NOTES

VINCENT TRAN

Contents

Lemma 0.1. *Take R a domain and L a finite field extension of $Q(R)$. TFAE*

(1) x is integral in L
(2) the minimal polynomial over $Q(R)$ of x has coefficients in R
(3) x is integral in $R_{(P)}$ for all maximal ideals P.

Proof. (1) $\iff$ (2): The reverse direction is obvious. For the forward, we can consider the Galois closure of L. This is still finite over $Q(R)$. Then the minimal polynomial of x over $Q(R)$ is $\prod(t - \sigma(x))$ for σ the Galois conjugates of x. Since $\sigma(x)$ are integral over R and the coefficients are combinations of the $\sigma(x)$ and in Q, the coefficients are in R.

(2) $\iff$ (3): one direction is easy. The other follows from the proof of the localness of being integrally closed. □

Proposition 0.2. *The integral closure of dedekind domains in a finite separable closure is a Dedekind domain.*

Proof. Take $R \subseteq Q$, L a finite separated extension of Q. Let R' be the integral closure of R in L. Suppose $[L : Q] = n$. Furthermore, R' is finitely generated and if R is a PID, then R' is free over R of rank n.

Our goal is to find $R' \subseteq M \subseteq L$. First we realize that L admits a basis over Q $b_1, \ldots, b_n$. For each b_i, it is the root of a polynomial over $\boldsymbol{Q}$. Thus there is s_i such

that $b_i' := s_i b_i \in R'$. So we have that

$$Rb_1' + \cdots + Rb_n' \subseteq R'.$$

Now we use that L is a separable extension. Recall that because L is separable, the blinear form $L \times L \to Q$ via trace is non-degenerate. Thus for $b_1', \dots, b_n'$, we can choose the dual basis c_j such that

$$\operatorname{tr}(b_i, c_j) = \delta_{ij}.$$

Claim:

$$R' \subseteq Rc_1 \oplus Rc_2 \oplus \cdots Rc_n.$$

Let $x \in R'$. Then $x = a_1c_1 + \cdots + a_nc_n$ for $a_i \in Q$. But, $a_i = \operatorname{tr}(b_i x)$. Since $b_i x$ is integral, $\operatorname{tr}(b_i x)$ is integral. Hence $a_i \in R'$. Hence R' is finitely generated and thus Noetherian.

If R is a PID, then $R' \subseteq R^n$ so that R' is free as well of rank n.

So we have that R' is Noetherian, a domain, and integrally closed. So finally, take P a non-zero prime ideal of R'.

Note that $P \cap R$ is a prime ideal of R. We shall show that it is non-zero. Take $0 \neq x \in P$ with minimal polynomial $t^n + \cdots + a_0$. Then by passing to the separable closure, we conclude that $0 \neq a_0 \in R$. Then $a_0 = x \cdot$ a polynomial so that $\frac{a_0}{x} \in R'$. Since $a_0 = \frac{a_0}{x} \cdot x$ and $x \in P$, so $a_0 \in P$ and hence $P \cap R$ is non-zero.

Now let $F = \frac{R}{R \cap P}$. This is a field. This injects into $\frac{R'}{P}$ and $\frac{R'}{P}$ is finite dimension over F because R' is finitely generated over R. Thus $\frac{R'}{P}$ is also a field so that P is maximal. Thus R' is a Dedekind domain.

Proof of R'/P being a field: Consider the linear operator $y \cdot : D \to D$ with D finite dimensional over F and $y \in D$. This is injective because D is a domain. By linear algebra, $y \cdot$ is also surjective. Hence every element in D is invertible. □

Corollary 0.3. *A basis for R' over R is also a basis for L over Q.*

We are especially interested in $R = \boldsymbol{Z}, \boldsymbol{F}_q[t], \boldsymbol{C}[t]$.

Example 0.4. Consider $R = \boldsymbol{C}[x] + \boldsymbol{C}[x]\sqrt{x^3 - 1}$. This is a Dedekind domain. Consider the submodule I of the free R-module R. If it was true that all submodules of a free module over a Dedekind domain was free, then I would be a rank 1 R module. Thus R is principal.

We have the prime ideal $(x - 1, \sqrt{x^3 - 1}) \subseteq R$. But this isn't principal.

Nevertheless, a local ring is a PID iff it is a Dedekind domain.

Example 0.5. Consider localizing the previous example. When we localize at $(x - 1, \sqrt{x^3 - 1})$, we see that $\sqrt{x^3 - 1}$ generates it: $\frac{x-1}{\sqrt{x^3-1}}$.

1. Basis

We want to compute bases of integral closures. Let R be a PID, L/Q a finite degree n separable extension. Specify R to $\boldsymbol{Z}$. Then

$$\mathcal{O}_L = \boldsymbol{Z}b_1 \oplus \cdots \boldsymbol{Z}b_n.$$

We shall use the trace quadratic form again.

Let b_i be a basis for L over Q. Then let $D_{L/Q}(b_1, \dots, b_n) = \det(\operatorname{tr}(b_i b_j))$. This is in Q and non-zero because the trace is non-degenerate (and this matrix detects

degeneracy). A quick intuition check: if b_i are in $\mathcal{O}_L$, then this determinant is in R.

Proposition 1.1. *Let $A \in \boldsymbol{GL}_n(Q)$. Then if we consider the basis $Ab_i = c_i$, then*

$$D_{L/Q}(c_1, \dots, c_n) = D_{L/Q}(b_1, \dots, b_n)(\det A)^2.$$

Proof. $\det(\operatorname{tr}(c_i c_j)) = \det A \det(\operatorname{tr}(b_i b_j)) \det A^T$ □

Example 1.2. Take $Q(\sqrt{d})$ with d square-free. Then the basis is $1, \sqrt{d}$ so that

$$D_{L/Q} = \det \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d.$$

With basis $1, \frac{1+\sqrt{d}}{2}$, we have that

$$D_{L/Q} = \det \begin{bmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{bmatrix} = d.$$

2. 1.15

Take R a Dedekind domain, Q the quotient field, L a finite separable extension, and S the integral closure of R in L. Then take $\alpha_1, \dots, \alpha_n \in L$ a basis for L over Q. If $\alpha_i \in S$: $D_{L/\boldsymbol{Q}}(\alpha_i) \in R$. If R is a PID, then $\exists \alpha_i$ such that $S = R\alpha_1 \oplus \cdots \oplus R\alpha_n$.

Now let α_i be a basis for S and β_i be a basis for L. Then notice that $\beta_i = \sum r_{ij}\alpha_j, r_{ij} \in R$. Let $M = (r_{ij}) \in M_{n\times n}(R)$. Since α_i, β_i are bases of L, $\det M \in R$ and is non-zero. Then

$$D_{L/\boldsymbol{Q}}(\beta_i) = (\det M)^2 D_{L/\boldsymbol{Q}}(\alpha_i).$$

If the β_i is a basis of S, then $\det M$ is a unit. Thus

$$D_L \coloneqq D_{L/\boldsymbol{Q}}(\alpha_i) \in (R \setminus \{0\})/((\boldsymbol{R}^\times)^2).$$

When R is $\boldsymbol{Z}$, $D_L \in \boldsymbol{Z}$.

Example 2.1. When R is $\boldsymbol{F}_p[x]$, then $(\boldsymbol{F}_p[x]^\times)^2$ is $\boldsymbol{F}_p^\times$ when $p \neq 2$. Then the discriminant is determined up to a scalar and sign, so we can force it to be monic.

Example 2.2. Take $\boldsymbol{Q}(\sqrt{D})$ with D square free. Then

$$D_{\boldsymbol{Q}(\sqrt{D})} = \begin{cases} 4D & D \neq 1 \pmod 4 \\ D & D = 1 \pmod 4 \end{cases}.$$

Note that $|\det M| = [S : \langle \beta_i \rangle]$.

In general, if $L = \boldsymbol{Q}(\theta)$, then $S \supseteq \boldsymbol{Z}[\theta]$.

Definition 2.3. The **index** of θ is $[S : \boldsymbol{Z}[\theta]]$.

Proposition 2.4. *Thus*

$$(\operatorname{ind}(\theta))^2 D_{L/K}(\theta) = D_{L/K}(1, \theta, \dots, \theta^{n-1}).$$

Proof. To see the index fact, notice that

$$\boldsymbol{Z}^n \xrightarrow{M} \boldsymbol{Z}^n$$

is injective and $[\boldsymbol{Z}^n : \operatorname{im}(M)] = |\det M|$ by selecting a nice basis for both spaces that makes M to be diagonal. □

Theorem 2.5. $D_L = 1, 0 \pmod 4$ *for* $R = \boldsymbol{Z}$.

In general, D_L *is a square mod* 4.

Proof.

Definition 2.6. Let α_i be a basis of S. Let

$$P = P(\alpha_1, \dots, \alpha_n) = \begin{bmatrix} \alpha_1^{(1)} & \cdots & \alpha_n^{(n)} \\ \vdots & \vdots & \vdots \\ \alpha_1^{(n)} & \cdots & \alpha_n^{(n)} \end{bmatrix}.$$

Then $P \in M_{n\times n}(\overline{Q})$.

Proposition 2.7. $(\mathrm{tr}(\alpha_i\alpha_j)) = P^T P$

Proof. The RHS has in (i, j) the sum of the Galois conjugates of $\alpha_i\alpha_j$. This is the trace of $\alpha_i\alpha_j$. □

The above then implies that D is a square. But we haven't shown yet that $\det P \in \boldsymbol{Z}$. In fact, in general it isn't. So instead we must consider it in a field extension.

We know that

$$\det P = \sum_{\sigma\in\mathbb{S}_n} (-1)^{\mathrm{sign}(\sigma)} \prod_{i=1}^{n} \alpha_i^{\sigma(i)}.$$

Thus

$$\det P = \sum_{\sigma\in A_n} \prod_{i=1}^{n} \alpha_i^{\sigma(i)} - \sum_{\sigma\notin A_n} \prod_{i=1}^{n} \alpha_i^{\sigma(i)}.$$

By looking at the Galois action on $A - B$, we conclude that A, B are Galois conjugates. Thus $A + B, AB \in R$. But $D_L = (A - B)^2 = (A + B)^2 - 4AB$, which is a square mod $4R$. □

Corollary 2.8. *Suppose* $D \neq 1 \pmod 4$. *We know that*

$$(\mathrm{ind}(\sqrt{D}))^2 D_{\boldsymbol{Q}(\sqrt{D})} = D_{\boldsymbol{Q}(\sqrt{D})/\boldsymbol{Q}}(1, \sqrt{D}) = 4D.$$

Thus we have two cases: $\mathrm{ind}(\sqrt{D}) = 1, 2$. *Since* $D \neq 1 \pmod 4$, $D_L = 0 \pmod 4$ *by the Theorem (if* $\mathrm{ind}(\sqrt{D}) = 2$, *then* $D_L \equiv D \neq 1 \pmod 4$*). This thus forces* $\mathrm{ind}(\sqrt{D}) = 1$, *as otherwise* D *wouldn't be square-free. Hence* $S = \boldsymbol{Z}[\sqrt{D}]$.

Recall that an Eisenstein polynomial with respect to prime p is such that $p \nmid a_n$, $p|a_{n-1}, \dots, a_0$, and $p^2 \nmid a_0$.

Lemma 2.9. *If* $\theta \in \mathcal{O}_L$ *is such that* $L = Q(\theta)$, *and the minimal polynomial of* θ *is Eisensteinian for* p. *Then* $p \nmid \mathrm{ind}\,\theta$. *Let the minimal polynomial be* $X^n + a_{n-1}X^{n-1} + \cdots + a_0$.

