$. Furthermore, the kernel of $\phi_{L/K}$ is $N_{L/K}(L^*)$ and this is inclusion reversing by Galois theory.

As a consequence, ϕ_K induces an isomorphism when passed to the profinite completion. Furthermore, $\phi_{L/K}(\mathcal{O}_K^*)$ gives the inertia subgroup of $\mathrm{Gal}(L/K)$.

88 Global Class Field Theory Statements

Let K be a global field. Let C_K be the idele class group (I_K/K^* where I_K are the ideles, the unit group of the adeles).

Then there is a global artin map ϕ_K that is a continuous surjection (C_K with ideles topology and $\mathrm{Gal}(\cdot/\cdot)$ with Krull topology)

$$C_K \xrightarrow{\phi_K} \mathrm{Gal}(K^{ab}/K)$$

where K^{ab} is the maximal abelian extension of K. This again induces an isomoprhism on the profinite completions.

For any finite abelian extension L/K, the quotient map $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$ composes to get a surjective map $\phi_{L/K} : C_K \to \mathrm{Gal}(L/K)$, which has kernel $N_{L/K}(C_L)$.

f L/K is unramified and π is any uniformizer for K, then $\phi_{L/K}(1, \ldots, 1, \pi, 1, \ldots) = \mathrm{Frob}_p \in \mathrm{Gal}(L/K)$.

Furthermore, $\phi_{L/K}(\mathcal{O}_\mathfrak{p}^*)$ gives the inertia subgroup for the ideal $\mathfrak{p}$ of K in $\mathrm{Gal}(L/K)$.

89 Conductor

The **conductor** is defined for local fields as p^n for the smallest n such that the local artin map ϕ_Q is trivial on $1 + p^n\mathbb{Z}_p$. The global conductor is the product of the local ones. If p is unramified, then $n = 0$ so this is a finite product of the primes that ramify.

90 Hilbert Class Field

The **Hilbert Class Field** is the maximal unramified abelian extension of K, and if we denote it by H, we have $Cl_K \cong \mathrm{Gal}(H/K)$ where the left hand side is the *ideal* class group.

91 Artin Reciprocity

Artin Reciprocity Statement: Let $K/\mathbb{Q}$ be an abelian extension. The primes of $\mathbb{Q}$ the split completely in K are determined by a congruence condition modulo the conductor $\mathfrak{f}_{K/\mathbb{Q}}$.

92 Adeles and Ideles

Let $K/\mathbb{Q}$ be a number field. Then **adeles** are $\mathbb{A}_K = \prod'_\nu K_\nu$ where ν ranges over all valuations of K, K_ν is the completion of K with respect to the valuation ν, and the $\prod'$ indicates a restricted product, meaning if $(\alpha_\nu) \in \mathbb{A}_K$ then for all but finitely many ν, $\alpha_\nu \in \mathcal{O}_\nu^*$ (i.e. lies in the valuation ring).

The **ideles** are the units within the adeles, i.e. $\mathbb{I}_K = \mathbb{A}_K^* = \prod'_\nu K_\nu^*$.

93 Idele Class Group

For each valuation ν, there is an embedding $K \hookrightarrow K_\nu$ so combining these maps we have $K^* \hookrightarrow \mathbb{I}_K$. Quotienting by the image of this injection we define the **idele class group** $C_K = \mathbb{I}_K/K^*$.

Algebraic Number Theory Quals Questions (– best questions –)

Chapter 1 - Algebraic Integers

1.1 Gaussian Integers

1 Show that the units of $\mathbb{Z}[i]$ are precisely those with $N(\alpha) = 1$

$\alpha = a + bi$ and unit means that $\alpha\beta = 1$ for some β. Norms are multiplicative, so $N(\alpha)N(\beta) = N(1) = 1$.

$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. So $N(Z[i]) \subseteq \mathbb{Z}+$ and only units are 1.

If $N(\alpha) = 1$ then $\alpha = a + bi$ and $N(\alpha) = a^2 + b^2 = 1$. The only solutions to this are $\alpha = \pm 1, \pm i$ all of which are units.

2 Compute the units of $\mathbb{Z}[\sqrt{-d}]$ for any integer $d > 1$.

$\alpha = a + b\sqrt{-d}$ and $N(\alpha) = a^2 + db^2$. Since this is always a positive integer, the only units are those with norm 1. Since $d > 1$, if $b^2 \neq 0$ this cannot happen, so $b = 0$ and $a^2 = 1$, i.e. $\alpha = a = \pm 1$.

3 Show that $\mathbb{Z}[i]$ is a UFD

Show that it is Euclidean by considering the Gaussian integers as a lattice.

Given $\alpha, \beta \in \mathbb{Z}[i]$, want to find γ, ρ such that $\alpha = \gamma\beta + \rho$ and $|\rho| < |\beta|$.

Divide through by β, we have α/β in $\mathbb{C}$ and want $\gamma + \rho/\beta$ with $|\rho/\beta| < 1$.

Sufficient that every point in $\mathbb{C}$ is less than 1 from some point in the $\mathbb{Z}[i]$ lattice. Picking the absolute center of one of these lattice regions, the distance will be $\sqrt{1/2} < 1$. And Euclidean implies UFD.

4 Determine the prime elements of $\mathbb{Z}[i]$

$\mathbb{Z}[i]$ is a UFD, so primes are exactly the irreducible elements

Given a prime π, $\pi \mid N(\pi) = p_1 \cdots p_r$ so π divides some p_i since π is prime. Then $\pi \cdot \gamma = p$ so $N(\pi) \mid N(p) = p^2$, hence $N(\pi) = p, p^2$.

we can split this into 3 cases: $p = 2$, $p \equiv 1, 3 \bmod 4$.

$p = 2$. [$\alpha = 1 + i$ or associates]

Here we have $\alpha \mid 2$ so $N(\alpha) \mid 2^2 = 4$. The solutions here are $\pm 1 \pm i$ (which are all the same up to associates, so represent by $1 + i$). Then $N(1 + i) = 1 + 1 = 2 = p$. If $1 + i = \beta\gamma$ then $N(\beta)N(\gamma) = 2$ so one of these has norm 1 and is a unit.

$p \equiv 1 \bmod 4$. [$\alpha = a + bi$ with $a^2 + b^2 = p$ or associates]

Well $p \equiv 1 \bmod 4 \iff p = a^2 + b^2$ for integers a, b. If $\alpha \mid p$ then $N(\alpha) = p, p^2$. If $N(\alpha) = p^2$ then α is associate of p. However if $N(\alpha) = p$ then $\alpha = a + bi$ (or some associate). This divides assoicates of p so these are the only primes in this category.

$p \equiv 3 \bmod 4$. [$\alpha = p$ or associates]

Well $p \equiv 1 \bmod 4 \iff p = a^2 + b^2$ for integers a, b, so there are no $\alpha = a + bi$ with $N(\alpha) = a^2 + b^2 = p$. If $\alpha \mid p$ then $N(\alpha) = p, p^2$. No α with $N(\alpha) = p$, so only α are those with $N(\alpha) = p^2$ which are associates of p.

1.2 Integrality

5 Show that every UFD is integrally closed.

UFD = unique factorization domain

integrally closed = every element of the fraction field that satisfies a monic polynomial lies in the ring

Let R be UFD and $\alpha \in \mathrm{Frac}(R)$ (i.e. $\alpha = r/s$ for $r, s \in R$) satisfying some monic polynomial

$$\alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_1\alpha + r_0 = 0$$

with $r_i \in R$. Since we have unique factorization, we may assume no prime element $p \mid r, s$.

Rewriting α in terms of r and s and clearing denominators,

$$r^n + r_{n-1}r^{n-1}s + \cdots r_1 r s^{n-1} + r_0 s^n = 0$$

We can rearrange to get

$$r^n = -s(r_{n-1}r^{n-1} + \cdots r_1 r s^{n-2} + r_0 s^{n-1})$$

so some prime factor of s divides r^n and thus divides r, a contradiction unless s is actually a unit in which case $\alpha \in R$ as desired.

6 Is $\mathbb{Z}[\sqrt{29}]$ a PID?

$K = \mathbb{Q}(\sqrt{29})$, since $29 \equiv 1 \mod 4$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{29}}{2}]$

PID $\implies$ UFD $\implies$ integrally closed so suffices to show this is not integrally closed.

Take $\frac{1+\sqrt{29}}{2} \in \mathcal{O}_K$ but not in $Z[\sqrt{29}]$ but is integral over it, hence not a PID.

7 What are some properties of integral elements/extensions?

finitely many elements $b_1, \ldots, b_n$ are inegral over $A \iff A[b_1, \ldots, b_n]$ is a finitely generated A-module.

$\implies$ Sums and products of integral elements are integral

$\implies$ Integral extensions stack. If $A \subseteq B$ is integral, and $B \subseteq C$ is too, then $A \subseteq C$ is also.

8 Find an integral basis for the quadratic field $\mathbb{Q}(\sqrt{D})$ where D is a square-free integer ($D \neq 0, 1$). Use these to compute the discriminant.

Integral Basis

$K = \mathbb{Q}(\sqrt{D})$ has elements of the form $q + r\sqrt{D}$ with $q, r \in \mathbb{Q}$. To compute integral basis, we want elements of ring of integers that generate $\mathcal{O}_K$ over $\mathbb{Z}$.

Ring of Integers: $D \equiv 1 \bmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$ and $D \equiv 2, 3 \bmod 4$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$

Want $q + r\sqrt{D}$ satisfying monic polynomial in $\mathbb{Z}$. Well the minimal polynomial for $q + r\sqrt{D}$ is

$$(x - (q + r\sqrt{D}))(x - (q - r\sqrt{D})) = x^2 - 2qx + (q^2 - r^2 D)$$

this is in $\mathbb{Z}[x]$ exactly when $2q, q^2 - r^2 D \in \mathbb{Z}$.

[show that this implies that $q, r \in \mathbb{Z}$]

$2q \in \mathbb{Z} \implies q \in \frac{1}{2}\mathbb{Z}$ $(4q^2 \in \mathbb{Z})$

$4q^2 - 4r^2 D \in \mathbb{Z} \implies 4r^2 D = (2r)^2 D \in Z \implies r \in \frac{1}{2}\mathbb{Z}$ (D square-free)

$\implies \frac{(2q)^2 - (2r)^2 D}{4} \in \mathbb{Z}$,so $(2q)^2 - (2r)^2 D \equiv 0 \mod 4$, cases by D

$D \equiv 1 \mod 4$: $\{0, 1\} - \{0, 1\} = 0 \implies 2q \equiv 2r \equiv 0, 1$ so could have q, r both odd half integers

$D \equiv 2, 3 \mod 4$: $\{0, 1\} - \{2, 3\}\{0, 1\} = 0 \implies 2q = 2r = 0$ so $q, r \in \mathbb{Z}$.

