Algebraic Number Theory Lecture Notes

Lecturer: Bianca Viray; written, partially edited by Josh Swanson

December 9, 2015

Abstract

The following notes were taking during a course on Algebraic Number Theorem at the University of Washington in Fall 2015. Please send any corrections to `jps314@uw.edu`. Thanks!

Contents

September 30th, 2015: Introduction—Number Fields, Integrality, Discriminants . . . 2

October 2nd, 2015: Rings of Integers are Dedekind Domains . . . 4

October 5th, 2015: Dedekind Domains, the Group of Fractional Ideals, and Unique Factorization . 6

October 7th, 2015: Dedekind Domains, Localizations, and DVR's . . . 9

October 9th, 2015: The ef Theorem, Ramification, Relative Discriminants . . . 11

October 12th, 2015: Discriminant Criterion for Ramification . . . 13

October 14th, 2015: Draft . . . 15

October 16th, 2015: Draft . . . 17

October 19th, 2015: Draft . . . 18

October 21st, 2015: Draft . . . 20

October 23rd, 2015: Draft . . . 22

October 26th, 2015: Draft . . . 24

October 29th, 2015: Draft . . . 26

October 30th, 2015: Draft . . . 28

November 2nd, 2015: Draft . . . 30

November 4th, 2015: Draft . . . 33

November 6th, 2015: Draft . . . 35

November 9th, 2015: Draft . . . 38

November 13th, 2015: Draft . . . 40

November 18th, 2015: Draft . . . 42

November 20th, 2015: Draft 43

November 23rd, 2015: Draft 46

November 25th, 2015: Draft 48

November 30th, 2015: Draft 50

December 2nd, 2015: Draft 52

December 7th, 2015: Draft 54

December 9th, 2015: Draft 57

List of Symbols **60**

Index **62**

September 30th, 2015: Introduction—Number Fields, Integrality, Discriminants

1 Remark

This is a course in algebraic number theory. An undergraduate course in elementary number theory studies $\mathbb{Z}$ and primes–for instance, there are infinitely many primes, even of the form $4k+3$, $8k+5$, etc., and in fact:

2 Theorem (Dirichlet)

For any $a, n \in \mathbb{Z}^+$ *with* $\gcd(a,n) = 1$, *there are infinitely many primes congruent to* a *mod* n.

Dirichlet's theorem essentially identifies linear polynomials in one variable (namely $a+nx$) which produce infinitely many primes. Question: what are the primes of the form $x^2+ny^2 = (x+\sqrt{-n}y)(x-\sqrt{-n}y) \in \mathbb{Z}[\sqrt{-n}]$? This naturally leads to the study of rings of the form $\mathbb{Z}[\sqrt{-n}]$. Algebraic number theory is primarily interested in the following objects:

3 Definition

A $\boxed{\text{number field}}$ is a finite degree field extension of $\mathbb{Q}$. If K is a number field, the $\boxed{\text{ring of integers}}$ $\boxed{\mathcal{O}_K}$ of K is the set of elements of K integral over $\mathbb{Z}$, i.e. those which satisfy a monic polynomial over $\mathbb{Z}[x]$.

Course texts: Osserman's notes; supplemented with some material from Lang, Neukirch, and Stein.

4 Aside

There are some closely related objects that won't make much of an appearance in this class. Let R be a commutative domain with fraction field F and suppose A is a finite-dimensional F-algebra. An $\boxed{R\text{-order}}$ $\boxed{\mathcal{O}}$ in A is a subring of A that is a finitely generated R-module with $F\mathcal{O} = A$. Claim: $\mathcal{O}_K$ is the (unique) maximal $\mathbb{Z}$-order in K. For instance, this claim requires $\mathcal{O}_K$ to be a ring, which we haven't proved yet.

5 Definition

A $\boxed{\text{global field}}$ is either a number field or a finite extension of $\mathbb{F}_p(t)$. Many of the things that hold for number fields also hold for global fields. For instance, rings of integers of number fields are analogous to the integral closures of $\mathbb{F}_p[t]$ in finite extensions of $\mathbb{F}_p(t)$.

6 Lemma

Let K be a number field, $x \in K$. Then x is an $\boxed{\textit{integral element}}$ (over $\mathbb{Z}$) if and only if there exists a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $xM \subset M$.

Proof If x is integral, it is a root of a monic polynomial $f(t) \in \mathbb{Z}[t]$, so let $M := \operatorname{Span}_{\mathbb{Z}}\{1, x, \ldots, x^{\deg f - 1}\}$. Then $xM \subset M$ since we can replace $x^{\deg f}$ with the negative of the non-top-degree terms of f. On the other hand, suppose $v_1, \ldots, v_n \in M$ are generators. Since $xM \subset M$, there exist integers $a_{ij} \in \mathbb{Z}$ such that $xv_j = \sum_i a_{ij} v_i$, so $xI - (a_{ij})$ has a nontrivial kernel (namely it contains $[v_1, \ldots, v_n]^T$), so its determinant is zero, but its determinant is also a monic polynomial in $\mathbb{Z}[x]$.