Proof. Notice that $\theta^n/p \in \mathcal{O}_L$ since it equals $\frac{-a_{n-1}\theta^{n-1}-\cdots-a_0}{p}$. Now suppose that $p \mid \mathrm{ind}\theta$. Then $\mathcal{O}_L/\boldsymbol{Z}[\theta]$ is a finite group H such that $p \mid |H|$. We know then that $\exists\overline{\alpha} \in H \setminus \{0\}$ such that $p\overline{\alpha} = 0$. Furthermore, $\alpha \in \mathcal{O}_L$ such that $p\alpha \in \boldsymbol{Z}[\theta]$. Then let

$$p\alpha = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}, b_i \in \boldsymbol{Z}.$$

Suppose that $p \mid b_0, b_1, \ldots, b_{j-1}$ and not b_j. Now let

$$\beta = \alpha - \frac{b_0 + b_1\theta + \cdots + b_{j-1}\theta^{j-1}}{p} = \frac{b_j\theta^j + \cdots b_{n-1}\theta^{n-1}}{p} \in \mathcal{O}_L.$$

Then $\beta \cdot \theta^{n-j-1} \in \mathcal{O}_L$. This equals

$$\frac{b_j\theta^{n-1} + \cdots + b_n\theta^{2n-j-1}}{p} = \frac{b_j\theta^{n-1}}{p} + \ldots$$

where the dots is in $\mathcal{O}_L$. Thus $b_j\theta^{n-1}/p \in \mathcal{O}_L$. But the norm of this is $b_j^n \cdot N(\theta^{n-1})/p^n$. We have established that $p^n \nmid a_0 = N(\theta^{n-1})$. Thus this isn't in $\boldsymbol{Z}$, giving us a contradiction. □

3. 1.17

Example 3.1. We shall show that an integral basis of $\mathcal{O}_{\boldsymbol{Q}(\sqrt{2})}$ is $1, \sqrt{2}$. We know that the discriminant of $D(1, \sqrt{2}) = 8$. Thus

$$(\operatorname{ind}\sqrt{2})^2 D_{\boldsymbol{Q}(\sqrt{2})} = 8.$$

Either the index is 1 or 2. But the above result implies that $2 \nmid \operatorname{ind}\sqrt{2}$ so that the index is 1.

Proposition 3.2. *Let θ be a root of $f(X) = X^n + a_{n-1}X + \cdots + a_0$. Then*

$$D(1, \theta, \ldots, \theta^{n-1}) = .$$

In an earlier result, we showed that

$$D(1, \theta, \ldots, \theta^{n-1}) = (\det P)^2.$$

Since $P_{ij} = (\alpha^i)^{(j)} = (\alpha^{(j)})^i$ By rearranging, P is a Vandermonde matrix. Thus

$$\det P = \prod_{i<j}(\alpha^{(j)} - \alpha^{(i)}).$$

Thus

$$(\det P)^2 = \left(\prod_{i<j}(\alpha^{(j)} - \alpha^{(i)})\right)^2 = (-1)^{n(n-1)/2}\prod_{i\neq j}(\alpha^{(i)} - \alpha^{(j)}.$$

This also equals

$$(-1)^{n(n-1)/2}\prod_{i=1}^{n}\prod_{j=1, j\neq i}^{n}(\alpha^{(i)} - \alpha^{(j)}).$$

Let the second product be β_i. Notice that the β_i are conjugates. So for a choice of β,

$$(-1)^{n(n-1)/2}\prod_{1}^{n}\beta^{(i)} = (-1)^{n(n-1)/2}N_{\boldsymbol{Q}(\beta)/\boldsymbol{Q}}(\beta).$$

Then notice that

$$\beta = f'(\alpha)$$

so that

$$D(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2}N(f'(\alpha)).$$

Example 3.3. Let p be an odd prime and consider $\boldsymbol{Q}(\zeta_p)$. The minimal polynomial of ζ_p is $\phi(x) = x^{p-1} + \cdots + 1$.

Question 3.1. $\boldsymbol{Q}[\zeta] \subseteq \mathcal{O}_{\boldsymbol{Q}(\zeta)}$?

Question 3.2. What is $D_{\boldsymbol{Q}(\zeta)}$?

First we compute

$$D(1, \zeta, \dots, \zeta^{p-1}).$$

By the above proposition, we can see that this equals $(-1)^{n(n-1)/2} N(f'(\zeta))$. By the product rule,

$$(x-1)\phi = x^p - 1 \implies (x-1)\phi' + \phi = px^{p-1} \implies (\zeta - 1)\phi'(\zeta) = p\zeta^{p-1} = \frac{p}{\zeta}.$$

Thus

$$\phi'(\zeta) = \frac{p}{\zeta(\zeta - 1)}.$$

Hence

$$D_\zeta = (-1)^{(p-1)(p-2)/2} \frac{N(p)}{N(\zeta)N(\zeta - 1)} = (-1)^{\binom{p-1}{2}} \frac{p^{p-1}}{(-1)^{p-1} N(\zeta - 1)}.$$

We can see that $N(\zeta - 1) = (-1)^{p-1} \cdot$ the constant term of $\phi(X+1)$ since $\phi(X+1)$ is monic and $\zeta - 1$ has $p-1$ conjugates. This constant term is p. Since p is odd, we end up with

$$D_\zeta = (-1)^{\binom{p-1}{2}} \frac{p^{p-1}}{p} = (-1)^{\binom{p-1}{2}} p^{p-2} = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

This tells us that D_L is an odd power of p up to sign. This also solves the $p = 3$ case.

Finally, to compute the index of ζ, we can see that $\boldsymbol{Z}[\zeta] = \boldsymbol{Z}[1 - \zeta]$. But because the minimal polynomial of $1 - \zeta$ is Eisenstein. Since $\operatorname{ind} \zeta = \operatorname{ind} 1 - \zeta$, an above proposition implies that $\operatorname{ind} \zeta = 1$. Thus

$$D_L = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Question 3.3. What does the sign of the discriminant measure?

Example 3.4. We now ask about when $\boldsymbol{Z}[\alpha] \hookrightarrow \mathcal{O}_L$ has finite index.

We instead look to $\mathcal{O}_L = \boldsymbol{F}_p[x]$. Then a finite index subring is the kernel of the map $f \mapsto f(1) - f(0)$. The kernel coincidentally works out to be a ring.

By analogy, we instead look to finite dimensional index subrings of $\boldsymbol{C}[x]$. The same map gives us a subring. So we are interested in functions that are the same on 0 and 1. This is the same as gluing $0, 1$ together.

4. 1.22

Proposition 4.1. *The sign of the discriminant of $\mathcal{O}_L$ is $(-1)^{r_2}$.*

Proof. By a formula, the sign of D_L is the same as the sign of $\det P^T P$. Then complex conjugation of P changes the determinant by $(-1)^{r_2}$. Thus $\det P^T P = (-1)^{r_2} \det P^* P = (-1)^{r_2} \det P \overline{\det P}$. Since $\det P \overline{\det P}$ is positive, we are done. □

Definition 4.2. A **fractional ideal** $I \subseteq Q(R)$ is an R module if $\exists a \in R$ such that $aI \subseteq R$.

Example 4.3. $R, I \trianglelefteq R$, $0 \neq a \in Q$, $aR \subseteq Q(R)$. Another example is $\frac{1}{2}\boldsymbol{Z} \subseteq \boldsymbol{Q}$.

Definition 4.4. If I, J are fractional ideals, then

$$IJ \coloneqq \langle ab | a \in I, b \in J \rangle$$

(R-module). If I, J are fraction, then IJ is also a fractional ideal.

Note that $RI = I$ since $I = 1 \cdot I \subseteq RI \subseteq I$ since I is an R module.

Definition 4.5. A fractional ideal is **invertible** if $\exists$ fractional ideal J such that $IJ = R$.

Example 4.6. The inverse of aR is $\frac{1}{a}R$. Not all non-zero ideals of R are invertible. But in Dedekind domains, all fractional ideals are invertible.

Theorem 4.7. *Let R be a Dedekind domain and I a non-zero fractional ideal. Then I is a unique product of (can be negative) powers of prime ideals.*

Example 4.8. $\langle x, y \rangle \subseteq \boldsymbol{C}[x, y]$ is not an invertible ideal.

Lemma 4.9. *Given non-zero ideal $I \subseteq R$, $\exists P_1, \ldots, P_k$ prime non-zero ideals such that*

$$P_1 \cdots P_k \subseteq I \subseteq P_1 \cap \cdots P_k.$$

Proof. Assume that there doesn't exist I such that this property isn't satisfied. Then there is a maximal I in this set by Noetherian property. Then I can't be prime because otherwise $P_1 = I$. Thus $\exists a, b \in R$ such that $ab \in I$ and $a, b \notin I$.

Now consider $I \subsetneq I + aR, I + bR$. Then the product of these two ideals is contained in I and also is in the intersection Since I was the maximal counter example, $I + aR, I + bR$ satisfies the property. Hence we are done. □

Lemma 4.10. *If $P \trianglelefteq R$ is prime, then P is invertible.*

Proof. We want $IP = R$ for a fractional ideal I. If I exists, then $I \subseteq \{x \in Q | \forall a \in P, xa \in R\}$. Let I be the set on the RHS. This is a fractional ideal. Then we shall show that $IP = R$.

Clearly $R \subseteq I$. Hence $P \subseteq IP$. Furthermore, by definition, $IP \subseteq R$. It is thus enough to show that $P \neq IP$ (since all non-zero primes are maximal).

So suppose $P = IP$. Then $\forall x \in I$, $xP \subseteq P$. Since P is finitely generated, $xP \subseteq P$. Hence $x \in R$ as it is then integral. Therefore $P = IP \iff I = R$. Thus all we need to show is that $I \neq R$.

Take $0 \neq a \in P$. Then there exists

$$P_1 \cdots P_k \subseteq aR \subseteq P_1 \cap \cdots P_k.$$

Suppose that none of the P_i are in P. Then the product of the elements not in P_i is not in P, but $aR \subseteq P$. Since non-zero primes are maximal, $P = P_i$.

Pick k to be minimal. Then $P_2 \cdots P_k \not\subseteq aR$. Thus $\exists b \in P_2 \cdots P_k$ such that $\frac{b}{a} \notin R$. Finally, we want to show that $\frac{b}{a} \in I$. Then $\frac{b}{a}P \subseteq \frac{1}{a}P_1P_2 \cdots P_k \subseteq R$ ($b \in P_2 \cdots P_k$). □

Corollary 4.11. *This proves the above counter-example is a counter-example: $\frac{f}{g}x \in \boldsymbol{C}[x, y], \frac{f}{g}y \in \boldsymbol{C}[x, y]$. But then g has at most x in denom, g has at most y. Contradiction. Thus $I = R$ for this prime ideal.*

Theorem. First we show for non-fractional ideals of R.

By the lemma, we have $P_1 \cdots P_k \subseteq I$. If $k = 0$, then $R \subseteq I$. If $k = 1$, then because all prime ideals are maximal, $I = P_1$.

Suppose we have shown this for $k - 1$. Then

$$P_1 \cdots P_k \subseteq I \subseteq P_1$$

because I is contained in some maximal ideal $\mathfrak{m}$. This maximal ideal has to be one of the P_i. If $\mathfrak{m}$ isn't one of the P_i, then there is a product of all these elements not in P_i that is in I, contradicting the primeness of $\mathfrak{m}$. Hence $P_2 \cdots P_k \subseteq P_1^{-1} I \subseteq R$ so that by induction hypothesis, we are done.

Now if I is a fractional ideal, then $aI \subseteq R$ so that $aI = a_1 \cdots a_\ell$ and $aR = P_1 \cdots P_k$. Hence $a^{-1}R = P_1^{-1} \cdots P_k^{-1}$ and $a^{-1}RaI = P_1^{-1} \cdots P_k^{-1} a_1 \cdots a_\ell$.

Finally, this decomposition is unique: If $P_1^{e_1} \cdots P_k^{a_k} = a_1^{f_1} \cdots a_\ell^{f_\ell}$. We can assume the e_i, f_i are positive by cross multiplying. The RHS equals $a_1(a_1^{f_1 - 1} \cdots a_\ell^{f_\ell}) \subseteq a_1$. By the same argument above, this implies that one of the $\mathfrak{p}_i = a_1$. Thus we can cancel it.

By induction, we have that R is some product of prime ideals. But then R is contained in one of those prime ideals, a contradiction. □

A slightly different formulation of the theorem is

Definition 4.12. $\mathrm{Div}(R) :=$ the abelian group of fractional ideals under the operation of $\cdot$. Every prime ideal is an element of $\mathrm{Div}(R)$. We have a map $\boldsymbol{Z} \to \mathrm{Div}(R)$ for every prime ideal $n \mapsto \mathfrak{p}^n$. Thus we have

$$\bigoplus_{\mathfrak{p} \in \max(R)} \boldsymbol{Z} \to \mathrm{Div}(R).$$

The theorem is equivalent to this map being an isomorphism.

We also have $Q^\times \to \mathrm{Div}(R)$ via $a \mapsto aR$. The kernel of this map is the set of a such that $aR = R$, so a is a unit. So we have

$$0 \to R^\times \to Q^\times \to \mathrm{Div}(R) \to \mathrm{cl}(R) \to 0.$$

The elements in the image of $Q^\times$ are principal. Thus $\mathrm{cl}(R) = 0 \iff R$ is a PID.