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \\ \mathbb{Z}[\sqrt{D}] & D \equiv 2,3 \mod 4 \end{cases}$$

Based on our formulation of the ring of integers, we have integral bases

$$\begin{cases} \{1, \frac{1+\sqrt{D}}{2}\} & D \equiv 1 \mod 4 \\ \{1, \sqrt{D}\} & D \equiv 2,3 \mod 4 \end{cases}$$

Discriminant:

Computing discriminant of each of these. Embeddings $\sqrt{D} \mapsto \pm\sqrt{D}$.

$D \equiv 1 \mod 4$

$$\det \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}^2 = (\tfrac{1-\sqrt{D}}{2} - \tfrac{1+\sqrt{D}}{2})^2 = D$$

$D \equiv 2,3 \mod 4$

$$\det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^2 = (-\sqrt{D} - \sqrt{D})^2 = 4D$$

9 When can we garuantee an integral basis exists? What are cases where it does not?

If L/K is separable and A is a PID (e.g. $\mathbb{Z} \subseteq \mathbb{Q}$ and $K/\mathbb{Q}$ algebraic number field)

When taking extensions of number fields $L/K/\mathbb{Q}$ we may not have that $\mathcal{O}_K$ is a PID so there may not be an integral basis for $\mathcal{O}_L$ over $\mathcal{O}_K$.

Examples: $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is not a PID $I = (2, 1+\sqrt{-5})$ so there should be some ring of integers over $\mathcal{O}_K$ that is not a free $\mathcal{O}_K$ module and hence does not have an integral basis.

10 How is the discriminant defined when $\mathcal{O}_L$ is not a free $\mathcal{O}_K$ module (no integral basis)?

When in a case where there is no integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$ (i.e. $\mathcal{O}_L$ is not a free $\mathcal{O}_K$ module), define the discriminant using ideals.

Let $n = [L : K] = [\mathcal{O}_L : \mathcal{O}_K]$ be the degree of the extension. Take all collections of $\omega_1, \dots, \omega_n$ and define the discriminant to be the ideal generated by the discriminants of all of these element collections.

How to compute?

Well given any $\alpha_1, \dots, \alpha_n$ we know that $(\mathrm{disc}(\alpha_i)) \subset \mathrm{Disc}\, L/K$ so $\mathrm{Disc}\, L/K \mid (\mathrm{disc}(\alpha_i)) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$.

Case: square-free factorization ($e_i = 1$).

A prime divides the discriminant $\iff$ it ramifies, so check each $\mathfrak{p}_i$ for ramification in L/K and take only the ramified ones to form the $\mathrm{Disc}\, L/K$.

General:

Localize at each prime, where $\mathcal{O}_{K,\mathfrak{p}}$ is now a PID (becasue it is a DVR) so we can compute the discriminant in the usual manner and determine the power of the prime that divides $\mathrm{Disc}\, L/K$.

11 Let $K = \mathbb{Q}(\sqrt{-5})$, find $\mathcal{O}_K$ and d_K.

Short way: $D = -5 \equiv -1 \equiv 3 \mod 4$ so then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $d = 4D = -20$.

Direct Computation:

Ring of integers are $q + r\sqrt{-5}$ with minimal polynomial in $\mathbb{Z}[x]$.

Minimal polynomial will be $(x - (q + r\sqrt{-5}))(x - (q - r\sqrt{-5})) = x^2 - 2qx + q^2 + 5r^2$

so then $2q, q^2 + 5r^2 \in \mathbb{Z} \implies q = a/2$ for $a \in \mathbb{Z}$ and $4q^2 + 20r^2 \in \mathbb{Z} \implies 20r^2 \in \mathbb{Z}$ so $r = b/2$ (cannot have 5 in denominator) for $b \in \mathbb{Z}$.

$q^2 + 5r^2 = \frac{a^2}{4} + 5\frac{b^2}{4} = \frac{a^2+5b^2}{4} \in \mathbb{Z} \implies a^2 + 5b^2 \equiv a^2 + b^2 \equiv 0 \mod 4$ so $a \equiv b \equiv 0 \mod 2$

hence $q, r \in \mathbb{Z}$ and so ring of integers is $\mathbb{Z}[\sqrt{-5}]$.

Taking an integral basis of $\{1, \sqrt{-5}\}$ we have

$$d_K = \det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}^2 = (-\sqrt{-5} - \sqrt{-5})^2 = (-2\sqrt{-5})^2 = 4 \cdot -5 = -20$$

12 Show that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is an integral basis for $K = \mathbb{Q}(\sqrt[3]{2})$.

First show that these all lie in the ring of integers.

well they satisfy the monic polynomials $x-1, x^3-2, x^3-4$ so all on $\mathcal{O}_K$.

Since $[K : \mathbb{Q}] = 3$, suffices to show that these are linearly independent over $\mathbb{Z}$

Well if not, then $n + m\sqrt[3]{2} + \ell\sqrt[3]{2}^2 = 0$ for some $n, m, \ell \in \mathbb{Z}$. This would provide a minimal polynomial for $\sqrt[3]{2}$ of degree ≤ 2, a contradiction because its minimal polynomial is $x^3 - 2$ (irreducible by Eisenstein's criterion)

13 The ring of integers $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module, how would you show this?

The map $(x, y) \mapsto Tr(xy)$ is a bilinear non-degenerate pairing.

[bilinear $= Tr((ax + b)y) = aTr(xy) + bTr(y)$, nondegenerate $= \forall y, Tr(xy) = 0 \implies x = 0$]

Nondegenerate bilinear pairings give dual bases. So let $\alpha_1, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$ (guaranteed by $\mathbb{Z}$ PID, or take any basis and scale to be in $\mathcal{O}_K$.). Generate a dual basis $\alpha_1', \ldots, \alpha_n' \in \mathcal{O}_K$ of $K/\mathbb{Q}$ using the pairing (i.e. $Tr(\alpha_i \alpha_j') = \delta_{ij}$).

Then let $\beta \in \mathcal{O}_K$ so we can write $\beta = q_1\alpha_1' + \cdots q_n\alpha_n'$ with $q_i \in \mathbb{Q}$. Take $Tr(\beta\alpha_i) \in \mathbb{Z}$ since the trace maps $\mathcal{O}_K \to \mathbb{Z}$. But also $Tr(\beta\alpha_i) = Tr(q_i\alpha_i'\alpha_i) = q_i \in \mathbb{Z}$ so $\beta \in \mathbb{Z}\alpha_1' + \cdots + \mathbb{Z}\alpha_n'$ and $\mathcal{O}_K$ has a basis over $\mathbb{Z}$ making it a $\mathbb{Z}$ module of the same dimension as $K/\mathbb{Q}$.

14 Let $f(x) = x^3 - x^2 - 2x + 1$. Show that f is irreducible over $\mathbb{Q}$. Then let $K = \mathbb{Q}[x]/f$ and show that K is abelian (Hint: discriminant of f is 49).

f is irreducible: f monic so Gauss's Lemma says irreducible if and only if irreducible over $\mathbb{Z}$. Since cubic, reducible implies a linear factor (root). But a root has to divide the constant term $+1$ so is only ± 1, both of which can be checked computationally and are not roots.

K is abelian. The discriminant of a polynomial is $\prod_{i \neq j}(\alpha_i - \alpha_j)^2$ where the α_i's range over all roots of f. Since $\mathrm{Disc}(f) = 49 = 7^2$ we have that $\prod_{i \neq j}(\alpha_i - \alpha_j) = 7 \in \mathbb{Z}$ so this is fixed by all permutations of the roots in the Galois group. Since $\deg(f) = 3$, we know that $\mathrm{Gal}(f) \subseteq S_3$. Applying a permutation to $\prod_{i \neq j}(\alpha_i - \alpha_j)$ permutes the order of the product and multiplies by the sign of the permutation. Since this is fixed, all permutations in the Galois group must be even, so $\mathrm{Gal}(f) = A_3 = \mathbb{Z}/3\mathbb{Z}$. Since K is a nontrivial (deg 3) subextension of the splitting field for f, which has Galois group $\mathbb{Z}/3\mathbb{Z}$ we see that K is actually the splitting field and has the Galois group $\mathbb{Z}/3\mathbb{Z}$ so is abelian.

1.3 Ideals

15 Give an example of a ring of integers without unique factorization.

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ (ring of integers for $\mathbb{Q}(\sqrt{-5})$ because $-5 \equiv 3 \mod 4$)

$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two distinct factorizations into irreducibles.

Claim: all factors are irreducible. $N(2) = 4$, $N(3) = 9$, $N(1 \pm \sqrt{-5}) = 6$. Would need an element with $N(\alpha) = 2, 3$ to divide any of these non-trivially.

$N(\alpha) = N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2, 3$

has no integer solutions. And we see from norms that none of these irreducibles divide each other (are associates)

16 Sketch of unique factorization for ideals in a Dedekind Domain

start with integral ideals (i.e. not fractional)

Existence: take collection of those without prime factorization, noetherian gives a maximal element, contained in some $\mathfrak{p}$ (maximal prime). Multiplying by inverse gives a factorization of $\mathfrak{a}\mathfrak{p}^{-1}$ which gives a factorization of $\mathfrak{a}$.

Uniqueness: Primes in each factorization divide each other, but all are maximal giving equality.

This extends to fractional ideals, which have the form $\mathfrak{a}/\mathfrak{b}$ for integral ideals $\mathfrak{a}, \mathfrak{b}$

17 Show that $18 = 2 \cdot 3 \cdot 3 = (1+\sqrt{-17})(1-\sqrt{-17})$ are two different decompositions into irreducibles in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-17})$.

Norms are 4,9, 18, so to have divisors need norms of 2,3,6,9.

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$ because $-17 \equiv -1 \equiv 3 \mod 4$.

$N(a+b\sqrt{-17}) = a^2 + 17b^2$.

No integer solutions for 2,3,6 but for 9, $N(\pm 3) = 9$ is the only solution. But this does not divide because $3(a+b\sqrt{-17}) = 1 \pm \sqrt{-17}$ means that a, b are not integers, contradiction.

So these are all irreducibles forming distinct factorizations of 18.

18 Decompose $33 + 11\sqrt{-7}$ into integral irreducibles in $\mathbb{Q}(\sqrt{-7})$.

Well $-7 \equiv 1 \mod 4$ so the ring of integers will be $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

Well first we can factor out 11, so $33 + 11\sqrt{-7} = 11 \cdot (3+\sqrt{-7})$.

Is 11 irreducible? Well if not the some $a + b\sqrt{-7}$ (or $\frac{a+b\sqrt{-7}}{2}$) has norm 11, so $a^2 + 7b^2 = 11$ which has solutions when $a = \pm 2$ and $b = \pm 1$ so we have $11 = (2+\sqrt{-7})(2-\sqrt{-7})$. These elements have prime norm so must be irreducible. Can't divide by 2 because the coefficients don't have the same parity.