7 Proposition

$\mathcal{O}_K$ is a ring.

Proof If $x, y \in \mathcal{O}_K$, then we have finitely generated $M, N \subset K$ such that $xM \subset M$ and $yN \subset N$. Then MN is also finitely generated and $(x \pm y)MN \subset MN$, $xyMN \subset MN$.

8 Proposition

If A is a UFD, then A is integrally closed (in its field of fractions).

Proof Let $a, b \in A$, $b \neq 0$. Assume a/b is integral over A, so there exists $c_0, \ldots, c_{n-1} \in A$ such that

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_0 = 0.$$

Multiply through by b^n to get

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_0 b^n = 0.$$

Hence $b \mid a^n$, so every prime dividing b divides a. If we had made a and b relatively prime to begin with, which is possible over a UFD, this forces b to be a unit in A, so $a/b \in A$.

9 Definition

Let $R \subset S$ be rings such that S is a finitely generated free R-module. (Technically either take R commutative, or take S to be a bimodule. Usually $K \subset L$ are fields with $\mathcal{O}_K \subset \mathcal{O}_L$.) For $\alpha \in S$, let $m_\alpha \colon S \to S$ be given by $x \mapsto \alpha x$. This is R-linear; we can equivalently consider m_α as a matrix with entries in R.

(a) The $\boxed{\text{norm}}$ $\boxed{N_{S/R}(\alpha)}$ is $\det m_\alpha$;

(b) The $\boxed{\text{trace}}$ $\boxed{\operatorname{Tr}_{S/R}(\alpha)}$ is $\operatorname{Tr} m_\alpha$;

(c) The $\boxed{\text{discriminant}}$ of $\alpha_1, \ldots, \alpha_n \in S$, $\boxed{\operatorname{Disc}_{S/R}(\alpha_1, \ldots, \alpha_n)}$, is $\det((\operatorname{Tr}(m_{\alpha_i \alpha_j}))_{i,j})$.

Note that the norm is multiplicative and the trace is R-linear. We will often drop the S/R, so for instance $\operatorname{Tr}(\alpha)$ means $\operatorname{Tr}(m_\alpha)$.

10 Proposition

If $\alpha_1, \ldots, \alpha_n \in S$ are an R-basis and $M \colon S \to S$ is R-linear, then

$$\operatorname{Disc}_{S/R}(M\alpha_1, \ldots, M\alpha_n) = (\det M)^2 \operatorname{Disc}_{S/R}(\alpha_1, \ldots, \alpha_n).$$

In particular, if M is invertible, these discriminants agree up to a unit in R, so the $\boxed{\textit{discriminant of } S}$ can be well-defined as the ideal in R generated by the discriminant of any basis.

PROOF If $M = (m_{ij})_{i,j}$ in the given basis, then $M\alpha_k = \sum_k m_{ki}\alpha_i$ by definition, so we compute

$$\begin{aligned}\operatorname{Tr}(M(\alpha_i)M(\alpha_j)) &= \operatorname{Tr}(\sum_{k,\ell} m_{ki}\alpha_i m_{\ell j}\alpha_j)\\ &= \sum_{k,\ell} m_{ki}m_{\ell j}\operatorname{Tr}(\alpha_i\alpha_j)\\ &= M(\operatorname{Tr}(\alpha_i\alpha_j))_{ij}M^T.\end{aligned}$$

Now take determinants.

11 Aside

The preceding proposition relates $\operatorname{Disc}_{S/R}(\operatorname{Span}_R\{\alpha_1,\ldots,\alpha_n\})$, $\operatorname{Disc}_{S/R}(\operatorname{Span}_R\{M\alpha_1,\ldots,M\alpha_n\})$, and the index of $B \subset A$—more details on the homework.

12 Proposition

If L/K is a separable field extension of degree n, then let $\sigma_1,\ldots,\sigma_n$ be the n embeddings $L \hookrightarrow \overline{K}$ which are the identity on K. Then

- $N_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$,
- $\operatorname{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$, *and*
- $\operatorname{Disc}_{L/K}(\alpha_1,\ldots,\alpha_n) = \det(\sigma_i(\alpha_j))^2$.

13 Corollary

The norm, trace, and discriminant of integral elements coming from a separable field extension are all integral.

PROOF Integrality is preserved by the σ_i, so the above quantities are all polynomial combinations of integral elements.

October 2nd, 2015: Rings of Integers are Dedekind Domains

Review of norm, trace, discriminant from last lecture:

Let $R \subset S$ be rings, $S \cong R^n$, $\alpha \in S$, $m_\alpha\colon S \to S$ by $x \mapsto \alpha x$, $N_{S/R}(\alpha) := \det m_\alpha$, $\operatorname{Tr}_{S/R}(\alpha) := \operatorname{Tr} m_\alpha$, and $\operatorname{Disc}_{S/R}((\alpha_i)_i) := \det(\operatorname{Tr}(\alpha_i\alpha_j)_{i,j})$.