Example 4.13. $R = \boldsymbol{Z}$ gives us

$$0 \to \{\pm 1\} \to \boldsymbol{Q}^\times \twoheadrightarrow \bigoplus_{p \text{ prime}} \boldsymbol{Z} \to \mathrm{cl}(\boldsymbol{Z}) = 0 \to .$$

Theorem 4.14 (Minkowski)**.** *For all rings of integers R, $\mathrm{cl}(R)$ is finite.*

Theorem 4.15 (Dirichlet)**.** $\mathcal{O}_L^\times \cong \boldsymbol{Z}^{r_1 + r_2 - 1} \oplus \mathrm{Tor}(\mathcal{O}_L^\times)$. *The latter term are the units of unity, which is also a finite group.*

Question 4.1. When is $P_1^{f_1} \cdots P_k^{f_k} \subseteq q_1^{e_1} \cdots q_\ell^{e_\ell}$?

Move everything to the LHS so that

$$q_1^{-e_1} \cdots q_\ell^{-e_\ell} P_1^{f_1} \cdots P_k^{f_k} \subseteq R.$$

But then $e_i > 0$. I.e. the fractional ideals form a poset.

Furthermore, the isomorphism is an anti-isomorphism of posets.

We state the setup again: let R be Dedekind domain, Q its fraction field, L a finite separable extension, $S = \mathcal{O}_L$. Then for all primes P of S, $q = P \cap R$ is a prime of R, $qS = (P \cap R)S \trianglelefteq S$. Now suppose we have $q' \trianglelefteq R$ such that $q'S \subseteq P$. Then $q'S \cap R \subseteq P \cap R$.

We can show that $q'S \cap R = q'$. Clearly $q' \supseteq q'S \cap R$. Now suppose we have $r \in \mathfrak{q}'S$ that is in R, if $r \notin q'$, then $rR + q' = R$ since q' is maximal. But then $ar + b = 1, a \in R, b \in q'$. Since $ar \in q'S$ and $b \in q'S$, a contradiction.

Thus we can go up and down via $q \mapsto q \cap R$ of $\max(S) \to \max(R)$. Then $p \in f^{-1}(q) \iff qS \subseteq p$. By the theorem, $qS = p_1^{a_1} \cdots p_k^{a_k}$ with $a_i > 0$. By the argument about posets, the fiber of $q \in \max(R)$ is exactly the p_i. With this method, we can find all maximal ideals of S.

Example 4.16. Take $\boldsymbol{Q}(i)$. Then $S = \boldsymbol{Z}[i]$ and $R = \boldsymbol{Z}$. Now we ask how $p\boldsymbol{Z}[i]$ decomposes.

Suppose $p = 3 \pmod 4$. Then p is inert, i.e. $p\boldsymbol{Z}[i]$ is still prime. This is because $\boldsymbol{Z}[i]/p\boldsymbol{Z}[i] = \boldsymbol{F}_p[x]/(x^2+1)$, which is a prime when $p = 3 \pmod 4$.

Now suppose $p = 1 \pmod 4$. In this case, $\boldsymbol{F}_p[x]/(x^2+1)$ is not a field. To fully factor it, we must also quotient out by $(x-a)$ or $(x+a)$ where $a^2 \equiv -1 \pmod 4$. Thus the factorization is $(p, i+a)(p, i-a)$.

Finally, if $p = 2$, then we want to know about $\boldsymbol{F}_2[x]/(x^2+1) \cong \boldsymbol{F}_2[y]/y^2$ via $x \mapsto y + 1$. This is a local ring. Then $(2) = (2, i-1)^2$.

5. 1.27

Let $R = \boldsymbol{Z}$. Then the maximal ideals q in $\mathcal{O}_L$ such that $p\mathcal{O}_L \subseteq q$. We have a map $\boldsymbol{Z}/p\boldsymbol{Z} \to \mathcal{O}_L/q\mathcal{O}_L$. Since $\mathcal{O}_L$ is a free $\boldsymbol{Z}$-module, ($\boldsymbol{Z}$ is a PID), $\mathcal{O}_L/p\mathcal{O}_L$ is an algebra over $\boldsymbol{Z}/p\boldsymbol{Z}$. This only needs R to be a PID.

So to find maximal ideals of S lying over p, take a maximal ideal of q of S/qS. Then $S/q \cong (S/pS)/q$. So we have a map $R/pR \to S/qS$, a field of dimension at most n. Thus S/qS is a field extension of R/pR.

Definition 5.1. Let $f_p = \dim_{R/pR} S/qS$.

Example 5.2. In $\boldsymbol{Z}[i]$, when $p \equiv 3 \pmod 4$, $f_p = 2$, if $p \equiv 1 \pmod 4$, $f_q = 1$, and if $p = 2$, $f_q = 1$.

Definition 5.3. So if we have $p \in \max(R)$, $pS = p_1 \cdots p_n$ with no repeats, we say that p is **unramified** in S or L.

So odd primes are unramified in $\boldsymbol{Z}[i]$.

Proposition 5.4. *The following are equivalent:*

1. *Note that p is unramified iff $qS = \cap p_i = \prod p_i$ where this indices over p_i such that $qS \subseteq p_i$.*
2. *In other words, we can test unramification via $\overline{p}_i \trianglelefteq S/pS \implies \cap \overline{p}_i = 0$.*
3. *Thus S/pS is reduced since the intersection is the nilradical.*

We have a map $S/pS \to \prod S/p_i$. This map is always surjective by Chinese Remainder Theorem. If p is unramified, this is injective, so it is an isomorphism. Thus

Proposition 5.5.

$$\sum_{pR \subseteq qS} f_q \leq n.$$

With equality iff p is unramified.

Definition 5.6. In the quadratic case, there are two possibilities: a prime stays prime, i.e. **inert**. If it splits into two primes, each $f_q = 1$, i.e. **totally split**. This definition makes sense for non-quadratic cases.

Definition 5.7. Take $p \in \max(R)$ and $pS = p_1^{e_1} \cdots p_k^{e_k}$. It **ramifies** if at least one of the e_i's is > 1.

Theorem 5.8.

$$\sum e_q f_q = n.$$

Proof. Note that $pS = p_1^{e_1} \cdots p_k^{e_k}$. We still have that

$$pS = \cap p_i^{e_i}.$$

Then by Chinese Remainder Theorem,

$$S/pS \cong \prod S/p_i^{e_i} S.$$

It suffices to show that $\dim_{R/pR} S/p_i^{e_i} = e_i f_i$ where $f_i = f_{p_i}$. We have a filtration

$$0 \subseteq p^{e-1}/p^e \subseteq p^{e-2}/p^e \subseteq \cdots \subseteq p/p^e \subseteq S/p^e.$$

We can then compute the dimension of S/p^e as

$$\sum_{i=0}^{e-1} \dim p^i/p^{i+1}.$$

Observe that p^i/p^{i+1} is a module over S/p and $\dim S/p = f_p$. So all we need to show is that p^i/p^{i+1} is one dimensional over S/p.

Nothing changes if we replace S by S_p, the localization since S/p is already a field. We have an obvious map

$$p^i/p^{i+1} \to p^i S_p/p^{i+1} S_p.$$

For surjectivity, take $x \in p^i, y \notin p$. Since $y \notin p$, $\exists z \in S$ such that $yz = 1 + a, a \in p$ since p is maximal. Now consider $xz - \frac{x}{y}$. This equals $\frac{x(yz-1)}{y} = \frac{xa}{y} \in p^{i+1} S_p$.

For injectivity, take $x \in P^i \cap p^{i+1} S_p$. Then $x = \frac{a}{b}, b \notin p, a \in p^{i+1}$. We can use unique prime ideal factorization to conclude that $p^{i+1} \mid (x)$. Thus $x \in p^{i+1}$.

So WLOG, S is a local Dedekind domain. But now S is a DVR.

Corollary 5.9. *Being a Dedekind domain is a local condition. Thus being a Dedekind domain is equivalent to being locally a DVR.*

We can show that S is a PID.

We have a map $S^\times \to \mathrm{Div}(S)$. If S is a field, we are done trivially. So S has one maximal ideal, making $\mathrm{Div}(S) \cong \boldsymbol{Z}$. We thus want to show that $S^\times \twoheadrightarrow \boldsymbol{Z}$. I.e., we just need to show that the maximal ideal is principal.

Let $p \trianglelefteq S$. Then $p^2 \subsetneq p$. Take $t \in p/p^2$. This generates p. Then tS has a unique factorization into ideals, namely $p^k, k \geq 0$. Since $tS \subseteq p$ and isn't in p^2. Hence $tS = p$.

Since S is a PID, $p = (t)$ so that $p^i/p^{i+1} = (t^i)/(t^{i+1})$ so that p^i/p^{i+1} has one generator, t^i. $\square$

6. 1.29

Proposition 6.1. *For a multiplicatively closed subset T, $\operatorname{Spec} T^{-1}R \hookrightarrow \operatorname{Spec} R$. Furthermore, $\operatorname{Spec} T^{-1}R = \{P \in \operatorname{Spec} R | P \cap T = \emptyset\}$.*

Proof. Easy □

Question 6.1. What is $\mathrm{IC}_L(T^{-1}R)$ for $T^{-1} = R \setminus \mathfrak{p}$.

Clearly $\mathrm{IC}_L(R) \subseteq \mathrm{IC}_L(T^{-1}R)$. In addition, we also know that $T^{-1}(\mathrm{IC}_L(R)) \subseteq \mathrm{IC}_L(T^{-1}R)$. By rescaling the minimal polynomial of elements in $\mathrm{IC}_L(T^{-1}R)$, $T^{-1}(\mathrm{IC}_L(R)) = \mathrm{IC}_L(T^{-1}R)$.

Thus $T^{-1}S = \mathrm{IC}_L(R_{\mathfrak{q}})$. The prime ideals of $T^{-1}S$ are contained in the prime ideals of S. Elements of $\operatorname{Spec} T^{-1}S$ are those such that P doesn't meet T, i.e. $R \cap P \subseteq \mathfrak{q}$. Since R is a Dedekind domain, $R \cap P = \mathfrak{q}$.

Thus the splitting of primes is a local problem.

Question 6.2. Are the inertial degrees preserved under localization?

Clearly the ramification degrees stay the same. In general, the dimension of S/P is the same dimension as $T^{-1}S/T^{-1}P$ as the filtration from an earlier proof of the sum formula stays the same.

Theorem 6.2. *Assume that $\exists x \in S$ such that $R[x] = S$. Also assume that $f = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ is a minimal polynomial for x. We know that $a_i \in R$ since $x \in S$. The $n = [L : Q]$ because $R[x] = S \implies Q[x] = L$.*

Now take $q \in \max(R)$ and let $\overline{f}$ be the image of f mod q. Since R/q is a field, let $\overline{f} = \prod g_i^{e_i}$ for $g_i \in R/q[T]$. Choose representatives of g_i, $\tilde{g}_i \in R[T]$. Let $p_i \subseteq S$ be such that $p_i = qS + \tilde{g}_i(x)S$. Then

1. *$p_i \in \max(S)$*
2. *$qS = \prod p_i^{e_i}$*
3. *$f_{p_i} = \deg g_i$*

Quick sanity check:

$$\sum \deg g_i \cdot e_i = n.$$

But this is because $f = \prod g_i^{e_i} \pmod P$.

Proof. (1,3) We check $S/p_i = (S/q)/(\tilde{g}_i(x))$. Then $S/q = ((R[T]/f(T))/q)/\tilde{g}_i(T)$. We can reorder to get $((R[T]/q)/\tilde{g}_i(x))/f$. This equals $((R/q)[T]/g_i)/\overline{f} \cong (R/q)[T]/g_i$. Since g_i is irreducible, we are done.

(2) Now we compute $\prod p_i^{e_i}$. We can see that

$$(qS + g_1S)(qS + g_2S) = q^2S + qg_1S + qg_2S + g_1g_2S.$$

We can first see that $\prod p_i^{e_i} \subseteq qS$. The only issue when doing the expansion on the RHS could be with $\prod g_i e^{e_i} S$. We just want to show that $\prod \tilde{g}_i^{e_i} \in qS$. So we look at it mod q: $0 = \overline{f} = \overline{\prod \tilde{g}_i^{e_i}} \in S/q$.