Is $3+\sqrt{-7}$ irreducible? Well $N(3+\sqrt{-7}) = 9 + 7 = 16$ so could be divisible by an element with norm $2, 4, 8$. This is because we can divide out by 2 since 3,1 have the same parity, so $3 + \sqrt{-7} = \frac{3+\sqrt{-7}}{2} \cdot 2$.

Are these irreducible?? Well $\frac{3+\sqrt{-7}}{2}$ has norm 4 (16/4). So any divisors have norm 2... $\frac{1}{4}(a^2 + 7b^2) = 2$ has solutions $a = \pm 1$ and $b = \pm 1$. Trying different combinations...

$$\frac{1+\sqrt{-7}}{2}\frac{1+\sqrt{-7}}{2} = \frac{1-7+2\sqrt{-7}}{4} = \frac{-3+1\sqrt{-7}}{2} \qquad \frac{1-\sqrt{-7}}{2}\frac{1-\sqrt{-7}}{2} = \frac{1-7-2\sqrt{-7}}{4} = \frac{-3-1\sqrt{-7}}{2}$$

$$\frac{1-\sqrt{-7}}{2}\frac{-1+\sqrt{-7}}{2} = \frac{-1+7+2\sqrt{-7}}{4} = \frac{3+\sqrt{-7}}{2}$$

$$\frac{1+\sqrt{-7}}{2}\frac{1-\sqrt{-7}}{2} = \frac{1+7+0\sqrt{-7}}{4} = 2$$

So far:

$$33 + 11\sqrt{-7} = (2+\sqrt{-7})(2-\sqrt{-7})(\tfrac{1-\sqrt{-7}}{2})(\tfrac{-1+\sqrt{-7}}{2})(\tfrac{1+\sqrt{-7}}{2})(\tfrac{1-\sqrt{-7}}{2})$$

Check that these are all irreducible:

Norms: 11, 2. Both are prime so cannot be split into non associate decomposition.

19 In $\mathbb{Z}[\sqrt{-3}]$ let $\mathfrak{a} = (2, 1+\sqrt{-3})$. Show that $\mathfrak{a} \neq (2)$, but $a^2 = 2\mathfrak{a}$. Conclude that ideals in $\mathbb{Z}[\sqrt{-3}]$ do not factor uniquely into prime ideals.

Claim 1: $\mathfrak{a} \neq (2)$

Since $(2) \subseteq \mathfrak{a}$ STP that $1+\sqrt{-3} \notin (2)$. Which is true because no integers satisfy $2c = 1$.
Claim 2: $\mathfrak{a}^2 = (2)\mathfrak{a}$
$\mathfrak{a}^2 = (4, 2+2\sqrt{-3}, -2+2\sqrt{-3})$ $\qquad 2\mathfrak{a} = (2)\mathfrak{a} = (4, 2+2\sqrt{-3})$
STP that $-2+2\sqrt{-3} \in 2\mathfrak{a}$, and $-2+2\sqrt{-3} = 2(-1+1\sqrt{-3}) = 2(1+1\sqrt{-3}-2) \in 2\mathfrak{a}$
Claim 3: $\mathbb{Z}[\sqrt{-3}]$ does not have unique factorization of ideals.
If we had unique factorization of ideals, then expressing that factorization for $\mathfrak{a}^2 = 2\mathfrak{a}$, we would be able to cancel all the primes of $\mathfrak{a}$ to get $\mathfrak{a} = (2)$ which is a contradiction.

Note: This is okay because $\mathbb{Z}[\sqrt{-3}]$ is *not* the ring of integers of $\mathbb{Q}(\sqrt{-3})$ (which is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$)

20 Given a number field K, what dedekind domains are contained in $\mathcal{O}_K$? What other dedekind domains (not necessarily inside $\mathcal{O}_K$) can be constructed out of $\mathcal{O}_K$?

For any number field $L/\mathbb{Q}$, since $\mathbb{Z}$ is a dedekind domain and integral closures of dedekind domains are also, $\mathcal{O}_L$ is a dedekind domain. So for K and any subextensions $K/L/\mathbb{Q}$, $\mathcal{O}_K$ and $\mathcal{O}_L$ are dedekind domains inside $\mathcal{O}_K$. In fact these will be the only ones, because any other dedekind domain $R \subseteq \mathcal{O}_K$ will have field of fractions $\mathrm{Frac}(R) \subseteq \mathrm{Frac}(\mathcal{O}_K) = K$ so will be the ring of integers of the subextension $\mathrm{Frac}(R)/\mathbb{Q}$.

For more dedekind domains, we turn to localization. Take any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and form the ring $\mathcal{O}_{K\mathfrak{p}}$ by localizing at the prime (invert all elements outside the prime). Since $\mathcal{O}_K$ has dimension 1, so does $\mathcal{O}_{K\mathfrak{p}}$. Furthermore, it has only two prime ideals (0) and $\mathfrak{p}$ so all ideals are powers of $\mathfrak{p}$ or (0) on which the ACC holds so this is Noetherian. Finally, since $\mathcal{O}_K$ is integrally closed in its field of fractions and these rings have the same field of fractions, one can show that $\mathcal{O}_{K\mathfrak{p}}$ is also integrally closed and hence a dedekind domain. In fact, it will be a Discrete Valuation Ring (DVR) which is stronger thana dedekind domain.

1.4 Lattices

21 Consider $\Gamma = \mathbb{Z}[i] \subset \mathbb{C}$. What is it's fundamental region? Is it complete? Volume?

The fundamental region is $[0,1) \times [0,i)$ or the unit square in the first quadrant of $\mathbb{C}$.

it is complete because $1, i$ are the basis vectors and as an $\mathbb{R}$-vector space $\mathbb{C}$ is 2-dimensional also. Also complete because translates of the fundamental mesh (bounded region) by the lattice covers all of $\mathbb{C}$.

volume: (intuitively this is a unit square so the volume should be 1)

$$\mathrm{vol}(\Gamma) = \left|\det\begin{pmatrix} \langle 1,1\rangle & \langle 1,i\rangle \\ \langle i,1\rangle & \langle i,i\rangle \end{pmatrix}\right|^{1/2} = \left|\det\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right|^{1/2} = |-1|^{1/2} = 1$$

22 Give an example of a (finitely generated) subgroup which is *not* a lattice.

Take $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$. Not discrete because multiples of $\sqrt{2}$ (being irrational) can be arbitrarily close to integers.

23 State the Minkowski's Lattice Point Theorem. Can the bound be improved?

Theorem *Let Γ be a complete lattice in the Euclidean vector space V and X a centrally symmetric, convex, subset of V. Suppose*

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma)$$

then X contains at least one nonzero lattice point $\gamma \in \Gamma$.

(note that if $x, -x \in X$ and their midpoint is, then $0 \in X \cap \Gamma$ for all lattices and X)

The bound cannot be improved.

Find some complete lattice Γ and centrally symmetric and convex set X such that $\mathrm{vol}(X) = 2^n \,\mathrm{vol}(\Gamma)$ with $\Gamma \cap X = \{0\}$.

Use $\Gamma = \mathbb{Z}[i] \subset \mathbb{C}$ and $X = \{x + iy : -1 < x, y < 1\}$ (open square centered at 0 with width 2, not including the boundary!).

$\mathrm{vol}(\Gamma) = 1$ $\mathrm{vol}(X) = 4 = 2^2 \,\mathrm{vol}(\Gamma)$

by picture $X \cap \Gamma = \{0\}$.

1.5 Minkowski Theory

24 In what way is an ideal of $\mathcal{O}_K$ a lattice? How can we compute the volume of an (integral) ideal?

Taking the embedding $j : K \to K_{\mathbb{R}}$ of a number field into its Minkowski Space, then $j(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$ given by $\mathbb{Z}$ combinations of the elements that generate $\mathfrak{a}$ over $\mathbb{Z}$ (not $\mathcal{O}_K$).

Computing its volume using the Hermitian inner product and the discriminant of the basis, we get

$$\mathrm{vol}(\mathfrak{a}) = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a})$$

where d_K is the discriminant of $K/\mathbb{Q}$ and $(\mathcal{O}_K : \mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ is the index of the ideal.

25 State the Minkowski Bound. How is it derived?

Every ideal $\mathfrak{a} \neq 0$ in $\mathcal{O}_K$ has some element $a \neq 0$ such that

$$|N_{K/\mathbb{Q}}(a)| \leq \tfrac{n!}{n^n}(\tfrac{4}{\pi})^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a})$$

$n = [K : \mathbb{Q}]$, $s =$ number of complex embeddings *pairs*,
d_K =discriminant of $K/\mathbb{Q}$, and $(\mathcal{O}_K : \mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.

Derivation Sketch:

Minkowski Lattice point theorem gives conditions (by volume) for intersections between lattices and centrally sym + convex regions.

Interpretting ideal as a lattice in the Minkowski space and choosing a clever centrally sym and convex region, get a bound that yields a point in the ideal within the region which translates to a bound on the norm of the element.

$X = \{(z_\tau) : \sum_\tau |z_\tau| < t\}$ choose clever t

1.6 The Class Number

26 What is the class number of a number field? Prove that it is finite.

$h_K = |Cl_K| = (J_K : P_K)$

Given a bound M, only finitely many ideals with $\mathfrak{N}(\mathfrak{a}) \leq M$, by considering their prime factorization and knowing that $\mathfrak{N}(\mathfrak{p}) = p^f$ for some f and only finitely many primes $\mathfrak{p}$ can lie over a particularly p.

Then use Minkowski bound to show that every class in Cl_K has an ideal with $\mathfrak{N}(\mathfrak{a}) \leq M$ so this bounds the number of classes and thus the size of Cl_K.

Details:

(Idea: take ideal, invert and find element to make integral ideal,
then find an element by Minkowski bound, and invert ideal again to get back to same class)

Bound $M = (2/\pi)^s \sqrt{|d_k|}$ fixed bound depending on the field.

Given any class of ideals in Cl_K, pick any ideal (may be fractional) $\mathfrak{a}$ in the class and choose $\gamma \in \mathcal{O}_K$ so that $\gamma\mathfrak{a}^{-1} = \mathfrak{b}$ is an integral ideal. Then some $\alpha \in \mathfrak{b}$ such that $|N(\alpha)| \leq M\mathfrak{N}(\mathfrak{b})$.

Define $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a}$. This is in the same class we started with. Then

$$\mathfrak{N}(\mathfrak{a}_1) = \mathfrak{N}(\alpha)\mathfrak{N}(\mathfrak{b}^{-1}) = |N(\alpha)|\mathfrak{N}(\mathfrak{b})^{-1} \leq M$$

27 Show that the magnitude of the discriminant, $|d_K|$, goes to ∞ as $[K:\mathbb{Q}] \to \infty$

Norm of an ideal is at least 1, so find an integral ideal in any class of the class group with $1 \leq \mathfrak{N}(\mathfrak{a}) \leq M$ then $1 \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ so a lower bound for the discriminant is

$$\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \leq \sqrt{|d_K|}$$

Take s as large as possible (since $\pi/4 < 1$) then $s = n/2$ and as $n \to \infty$ we have $\left(\frac{\pi}{4}\right)^{n/2}\frac{n^n}{n!} \to \infty$ (by inductive argument) so the discriminant magnitude does too.

28 Show that the quadratic field with discriminant $d_K \in \{5, 8\}$ has trivial class group.

This case is real so $s = 0$ and $r = 2$

computing the (better) minkowski bound:

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} = \frac{2}{4}\left(\frac{4}{\pi}\right)^0 \sqrt{|d_K|} = \tfrac{1}{2}\sqrt{|d_K|} < \tfrac{1}{2}\cdot 3 < 2$$

So every class has an integral ideal with norm less than 2 which as an integer will be 1, so it has no prime ideal factors meaning it has the unit ideal $(1) = \mathcal{O}_K$ in every class, so just one class.

29 Show that the quadratic field with discriminant $d_K \in \{-3, -4, -7, -8\}$ has trivial class group.

This case is real so $s = 1$ and $r = 0$

computing the (better) minkowski bound:

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} = \frac{2}{4}\left(\frac{4}{\pi}\right)^1 \sqrt{|d_K|} = \frac{1}{2}\cdot\frac{4}{\pi}\sqrt{|d_K|} = \frac{2}{\pi}\sqrt{|d_K|} = 2\frac{\sqrt{|d_K|}}{\pi} < 2$$

so every class has an integral ideal with norm 1 so again this is only the trivial class and so $h_K = 1$.

30 How would you compute the class group for a (quadratic) number field?

First, compute discriminant and ring of integers.

Using this, compute the minkowski bound for the field

each class in Cl_K has an integral ideal with norm less than M, consider just prime ideals/norms (building blocks)

for each rational prime, look at the possible factorizations in K that have norms less than M.

apply a "Dedkind Kummer" like Theorem to get the factorization of those primes in the ring of integers.

When $\mathcal{O}_K = \mathbb{Z}[\theta]$ with minimal polynomial $f(x)$. Then however $f(x)$ factors modulo p is how (p) factors in $\mathcal{O}_K$. (actually gives an explicit construction for those primes too!)

determine which, if any, are principal or which are *not* principal (take $N(\alpha) = N$ and find solutions or contradictions)

Find relations between them , e.g. $(\alpha) = \mathfrak{p}_1\mathfrak{p}_2$ implies $[\mathfrak{p}_1]^{-1} = [\mathfrak{p}_2]$.

31 Give a number field with non-trivial class group. How do you compute its class group?

Example: $K = \mathbb{Q}(\sqrt{-5})$ which has class group $Cl_K \cong \mathbb{Z}/2\mathbb{Z}$.

Computation: Minkowski Bound M_K bounds norms of ideals to consider for class group, depends on discriminant and complex embedding count

each ideal class has integral ideal with $N(\mathfrak{a}) \leq M_K$

Here $d_K = -20$ and $s = 1$

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} = \frac{2}{4}\frac{4}{\pi}\sqrt{20} = \frac{2}{\pi}2\sqrt{5} = (1+\varepsilon)(2+\varepsilon) < 3$$

So need to check primes over 2. (Dedekind Kummer or discriminant)

Since $2 \mid d_k$ it ramifies so in a quadratic field that means $(2) = \mathfrak{p}^2$ and so $[(1)], [\mathfrak{p}]$ generate Cl_K and $[\mathfrak{p}]$ has order 2.

Dedekind Kummer (for 3 for example) - Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ with min poly x^2+5 check how this factors mod 3. No roots so irreducible so (3) is inert (hence principal)

32 Compute the class group for $\mathbb{Q}(\sqrt{-5})$.

Discriminant:
$-5 \equiv 3 \mod 4$ so this has discriminant $d_K = 4D = -20$.
Minkowski Bound: (rememebder for $[K:\mathbb{Q}] = 2$ complex, should be $\frac{1}{2}\frac{4}{\pi}$)
$M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} = \frac{2}{4}\frac{4}{\pi}\sqrt{20} = \frac{2}{\pi}2\sqrt{5} = (1+\varepsilon)(2+\varepsilon) < 3$
So check all possible ideals with $\mathfrak{N}(\mathfrak{a}) = 1, 2$. $\mathfrak{N}(\mathfrak{a}) = 1 \implies \mathfrak{a} = \mathcal{O}_K$ is the trivial class.

Suffices to check prime ideals which generate the class group

Check each rational prime with power less than M_K and use Dedekind Kummer to determine how these split in $\mathcal{O}_K$.

Check relations between non-principal ideal classes

Hence $Cl_K = \{[\mathcal{O}_K], [\mathfrak{p}_2]\}$ and the class number is 2.

33 Compute the class group for $\mathbb{Q}(\sqrt{-23})$.

Discriminant:
$-23 \equiv -3 \equiv 1 \mod 4$ so this has discriminant $d_K = D = -23$. $[\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]]$
Minkowski Bound:
$M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} = \frac{2}{4}\frac{4}{\pi}\sqrt{23} = \frac{2}{\pi}\sqrt{23} \leq \frac{10}{\pi} < 4$
So check all possible ideals with $\mathfrak{N}(\mathfrak{a}) = 1, 2, 3$. $\mathfrak{N}(\mathfrak{a}) = 1 \implies \mathfrak{a} = \mathcal{O}_K$ is the trivial class.

Primes with norm 2 or 3 lie over (2) or (3) so we can check how these prime ideals split in $\mathcal{O}_K$ using Dedekind Kummer.

$\mathcal{O}_K = \mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{-23}}{2}$ so need its minimal polynomial (can also take complex conjugate).

$$\alpha^2 = \tfrac{1}{4}(1 - 23 + 2\sqrt{-23}) = \tfrac{1}{2}(-11 + \sqrt{-23}) = \tfrac{1+\sqrt{-23}}{2} - 6 = \alpha - 6 \implies p_\alpha(x) = x^2 - x + 6$$

$$p_\alpha(x) = (x-\alpha)(x-\overline{\alpha}) = (x - \tfrac{1+\sqrt{-23}}{2})(x - \tfrac{1-\sqrt{-23}}{2}) = x^2 - x\left(\tfrac{1+\sqrt{-23}+1-\sqrt{-23}}{2}\right) + \tfrac{1+23}{4} = x^2 - x + 6$$

For (2) and (3) look at how $p(x)$ factors mod $2, 3$.

Mod 2,3, $p(x) = x^2 - x + 6 = x^2 - x = x(x-1)$ so $(2) = \mathfrak{p}_1\mathfrak{p}_2$ and $(3) = \mathfrak{q}_1\mathfrak{q}_2$.

If any of these are principal, then $N(\alpha) = 2, 3$ for some α, which has no solutions.

Need to look at relations for these...

$\mathfrak{p}_i\mathfrak{q}_j = (\alpha)$ for some α? Well need $N(\alpha) = 2 \cdot 3 = 6 = \frac{1}{4}(a^2 + 23b^2)$ has solutions when $a, b = \pm 1$.

So $(\alpha) = \mathfrak{p}_1\mathfrak{q}_1$ (up to relabeling) $\implies [\mathfrak{p}_1]^{-1} = [\mathfrak{p}_2] = [\mathfrak{q}_1]$ and $[\mathfrak{p}_1] = [\mathfrak{q}_1]^{-1} = [\mathfrak{q}_2]$

$\{\mathcal{O}_K, [\mathfrak{p}_1], [\mathfrak{p}_2]\} \twoheadrightarrow Cl_K$

Relations between these? Well we know $[\mathfrak{p}_1]^{-1} = [\mathfrak{p}_2]$ so if $[\mathfrak{p}_1] = [\mathfrak{p}_2]$ then $\mathfrak{p}^2 = (\alpha)$, and α has norm 4, but the only element with norm 4 is 2, and $(2) \neq \mathfrak{p}_1^2$ so these are distinct classes (and each others inverses).

And $[\mathfrak{p}_2]^2$ has an ideal with norm 1,2,3, (actually 1,2) and we have found all of those so the group this generates is $\mathbb{Z}/3\mathbb{Z}$.

Hence $Cl_K = \{[\mathcal{O}_K], [\mathfrak{p}_1], [\mathfrak{p}_2]\}$ and the class number is 3.

34 Show that $|d_K| = 1$ if and only if $K = \mathbb{Q}$.

If $K = \mathbb{Q}$ then $d_K = 1$ by basis $\{1\}$.

Norm of an ideal is at least 1, so find an integral ideal in any class of the class group with $1 \leq \mathfrak{N}(\mathfrak{a}) \leq M$ then $1 \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ so a lower bound for the discriminant is

$$\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \leq \sqrt{|d_K|}$$

The smallest this can be is when $s = n/2$ but it can be shown (Stirling's Formula), $1 < \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}$ when $n > 1$ giving a contradiction unless $n = 1$ i.e. $K = \mathbb{Q}$.

1.7 Dirichlet's Unit Theorem

35 What does Dirichlet's Unit Theorem say? Give a sketch of the proof.

Dirichlet's Unit Theorem: Gives the structure of the units in a number field, specifically

$$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

where r is the number of real embeddings and s is the number complex embedding pairs (so $r + s - 1$ is $d - 1$ in the space of 'independent' embeddings)

Proof Sketch:

- Embed K into a multiplicative Minkowski Space, then using $\log|\cdot|$ translate into an additive version again.
- Look at the image of the group of units under this map which lands in a hyperplane of the space of dimension $r + s - 1$.
- Show that the image is a complete lattice in this space and so gives $\mathbb{Z}^{r+s-1}$.
- The kernel of the map embedding is the (finite) group of roots of unity in K, $\mu(K)$ so the units in K $\mu(K) \times \mathbb{Z}^{r+s-1}$ and the fundamental units are the ones that generate the free part.

36 Let K be the splitting field of $x^8 + 1$. What is the rank of the unit group in $\mathcal{O}_K$?

Step 1: determine the splitting field and its embeddings

The roots of this polynomial are the primitive 16th roots of unity, adjoining any one gives the splitting field, so $[K : \mathbb{Q}] = 8$

No real roots, so all complex pairs, and all embeddings are complex, $2s = [K : \mathbb{Q}] = 8$ so $s = 4$

Step 2: apply Dirichlet's Unit theorem

The rank of the unit group is $r + s - 1 = 0 + 4 - 1 = 3$ so there are 3 fundamental units.

1.8 Extensions of Dedekind Domains

37 How do intertia degrees and ramification degrees relate? Sketch a proof.

When L/K is separable, and $\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$. Let $f_i = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$ then

$$\sum_{i=1}^{r} e_i f_i = n = [L : K].$$

Note: If L/K Galois then e_i and f_i are the same for all primes, so $n = ref$.