By unique prime factorization, $q = \prod p_i^{e_i'}$ with $e_i' \leq e_i$. But then $\prod_i \tilde{g}_i^{e_i'} \in q$. It follows that $\prod g_i^{e_i'}(x) = 0$ in $S/q = \frac{R/q[T]}{f(T)}$. Thus $f | \prod g_i^{e_i'}$, a contradiction. Hence $e_i' = e_i$. □

Example 6.3. Let D be square free and $D \neq 1 \pmod 4$. Then $\mathcal{O}_{Q(\sqrt{D})} = \boldsymbol{Z} \oplus \boldsymbol{Z}[\sqrt{D}]$. The minimal polynomial is $x^2 - D$. Thus we seek factorizations of $x^2 - D \pmod p$.

If $p \nmid D$ and D is a QR mod p, then (p) splits completely into $(p, a - \sqrt{D})(p, a + \sqrt{D})$ with $a^2 = D \pmod p$.

If $p|D$, then (p) ramifies. Otherwise (p) is inert.

Suppose $p = 2$. Then because D is odd (even case covered earlier), $(2) = (2, \sqrt{D} - 1)^2$.

7. 1.31

Example 7.1. What if $D \equiv 1 \pmod 4$? Then $\mathcal{O}_{\boldsymbol{Q}(\sqrt{D})} = \boldsymbol{Z}\left[\frac{1+\sqrt{D}}{2}\right]$. The minimal polynomial is now $x^2 - x + \frac{1-D}{4}$.

We wish to understand how this splits mod p. If $p = 2$, then if $D \equiv 5 \pmod 8$, (2) is inert. Otherwise, $(2) = (2, \sqrt{D})(2, \sqrt{D} + 1)$.

p is odd: Same as before—depends on whether D is a QR mod p.

Now assume

(1) R is a PID
(2) $\forall q \in \max R$, R/q is perfect, i.e. every finite extension is separable.

So an example is $\boldsymbol{Z}$. Another is $\boldsymbol{F}_p[t]$ and $\boldsymbol{C}[t]$.

Recall that if R is a PID and L/Q is a finite separable extension, we defined

$$\operatorname{disc}_{L/\boldsymbol{Q}} = \det((\operatorname{tr} \alpha_i \alpha_j)) \in R \setminus \{\alpha\}/(R^\times)^2$$

where α_i are a basis. Now take $q \trianglelefteq R$ maximal.

Theorem 7.2. *q ramifies iff $q \mid D_{L/Q}$.*

Proof. We can localize and still keep all the properties we wanted of R in Example 7. Thus the discriminant is still defined, and the basis is still the same as $\operatorname{IC}_L(R_{\mathfrak{q}}) = T^{-1}\operatorname{IC}_L(R)$. Since we can factor

$$(D_{L/R})_q = q_q^i (p_1)_q \cdots (p_k)_q,$$

the discriminant still has the property that $q|D_{L/Q}$. We do this because the discriminants in L/R lives in a different set than L/R_q, so we need to identity them. So WLOG suppose R is local.

Claim 7.1. *If $b_1, \dots, b_n$ is a basis for S over R, iff $\overline{b_1}, \dots, \overline{b_n}$ is a basis of S/q over R/q.*

Proof. If $b_i \in S$ is a basis, then they span S over R, so $\overline{b_i}$ span S/q over R/q. As S/q is n-dimensional over R/q, n spanning vectors are a basis.

For the opposite direction, α_i is a basis for S over R iff $\exists B \in M_N(R)$ such that $B(\alpha_i) = b_i$ and B is invertible. Since $\overline{\alpha}_i$ is a basis for S/q, $\overline{b}_i$ is a basis implies that $\overline{B} \in M_n(R/q)$ is invertible. Thus we have reduced to $B \in M(R)$ is invertible iff $\overline{B} \in M_n(R/q)$ is invertible. Localness is the only thing needed.

We know that B is invertible iff $\det B$ is a unit. This thus reduces the problem to $n = 1$. But $\det B$ is a unit mod q as $\det B \notin q$ (here we use localness).

Thus we can lift $\overline{b}_i$ to a basis of S/q. □

So we have a basis α_i of S over R that is a basis mod q. We want to know $\det((\operatorname{tr}\alpha_i\alpha_j) \pmod q)$. This is the same as $\det((\operatorname{tr}\alpha_i\alpha_j \pmod q))$. But the trace of $S \xrightarrow{\alpha} S$ is the same as the trace of $S/q \xrightarrow{\overline{\alpha}} S/q$. Thus we can compute the traces of $\alpha_i\alpha_j \pmod q$.

For $\alpha_i\alpha_j, i \neq j$, they affect different coordinates mod q of $\prod S/p_i^{e_i}$, so mod q, it is just zero. Thus we are computing the determinant of a block matrix where each block is the trace matrix of $S/p_i^{e_i}$. Since the determinant is zero mod q, one of these blocks has determinant zero mod q. So we reduce to the action on one term of $\prod S/p_i^{e_i}$.

If $e_i = 1$, S/p_i is a finite field extension of R/q. The determinant is non-zero because S/p_i over R/q is non-degenerate by assumption of separableness.

If $e_i > 1$, then because R is local, R is a PID, so we can choose t that generates p_i. Inside $S/p_i^{e_i}$, we have $p_i/p_i^{e_i}$. Since $\dim S/p_i^{e_i} = e_{p_i}f_{p_i}$, $\dim p_i/p_i^{e_i} = f_{p_i}(e_i-1)$. So inside the trace matrix of $S/p_i^{e_i}$ has a block matrix that is $f_i(e_i-1)$ by $f_i(e_i-1)$. Inside this block, the traces of x_ix_j basis elements of $p_i/p_i^{e_i}$ are in $p_i/p_i^{e_i}$. All these elements are nilpotent. Thus the traces are zero, so the trace matrix of $S/p_i^{e_i}$ has three zero blocks, so the determinant is zero.

Hence $q|D$ iff $e_i > 1$ for some i. □

Corollary 7.3. *Since $D_{L/Q} \neq 0$, D_{L/R_q} is divisible by only finitely many primes. Therefore ramification happens at only finitely many primes.*

Example 7.4. The only prime that ramifies in $\boldsymbol{Q}(\zeta_p)$ is p since $D = (-1)^{\frac{p-1}{2}}p^{p-1}$.

8. 2.3

Theorem 8.1 (Dirichlet Unit Theorem)**.** *$\mathcal{O}_L^\times \cong \boldsymbol{Z}^{r_1+r_2-1} \oplus \mu(\mathcal{O}_L^\times)$ where $\mu(\mathcal{O}_L^\times)$ is finite group.*

Proof. Let $\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \ldots, \tau_{r_2}$. We can embed $\mathcal{O}_L^\times \to \boldsymbol{R}^{r_1+r_2}$ via

$$F : a \mapsto (\log|\sigma_1(a)|, \ldots, 2\log|\tau_1(a)|, \ldots, 2\log|\tau_{r_2}(a)|).$$

Obviously the roots of unity are in the kernel.

Lemma 8.2. *Let $C_1, \ldots, C_{r_1+r_2} > 0$. Then $\exists$ finite many $a \in \mathcal{O}_L$ such that $|\sigma_i(a)| \leq C_i$ and $|\tau_i(a)| \leq C_{i+r_2}$.*

Proof. We know that $\mathcal{O}_L \cong \boldsymbol{Z}\alpha_1 \oplus \cdots \oplus \boldsymbol{Z}/\alpha_n$ for some α_i. Let P be the matrix of embeddings as before. Then $(\det P)^2 = D_L$. Take $a = a_1\alpha_1 + \cdots + a_n\alpha_n$. Then

$$\begin{pmatrix} \sigma_1(a) \\ \vdots \\ \sigma_n(a) \end{pmatrix} = P \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Thus

$$P^{-1} \begin{pmatrix} \alpha_1(a) \\ \vdots \\ \alpha_n(a) \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Now take C' larger than any entry in P, C larger than all the $|\sigma_i(a)|, |\tau_i(a)|$. Then the entries of this

$$P^{-1} \begin{pmatrix} \alpha_1(a) \\ \vdots \\ \alpha_n(a) \end{pmatrix}$$

are between $(-nC'C, nC'C)$ so that there are $2nC'C+1$ choices for each a_i. Thus there number of possibilities for a is bounded by $(2nC'C+1)^n$. □

Remark 8.3. The intuition for this is that when $r_2 = 0$, the α_i forms a basis for $\boldsymbol{R}^n$. Then $\mathcal{O}_L$ is a lattice in $\boldsymbol{R}^n$. This lemma shows that the number of lattice points in a bounded shape has finitely many points.

Now take a such that $|\sigma_i(a)| = 1$ and $|\tau_i(a)| = 1$. Then a^k are also in the kernel. There can be only finitely many powers in this kernel by the above lemma. Thus a is a root of unity.

So we have this exact sequence

$$\mu(L) \to \mathcal{O}_L^\times \to \boldsymbol{R}^{r_1+r_2}.$$

The roots of unity in L are also in $\mathcal{O}_L$ since the minimal polynomial has coefficients in $\boldsymbol{Z}$.

Claim 8.1. $a \in \mathcal{O}_L^\times \implies \sum \log|\sigma_i(a)| + 2\sum \log|\tau_i(a)| = 0$

Proof. Pass to the Galois closure. If $x \in \mathcal{O}_L$, then $x \mid N_{L/\boldsymbol{Q}}(x)$ as $N(x)/x$ is a product of the other conjugates.

Then $x \in \mathcal{O}_L^\times$ iff $N(x) = \pm 1$. This is because if x is a unit, $N(x) \in \boldsymbol{Z}^\times = \pm 1$. If $N(x) = 1$, then $x|1$ so that x is a unit.

Thus $a \in \mathcal{O}_L^\times \implies |N(a)| = 1$. Furthermore, $|N(a)| = \prod |\sigma_i(a)| \cdot \prod |\tau_i(a)|^2$. Take the log of both sides to get this result. □

Hence the image of this map lives in a hyperplane V, which has dimension $r_1 + r_2 - 1$. So now we want to show that the image of $\mathcal{O}_L^\times$ in $\boldsymbol{R}^{r_1+r_2}$ is free of rank $r_1 + r_2 - 1$. We want to show that the image is a lattice in V.

Lemma 8.4. *If $\Gamma \subseteq \boldsymbol{R}^d$ is a subgroup that generates $\boldsymbol{R}^d$ as a vector space, then the following are equivalent:*

(1) $\forall \delta \subseteq \boldsymbol{R}^d$ bounded, $|\Gamma \cap \delta| < \infty$
(2) $\exists$ a basis for $\boldsymbol{R}^d$ $b_1, \dots, b_d$ such that $\Gamma = \boldsymbol{Z}b_1 \oplus \cdots \boldsymbol{Z}b_d$.

Proof. (2) $\implies$ (1) is a past lemma.

(1) $\implies$ (2): By assumption, $\exists c_1, \dots, c_d \in \Gamma$ a basis for $\boldsymbol{R}^d$. Now consider $\Gamma_0 = \boldsymbol{Z}c_1 \oplus \cdots \boldsymbol{Z}c_d \subseteq \boldsymbol{R}^d$. This is contained in Γ as well.

Then Γ/Γ_0 is finite. If $a \in \Gamma$, then $a = \sum a_i c_i, a_i \in \boldsymbol{R}$. Then $a_i = \lfloor a_i \rfloor + \delta_i$. So $a \equiv b + \Gamma_0$ when $b = \delta_1 c_1 + \cdots + \delta_d c_d$. This is a bounded set, so there are a finite number of these.

Now let $M = [\Gamma : \Gamma_0]$. Then $M\Gamma \subseteq \Gamma_0 \subseteq \Gamma$. Then $\Gamma_0 \subseteq \Gamma \subseteq \frac{1}{M}\Gamma_0$. Thus Γ is a subgroup of a free group of rank d, so Γ is free of rank $\leq d$. But Γ_0 is a subgroup of Γ of rank d, so Γ is free of rank d.

Finally, the generators of Γ span $\boldsymbol{R}^d$ since Γ spans $\boldsymbol{R}^d$. □

So consider any arbitrary lattice $\boldsymbol{Z}b_1 \oplus \cdots \boldsymbol{Z}b_d \subseteq \boldsymbol{R}^d$. Then we can take $\{b_i\}$, and the parallelipid formed with them is the fundamental parallelogram T. Then $\boldsymbol{R}^d = \bigsqcup_{z \in L}(z + T_{b_1,\dots,b_d})$. In addition, $\text{vol}(T_{b_1,b_d}) = |\det(b_i)|$.