Proof Sketch:

By Chinese Remainder Theorem

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L/\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}\mathcal{O}_L \cong \oplus_{i=1}^{r} \mathcal{O}_L/\mathfrak{q}_i^{e_i}\mathcal{O}_L$$

Computing dimensions of each as vector spaces over $\kappa = \mathcal{O}_K/\mathfrak{p}$...

$\dim_\kappa \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$

by taking a basis of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ over $\mathcal{O}_K/\mathfrak{p}$ and take representative elements and show that these are a basis of L/K and so have size n.

$\dim_\kappa \oplus_{i=1}^{r} \mathcal{O}_L/\mathfrak{q}_i^{e_i}\mathcal{O}_L = \sum_{i=1}^{r} e_i f_i$

take the descending chain $\mathcal{O}_L/\mathfrak{q} \supset \mathfrak{q}/\mathfrak{q}^2 \supset \cdots \mathfrak{q}^{e-1}/\mathfrak{q}^e$ each one of which is isomorphic to $\mathcal{O}_L/\mathfrak{q}$ which has degree f. The dimension of the overall jump is the sum of these, of which there are e, so $\dim_\kappa \mathcal{O}_L/\mathfrak{q}_i^{e_i}\mathcal{O}_L = e_i f_i$.

38 How does (2) split in the ring of integers of $\mathbb{Q}(\sqrt{7})$?

$K/\mathbb{Q}$ is primitive with $p(x) = x^2 - 7$ minimal polynomial. Taken modulo 2, this splits as $p(x) = x^2 - 1 = (x-1)(x+1) = (x+1)^2$ so (2) ramifies as $\mathfrak{p}_1^2$.

39 Consider $K = \mathbb{Q}(\sqrt{-5})$. Which primes ramify, split or remain inert.

Well since this is quadratic and $D = -5 \equiv 3 \mod 4$, the discriminant is $4D = -20$ so the primes that ramify are 2 and 5.

All other primes split completely or are inert, so using legendre symbol, p splits (completely) in $\mathcal{O}_K$ exactly when -20 is a square mod p. If -5 is a square mod p, then (p) splits (completely) in $\mathcal{O}_K$ and if not, then (p) is inert.

Well to flip this, use quadratic reciprocity which depends on p and 5 mod 4, but since $5 \equiv 1$ mod 4, always flips.

$$(-5/p) = (-1/p)(5/p) = (-1/p)(p/5) = (-1/p)(p/5)$$

If $p \equiv 1$ mod 4, then $(-1/p) = 1$ and if $p \equiv 3 \mod 4$ then $(-1/p) = -1$.

The qquares mod 5 are $1, 4$ so primes that are $1, 4$ mod 5 and 1 mod 4 or are $2, 3$ mod 5 and 3 mod 4 (that is $1, 9, 11, 19$ mod 20) split and primes that are $2, 3$ mod 5 and 1 mod 4 or $1, 4$ mod 5 and 3 mod 4 (that is $3, 7, 13, 17$ mod 20) are inert.

40 Is 79 a square mod 445?

Well 445 is not prime so we can't immediately apply quadratic reciprocity to reduce... but 79 will be a square mod 445 if it is a square mod every prime of 445, and 445 = 5*89 (round up by 5 to 450 which is 5*90). Is 89 prime? Yes! (check, divisibility by 2,3,5,7) [79 also prime because not div by 2,3,5,7]

So need to compute (79/5) and (79/89). $(79/5) = (4/5) = 1$

$(79/89) = (89/79)(-1)^{2k} = (89/79) = (10/79) = (2/79)(5/79)$

well $(2/79) = (-1)^{\frac{79^2-1}{8}}$ and $79 \mod 16 = -1$ so $79^2 - 1 = 0$ mod 16 so $(2/79) = 1$

Next, $(5/79) = (79/5)(-1)^{2k}$ because $5 \equiv 1 \mod 4$ so $= (79/5) = (4/5) = 1$ so 79 is a square mod 89 too (by good ol chinese remainder theorem)

Since 79 is a square mod all the primes of 445 it is a square mod 445 too!

41 Let $K = \mathbb{Q}(\alpha)$, where $\mathbf{Irr}_{\alpha,\mathbb{Q}}(x) = x^3 + 2x + 1$. What is the discriminant? Which primes ramify? How do 2 and 3 split in $\mathcal{O}_K$?

The discriminant of f is $-4b^3 - 27c^2 = -59$. Since $\operatorname{Disc}(f) = \pm(\mathcal{O}_K : \mathbb{Z}[\alpha])^2 \operatorname{Disc}(K)$ and 59 is square free, we have that $\operatorname{Disc}(K) = \pm 59$. Since 59 is prime, the only ramified primes are 59. Could determine the sign of the discriminant by reviewing the derivation of the discriminant of f and the discriminant of K using the Vandermonde matrix and considing signs.

Well $p(x) = x^3 + 2x + 1$, look at the factorization of this polynomial mod 2 and 3.

Mod 2: Check for roots, $p(x) = x^3 + 1$ has root for -1, so $x^3 + 1 = (x-1)(x^2 + x + 1)$. The quadratic has no roots, so this is the decomposition. Hence $(2) = \mathfrak{p}_1\mathfrak{p}_2$ where $f_1 = 1$ and $f_2 = 2$.

Mod 3: Check for roots, $p(x) = x^3 + 2x + 1$, 0 not a root, $1 + 2 + 1 = 1$ not a root, $2^3 + 2 * 2 + 1 = 8 + 4 + 1 = 13 = 1$ not a root, so this is irreducible and so (3) is inert with inertia degree 3.

42 Show that 2 splits completely in $\mathbb{Q}(\sqrt{17})$ but remains inert in $\mathbb{Q}(\sqrt{13})$.

Take $x^2 - 2$ the minimal polynomial for 2 and consider how it factors mod 17, well it splits if 2 is a square mod 17, that is $(2/17) = 1$. well mod 17, the squares are $1, 4, 9, 25 = 8, 36 = 19 = 2 \ldots$ so 2 is a square which means this polynomial splits and so does (2), which in a quadratic extension is split completely.

Now for $\mathbb{Q}(\sqrt{13})$, we can show this does not split *and* does not ramify. Again we consider squares, now mod 13, $1, 4, 9, 16 = 3, 25 = 12, 36 = 10, 47 = 21 = 8$ (only need to check up to halfway) and none of these are 2 so 2 does not split. The discriminant for $\mathbb{Q}(\sqrt{13})$... $D = 13 \equiv 1$ mod 4 so the discriminant is $D = 13$ and since 2 does not divide the discriminant it is unramified, so (2) is inert in $\mathbb{Q}(\sqrt{13})$.

1.9 Hilbert's Ramification Theory

43 What are the decomposition and inertia subgroups of $\operatorname{Gal}(K/\mathbb{Q})$? How does prime splitting decompose in the relevant subfields?

$G_{\mathfrak{p}}$ decomposition group is subgroup of size ef of the automorphisms that fix $\mathfrak{p}$. (has index r, the number of conjugates of $\mathfrak{p}$)

$I_{\mathfrak{p}}$ is the kernel of the map $G_{\mathfrak{p}} \to \operatorname{Gal}(\mathcal{O}_K/\mathfrak{p}/\mathbb{Z}/p\mathbb{Z})$.

By definition then, $G_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \operatorname{Gal}(\mathcal{O}_K/\mathfrak{p}/\mathbb{Z}/p\mathbb{Z})$ is the Galois group of a finite field extension, so is cyclic.

$$\begin{array}{cccc}
\text{totally ramified} & \mathfrak{p}_1^e\mathfrak{p}_2^e\cdots\mathfrak{p}_r^e & L & \mathrm{Gal}(L/L^I) = I_\mathfrak{p} \\
 & & \Big|\, e & \\
\text{inert} & \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r & L^I & \mathrm{Gal}(L/L^D) = G_\mathfrak{p} \\
 & & \Big|\, f & \\
\text{split completely} & \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r & L^D & \\
 & & \Big|\, r & \\
 & p & K &
\end{array}$$

44 Let K be the splitting field of x^4+1. What is $\mathrm{Gal}(K/\mathbb{Q})$? Which primes ramify in K? For which primes p is x^4+1 irreducible mod p?

The roots are primitive 8th roots of unity, so $K = \mathbb{Q}(\zeta_8)$. As a splitting field, it is Galois.

The automorphisms send ζ_8 to other *primitive* roots of unity, so $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$ and the $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$

Primes that ramify must divide the discriminant, and the discriminant for ζ_8 will be a power of 2, so 2 ramifies (can determine explicitly because $(2) = (1+i)^2$ and $i = \zeta_8^4$)

For p, Dedekind-Kummer says that (p) splits in K exactly as x^4+1 splits mod p. So need the primes p such that (p) is inert in K. If p is inert, then $e = 1$ and G_p the decomposition group is the whole of $\mathrm{Gal}(K/\mathbb{Q})$. However since $e = 1$ the inertia group is trivial and $G_p/I_p \cong \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p}/\mathbb{Z}/p\mathbb{Z})$ is a Galois group of an extension of finite fields, which is cyclic. However $\mathrm{Gal}(K/\mathbb{Q})$ is not cyclic, so no primes are inert and so x^4+1 is reducible mod p for all p.

45 Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G. For each prime $\mathfrak{p}$ let $I_\mathfrak{p}$ be its inertia group, show that the $I_\mathfrak{p}$ generate G.

Let $H = \langle I_\mathfrak{p}\rangle \leq G$ be a subgroup, giving a subextension $L/\mathbb{Q}$. For each prime $p \in \mathbb{Q}$, its ramification in L is the size of its inertia subgroup for any prime in L lying over p which is the image of $I_\mathfrak{p}$ in G/H which will be trivial since $I_\mathfrak{p} \subseteq H$. Thus no primes ramify in $L/\mathbb{Q}$, but the only such extension satisfying this is $L = \mathbb{Q}$ and so $G/H = \{1\}$, meaning that $H = G$.

1.10 Cyclotomic Fields

46 Which cyclotomic fields have finite unit groups?

Want to apply Diriclet's Theorem to determine when rank $(r+s-1)$ is 0.

Aside from $n = 1, 2$ ($\zeta_1 = 1$, $\zeta_2 = -1$) these are all complex fields with $r = 0$.

$n = 1, 2$ then $K = \mathbb{Q}$ and so $r = 1, s = 0$ and the rank is 0.

$n > 2$ Then $r = 0$ and $s = [K:\mathbb{Q}]/2 = \varphi(n)/2$, and we need $s = 1$ so $\varphi(n) = 2$

$\varphi(p_1^{e_1}\cdots p_k^{e_k}) = \prod_i p_i^{e_k-1}(p_i-1)$ so only allowed prime divisors for n are $2, 3$.

$\varphi(2) = 1$, $\varphi(4) = 2$, $\varphi(8) = 4$ too big!

$\varphi(3) = 2$, $\varphi(9) = 6$ too big!

already did $n = 2$

$n = 3, 4, 6$ also work!

$\boxed{\text{finite unit group} \iff n \in \{1, 2, 3, 4, 6\}}$

47 What can you say about subfields of $\mathbb{Q}(\zeta_p)$ that are quadratic over $\mathbb{Q}$?

Well $K = \mathbb{Q}(\sqrt{d})$ for some d will have discriminant d or $4d$ and must divide $d_{\mathbb{Q}(\zeta_p)} = p^*$ by ramification. We must have $p > 2$ for $\mathbb{Q}(\zeta_p) \neq \mathbb{Q}$, so then $p \mid d$ and can't have $4p$ so the unique quadratic field is:

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & p \equiv 1 \mod 4 \\ \mathbb{Q}(\sqrt{-p}) & p \equiv 3 \mod 4 \end{cases}$$

48 Let K be the splitting field of $x^8 + 1$. What is $\mathrm{Gal}(K/\mathbb{Q})$? Which primes ramify? What are the quadratic subextensions? For which primes is $x^8 + 1$ irreducible in $\mathbb{F}_p$? What is the rank of the unit group?

Well the roots are primitive 16th roots of unity so adjoining any one creates splitting field, hence $K = \mathbb{Q}(\zeta_16)$ and $[K : \mathbb{Q}] = \deg \Phi_{16}(x) = \varphi(16) = 2^3(2-1) = 8$.

$\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \cong (\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (can deduce by considering order of elements)

Ramified primes? Well ramified $\iff$ divide d_k and since $16 = 2^4$ the discriminant will also be a power of 2, so only 2 ramifies.

Quadratic subextensions? Well only 2 can ramify, so the possible quadratic fields are $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{2})$. How many should there be? Well quad subext means an index 2 subgorup of $\mathrm{Gal}(K/\mathbb{Q})$ of which there are two ($\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) so these are the two sub-extensions.

$x^8 + 1$ irreducible mod p? For p, Dedekind-Kummer says that (p) splits in K exactly as $x^8 + 1$ splits mod p. So need the primes p such that (p) is inert in K. If p is inert, then $e = 1$ and G_p the decomposition group is the whole of $\mathrm{Gal}(K/\mathbb{Q})$. However since $e = 1$ the inertia group is trivial and $G_p/I_p \cong \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p}/\mathbb{Z}/p\mathbb{Z})$ is a Galois group of an extension of finite fields, which is cyclic. However $\mathrm{Gal}(K/\mathbb{Q})$ is not cyclic, so no primes are inert and so $x^8 + 1$ is reducible mod p for all p.

Rank of $\mathcal{O}_K^\times$? Well $n = 8$ and all roots are imaginary, so $s = 4$ and $r = 0$ (counting embeddings) and by Dirichlet's Unit Theorem, rank is $r + s - 1 = 4 - 1 = 3$.

49 Show that $x^8 + 1$ is irreducible over $\mathbb{Q}$.

Cyclotomic polynomial trick here, $x^8 + 1$ irreducible $\iff$ $(y + 1)^8 + 1$ is irreducible, which satisfies Eisenstein's Criterion.

Chapter 2 - Theory of Valuations

2.1 The p-adic Numbers

50 Does 2 have a square root in $\mathbb{Z}_7$? [pre-Hensel's]

$x^2 = 2$ in $\mathbb{Z}_7$:

$\mathbb{Z}_7 \cong \lim_{\leftarrow k} \mathbb{Z}/7^k\mathbb{Z}$ with pointwise multiplication. Take $2 \in \mathbb{Z}_p$ which maps to $(2, 2, 2, \ldots)$ in the projective limit. Suffices to find a square-root in the limit.

Claim: 2 is a square mod 7^k for all k.
Proof: $2 = 3^2 \mod 7$ and for higher powers take the extension of the Legendre Symbol which is multiplicative so for evens always 1 and for odd k same as $(2/7) = 1$ so always has a square root.

Take the square root in the projective limit and map it back to $\mathbb{Z}_7$.

2.2 The p-adic Absolute Value

51 What is the product formula for $\mathbb{Q}$? Prove it.

Product Formula: For $a \in \mathbb{Q}^*$ and p ranging over all primes and ∞, $\prod_p |a|_p = 1$.
Proof:

$$a = \pm \prod_{p \neq \infty} p^{v_p(a)} = \frac{a}{|a|_\infty} \prod_{p \neq \infty} |a|_p^{-1} = a \left(\prod_p |a|_p \right)^{-1} \implies \prod_p |a|_p = 1$$

52 How can we construct $\mathbb{Q}_p$ using the p-adic absolute value?

$|x - y|_p$ gives a metric on $\mathbb{Q}$, analagous to $\mathbb{R}$, take the Cauchy Sequences w.r.t this metric and mod out by the nullsequences that approach 0 in the metric.

Then $|x|_p = \lim_{n\to\infty} |x_n|_p$ extends the metric to $\mathbb{Q}_p$.

As with $\mathbb{R}$, this is complete (every Cauchy Sequence in $\mathbb{Q}_p$ converges to a point in $\mathbb{Q}_p$), and $\mathbb{Z}_p = \{x : |x| \leq 1\}$.

This agrees with our initial construction of $\mathbb{Q}_p$ and $\mathbb{Z}_p$ only sums are no longer formal but actually converge w.r.t. the new metric.

53 What is the structure of $\mathbb{Z}_p$?

only one prime ideal, $\mathfrak{p}\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 1\}$ all ideals principal of the form $\mathfrak{p}^n\mathbb{Z}_p$.
$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ and again, $\mathbb{Z}_p \cong \lim_{\leftarrow k} \mathbb{Z}/p^k\mathbb{Z}$.

2.3 Valuations

54 How do the Approximation Theorem and Chinese Remainder Theorem relate?

Given primes $p_1, p_2, \ldots, p_n$ they have corresponding valuations $|\cdot|_{p_1}, \ldots, |\cdot|_{p_n}$.
Chinese Remainder Theorem: Define $N = p_1^{k_1} \cdots p_n^{k_n}$ for some k_i. Then

$$\mathbb{Z}/N\mathbb{Z} = \mathbb{Z}/\prod_i p_i^{k_i}\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i^{k_i}\mathbb{Z}.$$

Approximation Theorem: Given $a_1, \ldots, a_n \in \mathbb{Z}$, there exists some $x \in \mathbb{Q}$ such that $|x - a_i|_i < \varepsilon$.
Approximation $\implies$ CRT:

Let $\varepsilon = \min_i p_i^{-k_i}$ and suppose $x \in \mathbb{Z}$ (this is true for Strong Approx) then $|x - a_i|_i < \varepsilon$ means that $x \equiv a_i \mod p_i^{k_i}$. So then $x \mapsto \bar{x} \in \mathbb{Z}/N\mathbb{Z}$ is the desired element for CRT.

55 What are all the valuations on $\mathbb{Q}$? How do you know?

Only possible ones are $|\cdot|_p$ for all primes p and $|\cdot|_\infty$ the usual absolute value (and the trivial one which is ignored)

The first are all nonarchimedean, so if we had some other nonarchimedean valuation $||\cdot||$ then $||n|| \leq 1$ for all $n \in \mathbb{Z}$. If nontrivial, then some integer $||n|| < 1$ which by prime factorization means some $||p|| < 1$. Take $\mathfrak{a} = \{a \in \mathbb{Z} : ||a|| < 1\}$ then by maximality, $\mathfrak{a} = p\mathbb{Z}$ and then we can show that $||\cdot|| = |\cdot|_p^s$ for some s.

In the archimedean case there is a trick where $||n||^{1/\log n}$ is constant for all $n \in \mathbb{Z}$ so then use this to write $||n|| = (||n||^{1/\log(n)})^{\log(n)} = e^{s\log(n)} = |n|_\infty^s$ for some $s > 0$.

2.4 Completions

56 State Hensel's Lemma. Sketch a proof. What are some generalizations?

Hensel's Lemma *If $f \in \mathbb{Z}_p[x]$ with some $a_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(a_0) \equiv 0 \mod p$ but $f'(a_0) \neq 0 \mod p$ then there is a lift $\alpha \in \mathbb{Z}_p$ of a_0 such that $f(\alpha) = 0$.*

Proof Sketch

Uses Netwon's Method, take $f'(a_0) = \frac{f(a_0)}{a_0 - a_1}$ so $a_1 = a_0 - \frac{f(a_0)}{f'(a_0)}$. Iterate this process and use the conditions on $f(a_0)$ and $f'(a_0)$ to show that this converges to α a root of f.

Generalizations

Hensel's Lemma V2 *If $f \in \mathbb{Z}_p[x]$ with some $a_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $|f(a_0)|_p < |f'(a_0)|_p^2$ then there is a lift $\alpha \in \mathbb{Z}_p$ of a_0 such that $f(\alpha) = 0$.*

Hensel's Lemma V3 *If $f \in \mathbb{Z}_p[x]$ (with $f \not\equiv 0 \mod p$) with $\bar{f} = \bar{g}\bar{h} \mod p$, for relatively prime polynomials $\bar{g}, \bar{h}$ then there is a degree preserving lift $g = \bar{g} \mod p$ and $h = \bar{h} \mod p$ such that $f = gh$.*

57 Does 5 have a square root in $\mathbb{Q}_3$? What about 7?

Want to find solutions to $f(x) = x^2 - 5$ in $\mathbb{Q}_3$.

Well $f(x) \equiv x^2 + 1$ which has no roots in $\mathbb{Z}/3\mathbb{Z}$. If $f(\alpha) = 0$ then $|\alpha|_3^2 = |5|_3 \leq 1$, so $|\alpha|_3 \leq 1$ hence $\alpha \in \mathbb{Z}_3$.

If $\alpha \in \mathbb{Z}_3$ were a solution, then $a_0 \equiv \alpha \mod 3$ would be a solution to $f(x) \bmod 3$, so there is no square root of $\mathbb{Q}_3$.

On the other hand, $f(x) = x^2 - 7 \equiv x^2 - 1 = (x+1)(x-1)$ in $\mathbb{Z}/3\mathbb{Z}$ so there are roots here. There are simple because they are distinct roots, so they lift to roots of 7 in $\mathbb{Z}_3$. ($f'(x) = 2x$ and $\pm 2 \neq 0$ in $\mathbb{Z}/3\mathbb{Z}$)

2.5 Local Fields

58 What are local fields? Let K be a local field. Show that all ideals are powers of the maximal ideal.

Local Fields are those that are complete with respect to a discrete valuation (outputs in $\mathbb{Z} \cup \{\infty\}$) and has finite residue field.

Alternative definition of **local fields:** finite extensions of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.

Maximal ideals are then $\{\alpha : \nu(\alpha > 0\}$.