The difference between two choices of bases of the lattice is an invertible matrix over $\boldsymbol{Z}$. Hence the volume of the fundamental parallelogram is invariant, V_L.

Theorem 8.5 (Minkowski's Theorem)**.** *Let $S \subseteq \boldsymbol{R}^d$ be a bounded, symmetric ($S = -S$), convex set. Let L be a lattice. Then if $vol(S) > 2^d vol(L)$, $|S \cap (L \setminus O)|$. This is the optimal bound for $vol(S)$.*

Proof. Take $\frac{1}{2}S$. Its volume is $\frac{1}{2^d}vol(S) > vol(L)$. Claim: $\exists x, y \in \frac{1}{2}S$ distinct s.t. $x - y \in L$. This is sufficient since this implies that $2x, 2y \in S$, $-2y \in S$, so by convexity, $\frac{1}{2}(2x) - \frac{1}{2}(2y) = x - y \in L$. This is non-zero since $x \neq y$. Call $\frac{1}{2}S$ T.

So what we are really trying to show is that if $vol(T) > vol(L)$, $\exists x \neq y \in T$ such that $x - y \in L$. Pick a fundamental parallelogram P. Then dissect T into each part's intersection with othe fundamental parallelograms. I.e. $S = \sqcup_{z \in L}(S \cap (P + z))$. Translate these pieces into P. By the volume hypothesis, there must be two overlapping points. These two points differ by a lattice point by construction. □

Proposition 8.6. *Let S be a symmetric, convex, and have the property that $S = \cap_{i=1}^{\infty} S_i$, $S_{i+1} \subseteq S_i$, $vol(S_i) > 2^d vol(L)$. Then S has a non-trivial lattice point.*

Corollary 8.7. *If S is closed, then consider $S_i' := S_i + B(0, \frac{1}{i})$. Then $S = \cap S_i$ so we get a point.*

Proof. S_1 satisfies the conditions for the regular Minkowski's theorem, so it has a finite number of lattice points, $\{v_i\}$. The same is true for S_2, but the lattice points in S_2 is contained in $\{v_i\}$. Assume FTSOC that for each v_i , $\exists S_i$ such that $v_i \notin S_i$. But since $\{v_i\}$ is finite, $\exists S_i$ such that $v_j \notin S_i \forall j$. Contradiction. □

We want to show that there are finitely many $\alpha \in \mathcal{O}_L^\times$ such that $|\prod \log |\sigma(\alpha)| \prod \log |\tau(\alpha)|| < C$. We have a map $\mathcal{O}_L \to \boldsymbol{R}^{r_1} \oplus \boldsymbol{C}^{r_2} \cong \boldsymbol{R}^n$ given by the embeddings. The image of this is a lattice since $\mathcal{O}_L$ has an integral basis. Thus the intersection with any box has a finite number of elements in $\mathcal{O}_L$, which implies a finite number of elements of $\mathcal{O}_L^\times$ by moving between logs and exponents.

So finally, all we need to prove is that $\operatorname{im} F$ spans $\boldsymbol{R}^{r_1+r_2-1}$. This is because of Lemma 8.4.

We can find $v_1, \dots, v_d \in V$ (the hyperplane) such that they generate V and as a matrix, the sum of rows is 0, the diagonal is positive, the upper triangle is positive, and the lower triangle is negative.

Proof. We are trying to show that they generate V.

Suppose FTSOC $\exists t_1, \dots, t_d \in \boldsymbol{R}$ such that $\sum_i t_i (v_j)_i = 0 \forall j$. This represents a vector T that could span $\langle v_i \rangle^\perp$. We can suppose that not all of the t_i are equal, as otherwise this would be the relation we already know for the plane. WLOG, $t_1 \geq t_2, \dots, t_d$. Thus $(v_1)_1 = -\sum_{i>1} t_i (v_1)_i$.

So $\sum t_i (v_j)_i = t_1(-\sum(v_1)) + \sum_{i>1} t_i (v_j)_i > t_1(-\sum v_i) + t_1 (v_1)_1 = 0$. □

Then for $1 \leq i \leq r_1 + r_2$, $\exists \alpha \in \mathcal{O}_L^\times$ such that $|\sigma_i(\alpha)| > 1, |\sigma_j(\alpha)| < 1$. We have the embedding $\mathcal{O}_L \hookrightarrow \boldsymbol{R}^{r_1} \oplus \boldsymbol{C}^{r_2}$. This is a lattice, which has some volume V. Take the cube bounded by $1, 1, \dots, V$ with V in the i-th coordinate. Then by Minkowski's theorem, we find an element in $\mathcal{O}_L$.

The last thing we need to show is that the image of $\mathcal{O}_L^\times \to V$ spans V. We just need to find one guy in each coordinate is positive (diagonal is positive). This is the same as finding $\alpha \in \mathcal{O}_L^\times$ such that $|\sigma_i(\alpha)| > 1, |\sigma_j(\alpha)| < 1$. We can embed $\mathcal{O}_L \to \boldsymbol{R}^{r_1} \times \boldsymbol{C}^{r_2}$, and we want to understand this as a lattice in $\boldsymbol{R}^{r_1} \times (\boldsymbol{R}^2)^{r_2}$ via

$a + bi \mapsto (a, b)$. Take α_i an integral basis for $\mathcal{O}_L$. The matrix is

$$\begin{bmatrix} \sigma_1(\alpha_1) & \cdots \\ \vdots & \\ \Re\tau_1(\alpha_1) & \\ \vdots & \end{bmatrix}.$$

But we can easily move from P to this related matrix via $\frac{1}{2}\begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix}$. The determinant of this is $\frac{1}{2}$. So the volume of $\mathcal{O}_L$ in $\boldsymbol{R}^{r_1}(\boldsymbol{R}^2)^{r_2}$ is

$$\frac{|\det P|}{2^{r_2}} = \frac{\sqrt{|D_L|}}{2^{r_2}}.$$

Our goal now is to find non-zero $\alpha \in \mathcal{O}_L$ such that $|\sigma_i(\alpha)| < R_i$ and $|\tau_i(\alpha)| < C_i$. The volume is such a region is $2^{r_1}\prod R_i \pi^{r_2} \prod C_i^2$. We need this to be larger than $\frac{\sqrt{|D_L|}}{2^{r_2}} \cdot 2^n$ in order for us to use Minkowski's. Thus

$$\prod R_i \prod C_j^2 > \sqrt{|D_L|}\left(\frac{2}{\pi}\right)^{r_2}.$$

We can strengthen this to a $\geq$ by letting one of the R_i or C_i bounds be a $\leq$. This is because of the strengthened Minkowski's.

Take $M = 2\sqrt{D_L}$. We want to find an α so that one of the coordinates is bigger than one. The following argument will only be for the real coordinates, but a similar one works for complex. Take $R_1 = M$, $R_2 = \ldots, R_{r_1} = 1$. Then we have non-zero $\alpha_1 \in \mathcal{O}_L$ such that $|\sigma_1(\alpha_1)| \leq M$ and $|\sigma_i(\alpha_1)| \leq 1$. Now we find an α_2 that shrinks the non-one coordinates while preserving $|N(\alpha_i)| \leq M$, $\alpha_i \neq 0$, and $\forall i \in [2, n]$, $|\sigma_j(\alpha_{i+1})| \leq |\sigma_j(\alpha_i)|$.

Since $|N(\alpha_i)| \leq M$, there is a value C that repeats infinitely often. Then $\mathcal{O}_L/C\mathcal{O}_L$. This has size C^n. Thus $\alpha_i \equiv \alpha_j \pmod{C}$ happens infinitely often. Now consider $\frac{\alpha_{i+1}}{\alpha_i}$. This equals $\frac{\alpha_i}{\alpha_i} + \frac{\alpha_{i+1}-\alpha_i}{\alpha_i} = 1 + \frac{Cx}{\alpha_i}$ for $x \in \mathcal{O}_L$. Since $C = N(\alpha_i)$, $1 + \frac{Cx}{\alpha_i} \in \mathcal{O}_L$. Hence $\frac{\alpha_{i+1}}{\alpha_i} \in \mathcal{O}_L^\times$ (norm is one and is in $\mathcal{O}_L$.

Furthermore, since $|\sigma_j(\alpha_{i+1})| < |\sigma_j(\alpha_i)|$, $|\sigma_j(\frac{\alpha_{i+1}}{\alpha_i})| < 1$. Hence we have shown it generates V. □

Example 8.8. What happens when $r_1 + r_2 - 1 = 0$?

If $r_1 = 1, r_2 = 0$, then $L = \boldsymbol{Q}$. So Dirichlet's unit theorem tells us that the unit group is a finite group, namely the roots of unity. This is ± 1.

Otherwise, $r_1 = 0, r_2 = 1$, then $n = 2$ so that L is a quadratic extension, namely an imaginary quadratic extension (otherwise no complex embeddings). The only roots of unity in L has to have cyclotomic polynomial with degree ≤ 2. Thus $L = \boldsymbol{Q}(\sqrt{d})$ so that the degree is either $3, 4$ (the 6 case is the same as 3). So there are other roots of unity only if $d = -1$ or -3.

Example 8.9. What if $r_1 + r_2 - 1 = 1$.

Either we have a quadratic extension with 2 real embeddings, cubic with 1 real and 1 pair of complex, and quartic with 2 pairs of complex embeddings.

Now take $r_1 = 2$. Then $L = \boldsymbol{Q}(\sqrt{d})$, Take positive $d \not\equiv 1 \pmod 4$ so that $\mathcal{O}_L = \boldsymbol{Z}[\sqrt{d}]$. Since this is contained in $\boldsymbol{R}$, there are only two roots of unity. But there is an infinite part, namely a rank 1 part with a generator.

In addition, being a unit means we have found $a^2 - db^2 = \pm 1$, so we have found solutions to Pell's equations and there there exists a fundamental one. The fundamental unit is not canonical, but the other solutions just change signs. So we can take $a, b > 0$. We can also embed $\boldsymbol{Z}[\sqrt{d}]$ into $\boldsymbol{R}$ via taking the positive root, so $a + b\sqrt{d} > 1$.

Lemma 8.10. *If $\alpha = a + b\sqrt{d}, a, b \in \boldsymbol{N}$, then $\alpha^n = a_n + b_n\sqrt{d}$. Then $a_{n+1} > a_n$ and $b_{n+1} > b_n$.*

Proof. Straightforward induction. □

Thus if we find a solution, there are only finitely many possibilities to search for when looking for the fundamental one.

Example 8.11. $d = 2$: $a^2 - 2b^2 = \pm 1$.

We have $(1, 1)$. Its inverse if $\sqrt{2} - 1$. This is the fundamental unit. So all the solutions here are obtained from $(1 + \sqrt{2})^n$. Namely $a_n = \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}$, $b_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}$.

We want to understand the cokernel of $L^\times \to \mathrm{Div}(L)$, i.e. the ideal class group. Then for all ideals $I \subseteq \mathcal{O}_L$, $\mathcal{O}_L/I$ is finite, namely $\prod \mathcal{O}_L/P_i^{e_e}$. This has cardinality $\prod |\mathcal{O}_L/P_i|^{e_i}$. Then the map of ideals to $\boldsymbol{Z}_{\geq 0}$ via $I \mapsto |\mathcal{O}_L/I| = [\mathcal{O}_L : I]$ is multiplicative. Thus we can extend this to a map $\mathrm{Div}(L) \to \boldsymbol{Q}^\times_{>0}$.

Definition 8.12. This the **norm** of an ideal.

It satisfies

$$\begin{array}{ccc} L^\times & & \\ \downarrow & \searrow & \\ \mathrm{Div}\, L & \longrightarrow & \boldsymbol{Q}^\times \end{array}$$

We shall consider ideals as a lattice again and use Minkowski again.

9. 2.10

Suppose we have $I \in \mathrm{Div}(L)$. We have the norm map $N : \mathrm{Div}(L) \to \boldsymbol{Q}^\times_{>0}$. Whenever we compare norms via inequalities, there is an absolute value. It has these properties:

(1) $N((\alpha)) = N_{L/\boldsymbol{Q}}(\alpha)$
(2) If $I \subseteq \mathcal{O}_L$, then $N(I) = [\mathcal{O}_L : I]$.
(3) We have a map $L \to \boldsymbol{R}^n$ via

$$\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \Re(\tau_1(\alpha), \Im(\tau_1(\alpha), \dots).$$

(4) If $I \subseteq L$ is a fractional ideal, $i(I)$ is a lattice with volume $\frac{N(I)\sqrt{|D_L|}}{2^{r_2}}$.