Take any ideal $\mathfrak{a}$ of the valuation ring ($\{\alpha : \nu(\alpha) \geq 0\}$). Then by the discreteness of the valuation, there exists a minimum n such that $\nu(\alpha) = n$ for $\alpha \in \mathfrak{a}$. We will show that $\mathfrak{a} = (\pi)^n$, where π is an uniformizer. If α has valuation n, then $\alpha = \pi^n u$ for a unit u. Thus $\pi^n \in \mathfrak{a}$ by inverting the unit. Then all $(\pi^n) = (\pi^n u) \subseteq \mathfrak{a}$. Furthermore, any other $\beta \in \mathfrak{a}$ has decompositon $\beta = \pi^m u$ for some $m \geq n$ so $\beta = \pi^n(\pi^{m-n}u) \in (\pi^n)$ so $\mathfrak{a} = (\pi)^n$.

59 Which roots of unity lie in $\mathbb{Q}_2^*$? $\mathbb{Q}_7^*$? How would you determine it for a general $\mathbb{Q}_p^*$?

Suppose ζ is an nth root of unity in $\mathbb{Q}_p^*$, then $\|\zeta\|_p^n = \|\zeta^n\|_p = \|1\|_p = 1$ so $\|\zeta\|_p = 1$ and thus $\zeta \in \mathbb{Z}_p^*$. The structure of $\mathbb{Z}_p^*$ is $\mathbb{Z}_p \times \mathbb{Z}/p-1\mathbb{Z}$ when p is odd or $\mathbb{Z}_p \times \mathbb{Z}/2\mathbb{Z}$ when $p = 2$ with additive structures on both components. If $\zeta \in \mathbb{Z}_p^*$ then there is some element $(\alpha, a) \in \mathbb{Z}_p \times \mathbb{Z}/M\mathbb{Z}$ with order n where $M = p-1, 2$ depending on the case. Since $\mathbb{Z}_p$ is an integral domain $n\alpha = 0$ implies that $\alpha = 0$ so we have that a has order n in $\mathbb{Z}/M\mathbb{Z}$ so then $n \mid M$. Conversly, for any $n \mid M$, an element $a \in \mathbb{Z}/M\mathbb{Z}$ with order n allows us to choose $(0, a) \in \mathbb{Z}_p^*$ with order exaclty n so we see that $n \mid M = p-1, 2$ is a necesary and sufficient condition for $\zeta_n \in \mathbb{Z}_p^*$.

For $\mathbb{Q}_2^*$ we have only $n = 1, 2 \mid 2$ so the roots of unity are ± 1.

For $\mathbb{Q}_7^*$ we have $n = 1, 2, 3, 6 \mid 6 = 7-1$ so we have ζ_6^k for $k = 0, 1, 2, 3, 4, 5, 6$ in $\mathbb{Q}_7^*$.

2.7 Unramified and Tamely Ramified Extensions

60 Let $f = X^3 - X^2 - 2X + 1$. Show that f is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}[X]/f$. Show that K is abelian. You can use the fact that the discriminant of f is 49. Find the discriminant of K and its ring of integers. Which non-archimedean primes ramify in K? Does the infinite prime ramify in K?

First, f is cubic, so reducible $\iff$ it has a root in $\mathbb{Q}$. Gauss's Lemma says f reducible over $\mathbb{Q}$ $\iff$ f reducible over $\mathbb{Z}$ when f is **primitive** (in particular, when monic) Over $\mathbb{Z}$, the constant term is the product of roots, so possible roots are only ± 1, neither of which satisfies $f(x) = 0$, so f is irreducible.

Since f is irreducible, $K = \mathbb{Q}[x]/f$ is a degree 3 extension, as long as $K/\mathbb{Q}$ is Galois, this is abelian with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. We will suppose that L is the splitting field of f, and show that $[L : \mathbb{Q}] = 3$, and so $K/\mathbb{Q}$ is Galois.

Consider the discriminant $\mathrm{Disc}(f) = ((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3))^2 = \delta^2$. $\mathrm{Gal}(L/\mathbb{Q}) \subset S_3$, so either S_3 or $\mathbb{Z}/3\mathbb{Z}$. If we have an odd permutation, then $\delta \mapsto -\delta$ and even permutations fix δ. Since $\mathrm{Disc}(f) = 49 = 7^2$ and $\pm 7 \in \mathbb{Q}$, $\delta = \pm 7$ is fixed by all permutations in the Galois group, hence the Galois group is $A_3 = \mathbb{Z}/3\mathbb{Z}$. Thus $L = K$ and so $K/\mathbb{Q}$ is Galois.

Knowing that $\mathrm{Disc}(f) = 49$, want to find $\mathrm{Disc}\, K/\mathbb{Q}$. Well they are related by

$$\mathrm{Disc}(f) = \mathrm{Disc}\, \mathbb{Z}[\alpha]/\mathbb{Z} = (\mathcal{O}_K : \mathbb{Z}[\alpha])^2 \,\mathrm{Disc}\, K/\mathbb{Q}$$

so either $\mathrm{Disc}\, K/\mathbb{Q} = 49$ or $\mathrm{Disc}\, K/\mathbb{Q} = 1$, but then $K = \mathbb{Q}$ contradiction to irreduciblity, so $\mathrm{Disc}\, K/\mathbb{Q} = 49$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Primes ramify if and only if they divide $\mathrm{Disc}\, K/\mathbb{Q}$, so only 7 ramifies.

For the infinite place, we need to know if $K \subset \mathbb{R}$ or not. If not, then f has a complex conjugate pair of roots, let $\alpha, \beta, \overline{\beta}$ be the roots, then

$$\mathrm{Disc}(f) = \prod_{i \neq j}(\alpha_i - \alpha_j) = (\alpha - \beta)^2(\alpha - \overline{\beta})^2(\beta - \overline{\beta})^2 = \left((\alpha - \beta)\overline{(\alpha - \beta)}\right)^2 (\beta - \overline{\beta})^2 = |\alpha - \beta|^4(\beta - \overline{\beta})^2$$

If $\beta = a + bi$ then $\beta - \overline{\beta} = 2bi$ so $(\beta - \overline{\beta})^2 = -4b^2 < 0$. Then $\mathrm{Disc}(f) < 0$, since $\mathrm{Disc}(f) = 49$ we know that $K \subset \mathbb{R}$ and so ∞ does not ramify (into complex conjugation).

2.8 Extensions of Valuations

61 Let $K = \mathbb{Q}[\alpha]$ where α is a root of $x^n - 2$ for $n \geq 2$. What is $[K : \mathbb{Q}]$? How many ways can the archimedean absolute value on $\mathbb{Q}$ be extended? What about the 2-adic absolute value? What are the rank and torsion subgroup of $\mathcal{O}_K^*$?

(a) $f(x) = x^n - 2$ is irreducible by Eisenstein, so $[K : \mathbb{Q}] = \deg(f) = n$.

(b) Each embedding $\tau : K \to \mathbb{C}$ gives a valuation of K by $|\alpha| = |\tau\alpha|$.

From this formulation, we see that complex embedding pairs each give 1 valuation and real embeddings give their own.

n even: 2 real embeddings $\alpha \mapsto \pm\sqrt[n]{2}$ and $s = \frac{1}{2}(n - r) = \frac{n-2}{2}$

n odd: only 1 real embedding $\alpha \mapsto \sqrt[n]{2}$ and $s = \frac{1}{2}(n - r) = \frac{n-1}{2}$

and number of embeddings is $r + s$.

(c) Each prime above (2) gives an extension of $| \ |_2$, but $(2) = (\sqrt[n]{2})^n$ is totally ramified so only one extension of $| \ |_2$.

(d) Dirichlet's Unit Theorem gives the rank as $r + s - 1$ using the same r, s by parity of n above.

For the torsion part, we need to find $\mu(K)$.

If $\zeta_n \in K$ then every prime divisor $p \mid n$ yields $\zeta_p \in K$. For odd p, this gives a subextension $Q(\zeta_p)$ with discriminant p^* but (2) does not ramify here, and yet it totally ramified so $\zeta_p \notin K$ for odd p.

Consider the case of ζ_{2^n}, we know that $\zeta_2 \in K$ because $\pm 1 \in \mathbb{Q}$ so if $\zeta_4 \notin K$ then $\mu(K) = \pm 1$. Since $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, we consider the extension of $| \ |_\infty$. Since $\mathbb{Q}(i)$ has only complex embeddings, these extend to complex embeddings in K but we know there is at least one real embedding, so $\zeta_4 \notin K$ and hence $\zeta_{2^n} \notin K$ for $n \geq 2$.

62 Write down a polynomial f over $\mathbb{Q}_3$ such that $\mathbb{Q}_3[x]/(f)$ is a totally ramified quartic extension of $\mathbb{Q}_3$.

Let $f(x) = x^4 - 3$. This is irreducible by Eisenstein's, so adjoining a root gives a quartic extension. Furthermore, α the root, satisfies $\alpha^4 = 3$, so the ideal $(\alpha)^4 = (3)$ in $\mathcal{O}_K$, meaning that the extension is totally ramified.

63 What are all the valuations of $\mathbb{Q}(i)$?

Archimedean: the real abs val ramifies as as the complex absolute value $|\alpha| = |\alpha|_{\mathbb{C}}^2$

Nonarchimedean:

For each prime p, determine how it splits in $\mathcal{O}_K$. If $p = 2$ it ramifies, so $(2) = \mathfrak{p}^2$ and we have the valuation $| \ |_{\mathfrak{p}}$.

If p odd, then it does not ramify, so either splits or inert. Splitting happens when $x^2 + 1$ splits mod p, that is when -1 is a square mod p,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

In the split case, we get two valuations and in the inert case we have the same p-adic valuation as before, $| \ |_p$.

Class Field Theory Statements

64 State Local Class Field Theory. What properties uniquely determine the map?

Local Class Field Theory Statement: Let K be a local field. Then there is a local artin map ϕ_K that is a continuous surjection (K^* with topology induced by valuation and $\mathrm{Gal}(\cdot/\cdot)$ with Krull topology)

$$K^* \xrightarrow{\phi_K} \mathrm{Gal}(K^{ab}/K)$$

where K^{ab} is the maximal abelian extension of K. For any finite abelian extension L/K, the quotient map $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$ composes to get a surjective map $\phi_{L/K} : K^* \to \mathrm{Gal}(L/K)$. If L/K is unramified and π is any uniformizer for K, then $\phi_{L/K}(\pi) = \mathrm{Frob}_p \in \mathrm{Gal}(L/K)$. Furthermore, the kernel of $\phi_{L/K}$ is $N_{L/K}(L^*)$ and this is inclusion reversing by Galois theory.

As a consequence, ϕ_K induces an isomorphism when passed to the profinite completion. Furthermore, $\phi_{L/K}(\mathcal{O}_K^*)$ gives the inertia subgroup of $\mathrm{Gal}(L/K)$.