Proof. If $i : I \subseteq \mathcal{O}_L$, then this follows from $N(I) = [\mathcal{O}_L : I]$.

In general, if I is a fractional ideal, $\exists \alpha \in \mathcal{O}_L \setminus \{0\}$ such that $\alpha I \trianglelefteq \mathcal{O}_L$. This is by some proposition/lemma from a while ago. Then $\alpha I \subseteq I$ as sublattices, and $\alpha I \subseteq \mathcal{O}_L$. Thus $\mathrm{vol}(\alpha I) = \frac{N(\alpha I) \cdot \sqrt{|D_L|}}{2^{r_1}} = \frac{N(\alpha) N(I) \cdot \sqrt{|D_L|}}{2^{r_1}}$.

But $[I : \alpha I] = [\mathcal{O}_L : \alpha\mathcal{O}_L] = N(\alpha)$ since the index only depends on α as a matrix, not the basis which it acts on. Thus the LHS is $N(\alpha)\text{vol}(I)$ so that

$$\text{vol}(\alpha I) = N(\alpha)\text{vol}(I) = \frac{N(\alpha)N(I) \cdot \sqrt{|D_L|}}{2^{r_1}}$$

and

$$\text{vol}(I) = \frac{N(I) \cdot \sqrt{|D_L|}}{2^{r_1}}.$$

□

Our goal is to show that if I is a fixed ideal, $\exists \alpha \in I$ such that $N(\alpha) \leq N(I) \cdot C$ with C a constant. If $C = 1$, then $(\alpha) \subseteq I$ and both have the same norms, so $I = (\alpha)$. We would like to produce a point in the lattice $i(I)$ inside the region of points such that the product of the coordinates equals $N(I)$. But this region isn't convex. Instead we consider a subregion.

We know that

$$\begin{aligned} |N(\alpha)|^{\frac{1}{n}} &= (|\sigma_1(\alpha)||\sigma_2(\alpha)| \dots |\sigma_{r_1}(\alpha)|(\Re(\tau_1(\alpha))^2 + \Im(\tau_1(\alpha))^2) \cdots)^{\frac{1}{n}} \\ &\leq \frac{|\sigma_1(\alpha)| + \cdots + 2\sqrt{\Re(\tau_1(\alpha))^2 + \Im(\tau_1(\alpha))^2} + \cdots}{n} \end{aligned}$$

by AM-GM. We want to bound the RHS by $N(I)^{\frac{1}{n}} \cdot C^{\frac{1}{n}}$

For $B \in \boldsymbol{R}$ be

$$W_{r_1,r_2}(B) \subseteq \boldsymbol{R}^n \coloneqq \{a_1, \dots, a_{r_1}, x_1, \dots, x_{r_2}, y_1, \dots, y_{r_2} || \alpha_1| + \cdots + |\alpha_{r_1}| + 2\sqrt{x_1^2 + y_1^2} + \cdots \leq B\}.$$

We want to find C such that $\text{vol}(W_{r_1,r_2}(n(N(I))^{\frac{1}{n}} C^{\frac{1}{n}}) \geq 2^n \frac{N(I)\sqrt{|D_L|}}{2^{r_2}}$. The volume of W scales by raising to the n power, so we need C to be

$$\text{vol}(W_{r_1,r_2}(1)) \cdot n^n N(I) \cdot C \geq 2^n \frac{N(I)\sqrt{|D_L|}}{2^{r_2}}.$$

Thus let $C = \frac{2^n \cdot \sqrt{|D_L|}}{2^{r_2}\text{vol}(W_{r_1,r_2}(1))n^n}$.

If $r_2 = 0$, then we get a diamond shape. The volume of this is $\frac{2^{r_1}}{n!}$. For each complex dimension (r_2), we get $\frac{\pi}{4}$ factor in the volume. Thus $C = \sqrt{|D_L|} \cdot \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{r_2}$

Thus for $\alpha \in I$,

$$N(\alpha) \leq N(I) \cdot \sqrt{|D_L|} \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \leq N(I) \cdot \sqrt{|D_L|} \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{\frac{n}{2}}.$$

For $n = 2$, the second term $(f(n) \coloneqq \left(\frac{4}{\pi}\right)^{\frac{n}{2}})$ is $\frac{2}{\pi}$. We can see that

$$\frac{f(n+1)}{f'(n)} = \left(\frac{n}{n+1}\right)^n \cdot \frac{2}{\sqrt{\pi}}.$$

This is always less than 1 since $\left(\frac{n}{n+1}\right)^n \leq \frac{1}{2} < \frac{\sqrt{\pi}}{2}$. Thus $|N(\alpha)| \leq N(I)\sqrt{|D_L|} \cdot \frac{2}{\pi}$.

By picking $I = \mathcal{O}_L$, we get that $1 \leq |N(\alpha)| \leq \sqrt{|D_L|}\frac{2}{\pi}$ so that $\frac{\pi^2}{4} \leq |D_L|$. Thus $3 \leq |D_L|$. As a consequence, any non-trivial extension has non ± 1 discriminant, so there is always a prime that ramifies.

Now consider $\mathrm{Div}(L) \twoheadrightarrow \mathrm{cl}(L)$. Take $[I] \in \mathrm{cl}(L)$. Then $\exists 0 \neq \alpha \in I^{-1}$ such that $N(\alpha) \leq N(I^{-1}) \cdot \sqrt{|D_L|} \cdot \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2}$. We have by definition, $\alpha I \subseteq \mathcal{O}_L$. Thus

$$N(\alpha I) = N(\alpha)N(I) \leq N(I)N(I^{-1})\sqrt{|D_K|}\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}.$$

As $[\alpha I] = [I]$, we realize that $\forall a \in \mathrm{cl}(L)$, $\exists J \trianglelefteq \mathcal{O}_L$ such that

(1) $[J] = a$
(2) $N(J) \leq \sqrt{|D_L|}\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}$

Thus $|\mathrm{cl}(L)|$ is finite.

10. 2.12 Function Fields

Today we will cover Dirichlet's unit theorem for function fields. To do so, we need an analog of r_1, r_2.

Definition 10.1. Let $\mathcal{O}_L^{\pm}$ be the integral closure of $k[t, t^{-1}]$. Let $\mathcal{O}_L^{+}$ be the integral closure of $k[t]$. Let $\mathcal{O}_L^{-}$ be the integral closure of $k[t^{-1}]$. Let μ_L be the roots of unity in L. These are automatically in $\mathcal{O}_L$ for all of them.

We want to compare valuations. We are going to look at $t^{-1}\mathcal{O}_L^{-}$. This factors as $\prod_{i=1}^{r} Q_i^{e_i}$ (and these aren't detectable from pirmes in $k[t]$). These are "primes lying over ∞".

Consider the Riemann sphere. Then the natural functions as an algebraic geometer on $\boldsymbol{P}^1(\boldsymbol{C})$ are $\boldsymbol{C}(t)$. The functions defined everywhere except at infinity, i.e. no pole near 0 (neighborhood being $\boldsymbol{A}^2$), are $\boldsymbol{C}[t]$. The regular functions on $\boldsymbol{P}^1(\boldsymbol{C}) \setminus \{0\}$ are $\boldsymbol{C}[t^{-1}]$ and the regular functions on $\boldsymbol{P}^1(\boldsymbol{C}) \setminus \{0, \infty\}$ are $\boldsymbol{C}[t, t^{-1}]$. Thus the primes lying over ∞ are ones that lie in an affine chart near ∞.

Theorem 10.2 (Dirichlet's Theorem for function fields)**.**

$$\mathcal{O}_L^{+}/\mu_L \cong \boldsymbol{Z}^{r-1}$$

where r is the number of primes lying over ∞ for k a finite field. The statement for non-finite fields is

$$\mathcal{O}_L^{\times}/(\textit{algebraic points over } k) \cong \boldsymbol{Z}^{r-1}.$$

Proof. We want to make a map $\phi : \mathcal{O}_L^{\times} \to \boldsymbol{Z}^r$ and find that it lives in a hyperplane. Take $f \in \mathcal{O}_L^{\times}$ and let $f\mathcal{O}_L^{-} = \prod Q_i^{a_i}$. Let $\phi(f) = (a_1, \ldots, a_r)$. The norm of f is in $(k[t])^{\times}$, i.e. $N(f) \in k$. Thus the degree of $N(f) = 0$.

We can then see that $f\mathcal{O}_L^{-} = \prod \beta_i^{e_i'}$ with each β_i lying over p_i primes in $k[t^{-1}]$. Since $f \in \mathcal{O}_L^{\times}$, no primes in $k[t]$ can show up as one of the p_i. This is because $N(f) = \prod p_i^{e_i' f_i}$ has degree equalling $\sum e_i' \cdot \deg(p_i) \cdot f_i$. It turns out that the p_i are the only guys in the fractional factorization of f, so each $\beta_i = Q_i$. Thus $\deg N(f) = 0 = \sum e_i a_i \cdot (-1) f_i$, since the degree of p_i is -1 (p_i is $\frac{1}{t}$). Thus $\operatorname{im}\phi$ lives in a hyperplane.

We now wish to compute $\ker\phi$.

Lemma 10.3. *If $k = \boldsymbol{F}_q$ is finite, any algebraic element over k is a root of unity.*

Proof. Take g an algebraic element over k. Then $k[g]$ is a finite field, so $g^{|k[g]|-1} = 1$. □

Claim 10.1. $\ker\phi$ *is the set of roots of unity.*

Proof. Take $f \in \ker \phi$. We can see that $0 = \operatorname{ord}_{\beta_i}(f)$ for β_i lying over a prime in $k[t]$. In addition, $0 = \operatorname{ord}_{Q_i}(f)$ for Q_i lying over (t^{-1}). Thus $f \in \mathcal{O}_L^-$. Furthermore, $f \in \mathcal{O}_L^+ \cap \mathcal{O}_L^-$. Thus f is integral over $k[t]$ and $k[t^{-1}]$.

So the minimal polynomial of f is $\sum c_i T^i$ with each $c_i \in k[t], c_i \in k[t]^{-1}]$. Thus $c_i \in k$. Hence f is algebraic over k and is thus a root of unity. □

Finally, the last step is to find $r-1$ linear independent vectors in $\operatorname{im} \phi$, as this will show that $\mathcal{O}_L^\times / \mu_L \cong \phi(\mathcal{O}_L^\times) \cong \boldsymbol{Z}^{r-1}$. Our proof will use algebraic geometry.

The image of ϕ being full rank is equivalent to the cokernel of ϕ inside H is finite. Let H be the hyperplane. We know that $H = \{(a_1, \dots, a_r) | \sum e_i a_i f_i = 0\}$. Furthermore, such tuples come from a factorization of $f \in \mathcal{O}_L^\times$.

Given a function field $L/k(t)$, we can define a group $\operatorname{Div}(L)$ as $\sum_p a_p p$ where $p \in \operatorname{Spec} \mathcal{O}_L^+$ or $\mathcal{O}_L^-$ with $a_p \in \boldsymbol{Z}$. We have a subgroup $\operatorname{Div}^0(L)$ of divisors such that $\deg D = 0$ where $\deg D = \sum a_p \deg p$. We also define $\operatorname{Div}_-^0(L) \subseteq \operatorname{Div}^0(L)$ to divisors supported on primes over ∞ and $P(L)$ to be principal divisors.

Theorem 10.4 (Riemann-Roch)**.** *The last part of the theorem is equivalent to* $\operatorname{Div}_-^0(L)/P_-(L)$ *being finite. This theorem says this as a corollary.*

The cokernel of ϕ is exactly $\operatorname{Div}_-^0(L)$ and $\operatorname{im} \phi$ is exactly $P_-(L)$.

The meaning of Riemann-Roch is that given a divisor D, the set

$$L(D) = \{g \in L^\times : (g) + D \geq 0 \text{ everywhere}\}$$

and by everywhere we mean that $\sum c_p \geq 0$ where the c_p are the coefficients of $(g) + D$. I.e. there are no poles anywhere. E.g. $D = 5(0) - 2\infty$ means at most 5 poles at 0 and it needs two roots at ∞.

If we let $\ell(D) = \dim_k L(D)$, then the theorem states that

$$\ell(D) \geq \deg(D) + 1 - g$$

where g is some constant depending only on L.

Lemma 10.5. *The number of divisors $D \geq 0$ such that $\deg D = n$ is finite for $K/k(t)$ and k a finite field.*

Proof. The primes in $k[t]$ or $k[t^{-1}]$ are either monic irreducibles or (t^{-1}). For each prime in $k[t]$ or $k[t^{-1}]$, only finitely many lie over it. We know that B/p for p a prime in $k[t]$ or $k[t^{-1}]$, $\deg B = \deg p \cdot$ non-zero integer. Thus $\deg \sum c_\beta \cdot \beta = \sum c_\beta \deg \deg p \cdot$ non-zero integer. We know that $c_\beta \geq 0$. In order for the degree to be $\leq n$, there are a finite number of possibilities for c_β. There are only finitely many monic irreducibles with degree $\leq n$. □

Now we can see that $\operatorname{Div}_-^0(L)/P_-(L) \subseteq \operatorname{Div}^0(L) \subseteq P(L)$. Fix any divisor D of degree 1, for a divisor A of deg 0, $\deg gD + A = g \implies \ell(gD + A) \geq 1$. Thus $B \coloneqq gD + \tilde{A} + (h) \geq 0$ for $h \in L^\times$ so that $A \equiv B - gD$. Then B is an effective divisor (coefficients being ≥ 0) of bounded degree. A reference is Rozin. □

11. 2.14 Some Computations

Example 11.1. Consider $\boldsymbol{Q}(\sqrt{-7})$. Then $d_L = -7$, $r_1 = 0$, $r_2 = 1$, $n = 2$. Thus $|\operatorname{cl}(L)| \leq \sqrt{7} \cdot \frac{2}{4} \cdot \frac{4}{\pi}$. This upper bound is less than 2, so $|\operatorname{cl}(L)| = 1$ so we learn that $\boldsymbol{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ is a PID.

Example 11.2. Consider $L = \boldsymbol{Q}(\sqrt{-15})$. Then $N(J) \leq 2$. Since the ideal norm is multiplicative, it suffices to consider prime ideals with norm 2. But the only such are the ones lying over 2.

So we wish to know how 2 factors in $\boldsymbol{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$. The minimal polynomial of $\frac{1+\sqrt{-15}}{2}$ is $x^2 - x + 4$. Mod 2, this splits, so 2 splits. Therefore there are two primes lying over 2, and because $N(2) = 4$, $N(p_i) = 2$. Thus these are the only ideals with norm 2.

Now we wish to find out whether p_i is principal. Suppose $p_i = (\alpha)$. Then $|N(\alpha)| = N(p_i) = 2$. Since $\alpha = a + b\frac{1+\sqrt{-15}}{2}$, $N(\alpha) = a^2 + ab + 4b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{15}{4}b^2$. We want to know if this can equal 2. If $b = 1$, then we already get a contradiction. Thus $b = 0$, and we get that $a^2 = 2$, a contradiction. Thus p_i is not principal.

So we know that there is a non-trivial element in $\mathrm{cl}(L)$. We also know that p_2 is non-trivial. Thus $\mathrm{cl}(L) = \frac{\boldsymbol{Z}}{2\boldsymbol{Z}}$ or $\boldsymbol{Z}/3\boldsymbol{Z}$.

We can see that $p_1^2 \neq (2)$ since 2 doesn't ramify (it doesn't divide d_L). Finally, we know that $\left(\frac{1+\sqrt{-15}}{2}\right) = p_1^2$, p_2^2, or $p_1 p_2$. The latter is 2, so it can't equal $\left(\frac{1+\sqrt{-15}}{2}\right)$. Thus $\left(\frac{1+\sqrt{-15}}{2}\right) = p_1^2$. Since we have an order 2 element, $\mathrm{cl}(L) = \boldsymbol{Z}/2\boldsymbol{Z}$.

We also know that $\mathcal{O}^\times_{\boldsymbol{Q}(\sqrt{-15})} = \pm 1$ by Dirichlet's unit theorem. So we have

$$0 \to \boldsymbol{Z}/2\boldsymbol{Z} \to \boldsymbol{Q}(\sqrt{-15})^\times \to \mathrm{Div}(L) \to \boldsymbol{Z}/2\boldsymbol{Z} \to 0.$$

Recall that $W_{r_1,r_2}(B) = \mathrm{vol}((a_1, \ldots, a_{r_1}, x_1, y_1, \ldots, x_{r_2}, y_{r_2}) \in \boldsymbol{R}^n | \sum |a_i| + 2\sum \sqrt{x_i^2 + y_i^2})$. We know that $W_{r_1,r_2}(B) = B^n W_{r_1,r_2}(1)$. We can divide up $W_{r_1,r_2}(1)$ into quadrants to reduce to computing $2^{r_1} V_{r_1,r_2}(B)$ where V has all positive coordinates. We know that

$$V_{r_1,r_2}(1) = \int_0^1 V_{r_1-1,r_2}(1-u_1)du_1 = \int_0^1 (1-u_1)^{n-1})du_1 V_{r_1-1,r_2}(1) = \frac{1}{n} V_{r_1-1,r_2}(1).$$

So we have

$$V_{r_1,r_2}(1) = \frac{1}{n(n-1)\cdots(n-(r_1-1))} V_{0,r_2}(1).$$

By using polar coordinates $(l_1, \ldots, l_{r_2}, \theta_1, \ldots, \theta_{r_2})$, we get that

$$\int_B 1 = \int_{0 \leq \theta \leq 2\pi, \sum l_i = 1} 1 \frac{1}{4^{r_2}} l_1 \cdots l_{r_2} = \frac{(2\pi)^{r_2}}{4^{r_2}} \int_{\sum l_i \leq 1} \prod l_i.$$

We split this integral vis a via Fubini's theorem to get $\prod \frac{1}{2r_i(2-1)}$. Everything comes together to get the $n!$.

There can be better convex shapes inside the region that gives us better bounds.

12. 2.17 Kummer's Theorem

We shall show specific cases of Fermat's Last Theorem.

It is enough to prove it for $n = p$ an odd prime and $n = 4$. This is because

$$x^n + y^n = z^n$$
$$(x^m)^p + (y^m)^p = (z^m)^p$$

where $n = pm$. Otherwise, $n = 2^k$ so that

$$(x^{2^{k-2}})^4 + (y^{2^{k-2}})^4 = (z^{2^{k-2}})^4.$$

We shall prove Fermat's Last Theorem for regular primes.

Definition 12.1. The **class number** is $|\operatorname{cl}(L)|$, n_L.

Definition 12.2. A prime p is regular if $p \nmid n_{\boldsymbol{Q}(\zeta_p)}$.

The first irregular prime is 37 and there are only two more up to 100!

Example 12.3. Consider $n = 2$, so that Fermat's Last Theorem doesn't work. So take $x^2 + y^2 = z^2$.

We first reduce to the case where x, y, z are pairwise coprime. This is easy. Then we can factor $x^2 + y^2$ as $(x + yi)(x - yi)$.

z is odd: then 2 is prime to z^2. Hence no prime ideal factor $(x \pm iy)$ lies over 2. Then notice that $x+iy+x-yi = 2x$ and $x+iy-(x-iy) = 2iy$, so if $x+iy, x-iy$ share a common factor, that factor divides $2x, 2iy$. But this is impossible since x, y are pairwise coprime and no factor of $x \pm iy$ divides 2. Therefore $x+iy$ is relatively prime to $x - yi$. Thus $x+iy$ is, up to a unit, a square. Because ± 1 are squares, we know that $x + iy$ is either i times a square or is a square. If $x + iy = i\alpha^2$, we have $y - ix = \alpha^2$. By permuting if necessary, we can WLOG suppose that $x + iy = \alpha^2$. Thus $x = m^2 - n^2$ and $y = 2mn$ for $m, n \in \boldsymbol{Z}$ where $\alpha = m + ni$.

z is even: Then x, y are both odd. Then $(x + iy)(x - iy)$ is divisible by 4. No factor on the left is divisible by 2, as otherwise x, y are even. Thus $1 + i \mid (x + iy)$, and divides it at most once. The same is true for $x - iy$. But we need a power of 4 to get that $(x + iy)(x - iy)$ is divisible by 4.

Question 12.1. What are the z such that $x^2 + y^2 = z$. Then $z = N(\alpha), \alpha \in \boldsymbol{Z}[i]$. We can factor α as $p_1^{k_1} \dots$ so that $N(\alpha) = \prod N(p_i)^{k_i}$. Since $N(p) = p^2$ for $p \equiv 3 \pmod 4$, $N(1 \pm i) = 2$, and $N(p_1) = p$ for $p \equiv 1 \pmod 4$ and $p_1 p_2 = p$. So z is a sum of two squares iff the primes 3 mod 4 in it are to even powers (the p_1, p_2 must come in pairs since z is an integer).

Theorem 12.4. *Fermat's Last Theorem is true for n an odd regular prime.*

Proof. Since p is odd, we can look to find no solutions to $x^p - y^p = z^p$. Suppose FTSOC there was a solution. Then the LHS is $\prod(x - \zeta^i y)$ where $\zeta = \zeta_p$. So we have $\prod(x - \zeta^i y) = z^p$.

Any prime factor of z has to appear in the LHS p times. But we hope that they all land in one factor.

So we hope to show that each factor is relatively prime. Let $a_i = x - \zeta^i y$ and $a_j = x - \zeta^j y$ for $i \neq j$. Then $\frac{a_i - a_j}{\zeta^j - \zeta^i} = y$ Solving for x, we get $\frac{a_i - \zeta^{i-j} a_j}{1 - \zeta^{i-j}}$. Thus only way that a_i, a_j can fail to be relatively prime is that it divides $\zeta^{i-j} - 1$. Let $\ell = i - j$.

By conjugating, the norm of $N(\zeta^\ell - 1)$ are all the same. Thus we want to compute $N(1 - \zeta)$. This norm is p since it is $\phi(1)$ where ϕ is the minimal polynomial of ζ. Since the discriminant is p^{p-2}, p ramifies.

We want to know how p factors, and we do so by factoring $\phi(x)$. Then $\phi(x) = \frac{x^p - 1}{x - 1} = \frac{(x-1)^p}{x-1} = (x - 1)^{p-1}$. Thus (p) ramifies into $p - 2$ prime ideals. Say $p\boldsymbol{Z}[\zeta_p] = \tilde{p}^{p-1}$.

We have that $\tilde{p}$ is principal iff there is an element of norm p, since taking norms of both sides $p\boldsymbol{Z}[\zeta_p] = \tilde{p}^{p-1}$ forces $N(\tilde{p}) = p$. For the inverse, if we have α of norm p, then (α) factors as $\prod p_i^{e_i}$. We take the ideal norm of both sides to force the prime ideals pying over non p primes to be zero powers and the power of $\tilde{p}$ to be 1 (as $\tilde{p}$ is the only prime lying over p).

We have an element of norm p, $1-\zeta$. Thus $(1-\zeta) = (1-\zeta^2) = \cdots$. Thus $\frac{1-\zeta^i}{1-\zeta^j}$ is a unit in $\boldsymbol{Z}[\zeta]$. Hence the potential only common factor of a_i, a_j is $1-\zeta$. But then $1-\zeta \mid z$ so that $p \mid z$.

So suppose $p \nmid z$.

As each $x-\zeta^i y$ are coprime to each other and z^p is a p-th power, then $(x-\zeta^i y) = I^p$ for $I \mid (x-\zeta^i y)$. But then $[I^p] = 0$ so that $p \mid |\operatorname{cl}(L)|$, contradicting our assumption of p's regularity.

If we have $p \nmid z$, then so far we have shown that $(x-\zeta^i y) = u_i t_i^p$ for some $t_i \in \boldsymbol{Z}[\zeta]$. Now we look at things mod p: $\boldsymbol{Z}[\zeta]/p \cong \boldsymbol{Z}[t]/(\phi, p) = \boldsymbol{F}_p[t]/\phi$. The first term is the same as $\boldsymbol{Z}[1-\zeta]/p = \boldsymbol{F}_p[s]/s^{p-1}$. In this ring, raising anything to the p power annihilates the s terms. Observe that $x-\zeta y = x-y+(1-\zeta)y$.