Uniqueness: ϕ_K is the *unique* continuous homomorphism $K^* \to \mathrm{Gal}(K^{ab}/K)$ such that every finite unramified L/K and uniformizer π of K $\phi_{L/K}(\pi)$ is the Frobenious element of $\mathrm{Gal}(L/K)$ and that $\phi_{L/K}$ has kernel $N(L^*)$ inducing the desired isomorphism with the Galois group.

65 State Global Class Field Theory. How does it relate to the local maps? What needs to be checked to show that the composition is well defined on C_K?

Global Class Field Theory Statement: Let K be a global field. Let C_K be the idele class group (I_K/K^* where I_K are the ideles, the unit group of the adeles).

Then there is a global artin map ϕ_K that is a continuous surjection (C_K with ideles topology and $\mathrm{Gal}(\cdot/\cdot)$ with Krull topology)

$$C_K \xrightarrow{\phi_K} \mathrm{Gal}(K^{ab}/K)$$

where K^{ab} is the maximal abelian extension of K. This again induces an isomoprhism on the profinite completions.

For any finite abelian extension L/K, the quotient map $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$ composes to get a surjective map $\phi_{L/K} : C_K \to \mathrm{Gal}(L/K)$, which has kernel $N_{L/K}(C_L)$.

f L/K is unramified and π is any uniformizer for K, then $\phi_{L/K}(1, \ldots, 1, \pi, 1, \ldots) = \mathrm{Frob}_p \in \mathrm{Gal}(L/K)$.

Furthermore, $\phi_{L/K}(\mathcal{O}_\mathfrak{p}^*)$ gives the inertia subgroup for the ideal $\mathfrak{p}$ of K in $\mathrm{Gal}(L/K)$.

Local to Global: The global map when restricted to $K_v \hookrightarrow C_K$ gives back the local artin map of K_v. Conversely, we could construct the global map by taking the product of the local maps on each K_v. To make sure this is compatible with our defintion, this first needs to give a finite product so all but finitely many maps must be trivial. Furthermore, the product of these maps must also be trivial on the image of $K^* \hookrightarrow C_K$ since this lies in the quotient of the global map.

66 What is Artin Reciprocity? How is Quadratic Reciprocity a special case?

Artin Reciprocity Statement: Let $K/\mathbb{Q}$ be an abelian extension. The primes of $\mathbb{Q}$ the split completely in K are determined by a congruence condition modulo the conductor $\mathfrak{f}_{K/\mathbb{Q}}$.

Note: the conductor is defined for local fields as p^n for the smallest n such that the local artin map $\phi_\mathbb{Q}$ is trivial on $1 + p^n\mathbb{Z}_p$. The global conductor is the product of the local ones. If p is unramified, then $n = 0$ so this is a finite product of the primes that ramify.

Quadratic Reciprocity: While typically stated in terms of Legendre symbols, this statement could be retooled to say that the primes that split (completely) in $\mathbb{Q}(\sqrt{q})$ are determined by a congruence condition modulo $\mathrm{Disc}(\mathbb{Q}(\sqrt{q}))$. In this case, the discriminant is also the conductor (in magnitude, when ignoring the possible infinite place), so the Artin Reciprocity statement generalizes quadratic extensions to any finite abelian extension.

67 Let L/K be an extension of number fields in which almost all primes (all but finitely many) in K split completely in L. What can we conclude about L? Hint: Chebotarev Density.

Claim: $L = K$ when almost all primes split completely.

We begin by assuming that L/K is Galois and then extend to the non-Galois case. If a prime ideal $\mathfrak{p}$ in K splits completely, then it is unramified and thus has a frobenius automorphism $\varphi_{\mathfrak{q}} \in \mathrm{Gal}(L/K)$ for each $\mathfrak{q}$ lying over $\mathfrak{p}$ (or equivalently a uniquely defined conjugacy class of frobenius elements for $\mathfrak{p}$). These generate the decomposition group for each $\mathfrak{q}$ which is trivial since $\mathfrak{p}$ splits completely. Thus $\varphi_{\mathfrak{q}} = 1$ for all $\mathfrak{q}$. Conversely, if there is a $\mathfrak{q}$ over $\mathfrak{p}$ with frobenius $\varphi_{\mathfrak{q}} = 1$ then the decomposition group is trivial and $\mathfrak{p}$ splits completely.

Chebotarev density says that

$$\text{density}\,(\text{primes } \mathfrak{p} \text{ in } K \text{ with some } \mathfrak{q} \mid \mathfrak{p} \text{ and } \varphi_{\mathfrak{q}} = 1) = \frac{\#\{\tau 1 \tau^{-1}\}}{\#\,\mathrm{Gal}(L/K)} = \frac{1}{[L:K]}$$

Since we have shown the left hand side is also the density of primes that split completely, if almost all primes split completely this density is 1, making $[L:K] = 1$, i.e. $L = K$.

Now in the non-Galois case, take the Galois closure M of L over K. Then from Galois theory primes split completely in L/K if and only if they split completely in M/K. So lifting almost all primes split completely from L to M and applying the first part, we have that $M = K$ which implies that $L = K$ as desired.

68 How many quadratic extensions of $\mathbb{Q}_2$ are there? $\mathbb{Q}_5$?

Suppose $L/\mathbb{Q}_2$ is a quadratic extension, then by local CFT there is a surjective map

$$\mathbb{Q}_2^* \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/\mathbb{Q}_2) \cong \mathbb{Z}/2\mathbb{Z}$$

Since $2\mathbb{Z}$ is trivial in the image, $(\mathbb{Q}_2^*)^2$ will always lie in the kernel of the map so we can quotient out by this, $(\mathbb{Q}_2^*)^2 = (2^n \times \mathbb{Z}_2)^2 \cong 2(\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}) = 2\mathbb{Z} \times 2\mathbb{Z}_2 \times 1$ and quotienting gives

$$\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong (\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z})/(2\mathbb{Z} \times 2\mathbb{Z}_2 \times 1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^3.$$

Each choice of *surjective* map from $(\mathbb{Z}/2\mathbb{Z})^3$ to $\mathbb{Z}/2\mathbb{Z}$ gives a distinct quadratic extension. There are 8 total maps, and 1 trivial so this gives **7 quadratic extensions of $\mathbb{Q}_2$.**

If we repeat the same process for $\mathbb{Q}_5$, this time we have

$$\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^2 \cong (\mathbb{Z} \times \mathbb{Z}_5 \times \mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z} \times 2\mathbb{Z}_5 \times 2\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times 1 \times \mathbb{Z}/2\mathbb{Z}$$

so there are 4 total maps, 1 trivial, giving **3 quadratic extensions of $\mathbb{Q}_5$.**

These results can be verified using lmfdb. Example:
`http://www.lmfdb.org/padicField/?n=2&p=5&search_type=List`

69 In the case of $K = \mathbb{Q}$, how does the global artin map simplify?

First, we have that $\mathbb{Q}^{ab} = \mathbb{Q}(\zeta)$ (the extension obtained by adjoining all roots of unity) by Kronecker-Weber.

Next, we can simplify the left hand side of the map. The kernel is the connected component of 1 in $C_{\mathbb{Q}}$. Since $\mathbb{Q}_p$ is totally disconnected, the connected component in each of these is simply $\{1\}$ but for

$\mathbb{Q}_\infty^* = \mathbb{R}^*$ the connected component is $\mathbb{R}^+$. Quotienting out by this we will show gives the product $\prod_p \mathbb{Z}_p^*$.

Initially, the quotient will be $(\prod_p \mathbb{Q}_p^* \times \mathbb{R}^*/\mathbb{R}^+)/\mathbb{Q}^*$. Take any $(\alpha_p)_p \in \prod_p \mathbb{Z}_p^*$ and map it to the element $((\alpha_p)_p \times 1)/\mathbb{Q}^*$ in $(\prod_p \mathbb{Q}_p^* \times \mathbb{R}^*/\mathbb{R}^+)/\mathbb{Q}^*$. We first show that this is injective. If some other $(\beta_p)_p$ maps here as well, then for some $q \in \mathbb{Q}^*$, we have $(q\alpha_p)_p \times \frac{|q|}{q} = (\beta_p)_p \times 1$.

In particular, this means that $q = \beta_p/\alpha_p \in \mathbb{Z}_p^*$ for all p so q has no prime divisors in its numerator or denominator. And since $|q|/q = 1$ we have that q is positive, hence $q = 1$ and $\alpha_p = \beta_p$ for all p.

Now to show surjectivity, take any $(\gamma_p)_p \times \pm 1/\mathbb{Q}^*$. By the restricted product of the adeles, all but finitely many γ_p lie in $\mathbb{Z}_p^*$ already, so we need to find a choice of q that corrects the others. For each $\gamma_p \notin \mathbb{Z}_p^*$, take $a_p = p^{-\nu_p(\gamma_p)}$ Taking $\pm \prod_p a_p \in \mathbb{Q}^*$ (sign matching original sign of element) this will cancel out the places where $\gamma_p \notin \mathbb{Z}_p^*$ but will be a unit in all others, keeping those in $\mathbb{Z}_p^*$ that were already. By matching sign this ensures that we have something of the form $(\alpha_p)_p \times 1/\mathbb{Q}^*$ which is in the image of our map which is thus surjective and an isomorphism.

Putting it altogether we have for $\mathbb{Q}$ the isomorphism

$$\prod_p \mathbb{Z}_p^* \xrightarrow{\phi_{\mathbb{Q}}} \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

which makes sense becaause the Galois group on the right is the inverse limit of $(\mathbb{Z}/n\mathbb{Z})^*$ which does indeed give the structure on the left.

70 How do the idele class group and the ideal class group relate?

There is a surjective map $C_K \to Cl_K$. We define first by taking $\mathbb{I}_K \to J_K$ where $(\alpha_\nu) \mapsto \prod_{\nu=\nu_p} p^{\nu_p(\alpha_p)}$. Quotienting out by principal elements on both sides gives a surjection $C_K \to Cl_K$.

71 What is the Hilbert Class Field? How can we see that it has that galois group?

The hilbert field of K is the maximal abelian unramified extension of K. It's Galois group is isomoprhic to the ideal class group for K.

We can see this is the Galois group from the global artin map. The field is the largest abelian unramified extension, so we want the smallest open finite index subset of C_K and show that this is also the kernel of the map $C_K \to Cl_K$.

The norm group must contain all the finite $\mathcal{O}_\mathfrak{p}^*$ since these map to the inertia subgroups. There is some fussing with infinite places, but the kernel of the map $C_K \to Cl_K$ is $(\prod_{\mathfrak{p}\nmid\infty} \mathcal{O}_\mathfrak{p}^* \times \prod_{\nu|\infty} K_\nu^*)K^*$ which is the smallest group that contains all $\mathcal{O}_\mathfrak{p}^*$.