We use what we have shown before to see that $x-\zeta y = u_1 t_1^p$ and $x-\zeta^{p-1}y = u_{p-1}t_{p-1}^p$. These two equations are complex conjugates of each other, so $t_1 = \overline{t_{p-1}}$. As $t_1^p \equiv t_{10} \equiv t_{p-1,0} \equiv t_{p-1}^p$. We know that $\frac{u_1}{u_{p-1}} \in \boldsymbol{Z}[\zeta]^\times$, and because $u_1 = \overline{u_{p-1}}$, the absolute value of $\frac{u_1}{u_{p-1}}$ is one. Thus $\frac{u_1}{u_{p-1}}$ when decomposed into $\mu \oplus \boldsymbol{Z}^{\frac{p-3}{2}}$ has no terms from the free part. Thus $\frac{u_1}{u_{p-1}} = \pm\zeta^i$. So by equating, $(x-\zeta y) = \pm\zeta^i(x-\zeta^{p-1}y) \pmod p$. This is a contradiction, since the powers of ζ form a basis of $\boldsymbol{Z}[\zeta]/p$ and $p \nmid x$ nor $p \nmid y$ (by symmetry) The only cases of overlapping basis vectors are when $i = 1, 2$.

If $i = 1$, $x-\zeta y = \pm\zeta x - y$. If $x-\zeta y = \zeta x - y$, then $x = -y \pmod p$. But then $p \mid x^p - y^p = z^p$, a contradiction.

If $i = 2$, $x-\zeta y = \pm\zeta^2 x - \zeta y$. In this case, this implies that $p \mid x$, a contradiction.

Now suppose $p \mid z$. Let n be the largest power of p that divides z. Then $x^p + y^p + p^{np} z_0^p = 0$. Since $(p) = (1-\zeta)^{p-1}$, $p = \Sigma(1-\zeta)^{p-1}$ for $\Sigma \in \boldsymbol{Z}[\zeta]^\times$. So as elements of $\boldsymbol{Z}[\zeta]$,

$$\alpha^p + \beta^p + \Sigma(1-\zeta)^{pm}\gamma^p = 0$$

where $m = (p-1)r$. We shall prove that there is no solution with $1-\zeta \mid \alpha\beta\gamma$ with $\Sigma \in \boldsymbol{Z}[\zeta]^\times$.

Translating to ideals, $\prod(\alpha+\zeta^i\beta) = (\alpha^p+\beta^p) = (1-\zeta)^{pm}(\gamma)^p$.

Suppose $m = 1$. Then we have to distribute p terms of $1-\zeta$ across $\prod(\alpha+\zeta^i\beta)$. If each term in the product has exactly one $(1-\zeta)$, then $\alpha+\zeta^i\beta = (1-\zeta)u$ for some $u \in \boldsymbol{Z}[\zeta]$. Then notice that $\boldsymbol{Z}[\zeta]/(1-\zeta)^2 \cong \boldsymbol{Z}[\zeta]/(p,(1-\zeta)^2) \cong \boldsymbol{F}_p[1-\zeta]/(1-\zeta)^2 \cong \boldsymbol{F}_p[s]/s^2$. So $\alpha+\zeta^i\beta = u_i s \in \boldsymbol{Z}[\zeta]/(1-\zeta)^2$ for $u_i \in (\boldsymbol{Z}[\zeta]/(1-\zeta)^2)^\times$. As i varies, we know that there must be j such that $\alpha+\zeta^i\beta = \alpha+\zeta^j\beta \pmod{(1-\zeta)^2}$ since there are $p-1$ choices for u_i and p terms. Thus $(\zeta^i-\zeta^j)\beta = 0 \pmod{(1-\zeta)^2}$ so that $(1-\zeta^{j-i})\beta = 0 \pmod{(1-\zeta)^2}$. But since $(1-\zeta) = (1-\zeta^{j-i})$, $(1-\zeta) \mid (\beta)$, contradiction. Therefore none of them are divisible exactly once.

If one of them has multiplicity, then $\alpha+\zeta^i\beta = 0 \pmod{(1-\zeta)^2}$. If two of the indices have this property, then their difference is divisible by $(1-\zeta)^2$, forcing β to be divisible by $(1-\zeta)$.

This argument works for $m \geq 2$ to allow us to conclude that the Pidgeonhole principle forces $(1-\zeta)^2$ into exactly one term, say it is the j-th, and the rest are divisible exactly once by $(1-\zeta)$. WLOG, we can assume that $j = 0$ by multiplying β by powers of ζ. Thus $\alpha+\beta = 0 \pmod{(1-\zeta)^{pm-(p-1)}}$ but not more powers.

Let $(\alpha, \beta) = g$. $\square$

13. 2.24

Today we will be working in a Galois extension $L/\boldsymbol{Q}$. In this case, $efr = n$.

Proposition 13.1. *The Galois group action on the primes lying over an integral prime is transitive.*

Proof. Suppose otherwise, that $\sigma(q_1) \neq q_2$ for all σ. By CRT, there exists x such that $x \equiv 0 \pmod{q_1}$ and $x \equiv 1 \pmod{\sigma(q_2)}$ for all σ. Then $N(x) = \prod \sigma(x) \in R \cap q_1$. But this is contained in q_2, implying that by primeness, one of the $\sigma(x) \in \sigma(q_2)$, a contradiction. □

Definition 13.2. The **decomposition group** of q, G_q is the stabilizer of G on q.

Then $G_{q'}$ is conjugate to G_q and all the conjugate subgroups also are the stabilizer of a prime. The fixed subfield of L is called L^ℓ. Then L/L^ℓ is Galois with Galois group G_q. Furthermore, $[L : L^\ell] = ef$ and $[L^\ell : \boldsymbol{Q}] = r$.

The number of primes lying over q^d is one, because G_q acts transitively on the primes lying over q^d, and G_q fixes q. Furthermore, S^d is the smallest integral extension in which q lies over only one prime (if there was $\sigma \in H = \mathrm{Gal}(E/\boldsymbol{Q})$ that isn't in G_q, then σq is also over $\mathcal{O}_E \cap q$ but isn't q. Thus by reversing the order, we get that $L^\ell \subseteq E$). Thus $q^d S = q^{e'}$. We have $R/p \to S^d/q^d \to S/q$. Call the degree of this latter map f'. By considering L/L^ℓ, we get that $e'f' = [L : L^\ell] = ef$.

We want $f' = f, e' = e$. It is enough to show that $R/p \cong S^d/q^d$. As they are both fields, it suffices to show that the map is a surjection. So take $x \in S^d$. We want to find $z \in R$ such that $z = x \pmod{q^d}$. Our plan is to find $y \in S^d$ such that $N(y) = x \pmod{q^d}$.

We know that $N_{L^\ell/\boldsymbol{Q}}(y) = y \prod \sigma y$ with $\sigma \in G/G_q$ where these are the non-trivial cosets. Now take $y \equiv x \pmod{q^d}$ and $y \equiv 1 \pmod{\sigma(q^d)}$ for all $\sigma \notin G_q$. Then the norm of y is $x \bmod q^d$. Thus $R/p \cong S^d/q^d$, implying that $f_{L^\ell/\boldsymbol{Q}} = 1$ and $e_{L^\ell/\boldsymbol{Q}} = 1$ (the latter is because if p ramified in L^ℓ, then we would have ramification degree $2e$ in L, a contradiction).

We also know that G_q acts on S/q.

Proposition 13.3. *We claim that if S/q is Galois over R/p, then $G_q \to \mathrm{Aut}((S/q)/(R/p))$ is surjective, and furthermore p is unramified iff the map is a bijection.*

Proof. If the map is surjective, then a group of ef size maps to a group of f size, so $e = 1$.

WLOG, we can replace $\boldsymbol{Q}$ with L^ℓ so that $G_q = G$. Take $x \in S/q$ such that $R/p(x) = S/q$. Take $\tilde{x} \in S$ such that $\tilde{x} \pmod{q} = x$ and let f be the minimal polynomial of $\tilde{x}$. Then $f(\tilde{x})$ is mod p the minimal polynomial for x. Then $f = \prod(t - \tilde{x_i})$. So we can switch the image of the roots around via the Galois group action. Thus S/q over R/p is Galois. □

14. 2.26

Definition 14.1. The kernel of $G_q \to \mathrm{Gal}((S/q)/(R/p))$ is called I_q, the **inertial group**.

Thus p is ramified if $|I_q| \neq 1$.

Example 14.2. Let $R = \boldsymbol{Z}$. Then $\forall p \nmid D$, $\mathrm{Gal}(\mathcal{O}_L/q/\boldsymbol{F}_p) = \boldsymbol{Z}/f\boldsymbol{Z}$ with a canonical generator: the Frobenius Fr_q. For a different prime q', $\mathrm{Fr}_{q'}$ is conjugate to Fr_q because $\sigma(q) = q'$ gives us $\mathrm{Fr}_{q'} = \sigma \,\mathrm{Fr}_q\, \sigma^{-1}$.

Example 14.3 (Σ_3 Galois extension)**.** Let $L = \boldsymbol{Q}(\sqrt{-3}, \sqrt[3]{(2)})/\boldsymbol{Q}$. This is Galois, being the splitting field of $X^3 - 2$ ($\zeta_3 \in L$).

We have a sub quadratic field, so we have an integral basis $1, \zeta_3$ for $\mathcal{O}_{\boldsymbol{Q}[\sqrt{-3}]}$. Furthermore, we have a basis of L over $\boldsymbol{Q}(\sqrt{-3})$ being $1, \sqrt[3]{2}, \sqrt[3]{4}$. So a potential basis is $1, \zeta_3, \sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \sqrt[3]{4}, \zeta_3\sqrt[3]{4}$.

The matrix P is then $P_{\boldsymbol{Q}(\sqrt{-3})} \otimes P_{\boldsymbol{Q}(\sqrt[3]{2})}$. So the determinant of this is $\det(P_{\boldsymbol{Q}(\sqrt{-3})})^{[L_2:\boldsymbol{Q}]} \det(P_{\boldsymbol{Q}(\sqrt[3]{2})})^{[L_1:\boldsymbol{Q}]}$. This is $(-3)^3 \cdot (-27 \cdot 4)^2 = -3^9 \cdot 2^4$. So the only primes that could ramify are $2, 3$. We know for sure that 3 ramifies, because the real discriminant differs by a square, and the power of 3 is odd. Hence 3 definitely divides the discriminant. Furthermore, 2 also ramifies because $X^3 - 2$ is an Eisenstein polynomial for 2, so the index isn't divisible by 2.

We want to understand the frobenius element, so we look at conjugacy classes in Σ_3. There are three.

Now take $p \neq 2, 3$. Then p is either split or inert. We know that p cannot be inert, because then the decomposition group would be Σ_3, but the decomposition group is cyclic. If $p = q_1 q_2$, then the Frobenius is a 3 cycle. If $p = q_1 q_2 q_3$, then the Frobenius is a 2 cycle. And if p splits completely, then the Frobenius is the identity.

Next, we look at how $p \neq 2, 3$ factors in $\boldsymbol{Q}(\sqrt{-3})$. Then if (p) is inert in $\boldsymbol{Q}(\sqrt{-3})$, then (p) has to split into 3 pieces (it can't be inert) because the degree of $L/\boldsymbol{Q}(\sqrt{-3})$ is 3. This behavior depends on whether -3 is a square mod p. In $\boldsymbol{Q}(\sqrt[3]{2})$, the behavior depends on whether 2 is a cube mod p. If 2 isn't a cube, then p splits into two primes in L.

Theorem 14.4 (Chebotarev Density Theorem)**.** *Let $L/\boldsymbol{Q}$ be Galois with Galois group G, $C \subseteq G$ be a conjugacy class, for x let $A_x^C = \#\{p \text{ prime } | p \text{ is unramified }, \mathrm{Fr}_p \in C\}$. Then*

$$\frac{A_x^C}{\#\{p \text{ prime } | p < x\}} \to \frac{\#C}{\#G}.$$

Example 14.5. Take $\boldsymbol{Q}(\sqrt{-3})$. Then $G = \boldsymbol{Z}/2\boldsymbol{Z}$. Then (p) is inert iff p is 2 mod 3. So Chevotarev tells us that half the primes are 1 mod 3 and the other half is 2 mod 3.

Example 14.6. Take $y^2 = x^3 - ax + b$ and $\boldsymbol{C}[x][y]$. There is a map into $\boldsymbol{C}$ with fibers bounded in size by 3. Here, $(x - \lambda) = \prod q_i^{e_i}$. Since S/q_i is finite over $R/(x - \lambda) = \boldsymbol{C}$, there is just ramification.