If $x_1,\ldots,x_n \in S$ are an R-basis for S, and $M\colon S \to S$ is R-linear, then $\operatorname{Disc}(M(x_i)) = (\det M)^2\operatorname{Disc}((x_i))$. Moreover, if L/K is a separable field extension of degree n, and if $\sigma_1,\ldots,\sigma_n\colon L \hookrightarrow \overline{K}$ are the n embeddings of L into the algebraic closure of K which fix K, then $N_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$, $\operatorname{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$, $\operatorname{Disc}_{L/K}(\alpha) = \det(\sigma_i(\alpha_j))^2$.

Indeed, if L/K is inseparable, $\operatorname{Tr}(\alpha) = 0$ for all $\alpha \in L$ and $\operatorname{Disc}((\alpha_i)_i) = 0$ whenever $\alpha_i \in L$. More details and proofs in the homework and Osserman's notes.

As a corollary, if L/K is an extension of number fields and K contains a subring R, and if $\alpha \in L$ is integral over R, then $N(\alpha), \operatorname{Tr}(\alpha)$ are integral over R. Similarly if $\alpha_1,\ldots,\alpha_n \in L$ are integral over R, then $\operatorname{Disc}((\alpha_i))$ is integral over R. In particular, if $R = \mathbb{Z}$ and $K = \mathbb{Q}$, then the discriminant of elements of $\mathcal{O}_L$ are in $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

14 Lemma

Let L/K be an extension of fields. Assume $L = K(\alpha)$ for some α. Let $f(x)$ be the minimal polynomial of α over K (in this class, f is thus assumed monic). Then

$$\mathrm{Disc}_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 =: \boxed{\mathrm{Disc}\, f(x)},$$

where $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of $f(x)$.

Proof In this case, $(\sigma_i(\alpha^j))$ is a Vandermonde matrix. (If the extension is inseparable, both sides are zero, so it still works.)

15 Lemma

Let L/K be a field extension of degree n with $\alpha_1, \ldots, \alpha_n \in L$. Then $\mathrm{Disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$ if and only if $\alpha_1, \ldots, \alpha_n$ is a K-basis for L and L/K is separable.

Proof Assume L/K is separable, so $L = K(\beta)$ for some β.

$\Leftarrow$ By the previous lemma, $\mathrm{Disc}(1, \beta, \ldots, \beta^{n-1}) \neq 0$. We can use an (invertible) change of basis matrix to send β^i to α_i and an earlier proposition then says that $\mathrm{Disc}((\beta^i))$ and $\mathrm{Disc}((\alpha_i))$ differ by a unit (in R).

$\Rightarrow$ If $\{\alpha_1, \ldots, \alpha_n\}$ is K-linearly dependent, then $\{\sigma_j(\alpha_i)\}_{i=1}^n$ is K-linearly dependent with the same dependence relation, for each j. Hence $\det(\sigma_j(\alpha_i))^2 = 0$.

The preceding discussion was quite general, though here are some special properties in the case $R = \mathbb{Z}$ involving rings of integers.

16 Notation

Let $\boxed{K}$ be a number field.

17 Proposition

Let $I \subset \mathcal{O}_K$ be a nonzero ideal. Then I contains a $\mathbb{Q}$-basis for K, and among the $\mathbb{Q}$-bases for K contained in I, any basis with minimal absolute value of the discriminant is a $\mathbb{Z}$-basis for I. In particular, I is a free $\mathbb{Z}$-module of rank n.

Proof Let $n = [K : \mathbb{Q}]$ and let $\alpha_1, \ldots, \alpha_n$ be any $\mathbb{Q}$-basis for K. Notice that for all i, there exists some $d_i \in \mathbb{Z}$ such that $d_i\alpha_i \in \mathcal{O}_K$ (essentially, take d_i large enough to clear all denominators of the minimal polynomial). Then if $0 \neq \beta \in I$, $\beta d_1\alpha_1, \ldots, \beta d_n\alpha_n$ is a $\mathbb{Q}$-basis for K contained in I. By the comments in the above review, the discriminant of (α_i) is in $\mathbb{Z}$.

Now let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K contained in I of minimal $|\mathrm{Disc}(\alpha_i)|$. If $\beta \in I$, then $\beta = \sum_i a_i\alpha_i$ for some $a_i \in \mathbb{Q}$. Assume to the contrary that $a_1 \notin \mathbb{Z}$. Write $a_1 = b + \epsilon$ where $b \in \mathbb{Z}$ and $0 < \epsilon < 1$. Let $\alpha'_1 := \beta - b\alpha_1$ and consider $\{\alpha'_1, \alpha_2, \ldots, \alpha_n\}$. This is clearly a $\mathbb{Q}$-basis for K and is contained in I. The change of basis matrix from $\{\alpha_1, \ldots, \alpha_n\}$ to $\{\alpha'_1, \alpha_2, \ldots, \alpha_n\}$ in the $\{\alpha_1, \ldots, \alpha_n\}$ basis is lower triangular with $\epsilon, 1, \ldots, 1$ on the main diagonal, which has squared determinant $0 < \epsilon^2 < 1$, giving a contradiction.

(Aside: the above change of basis proposition says that the discriminant of any two bases have the same sign, since they differ by the square of the determinant of a matrix over $\mathbb{Q}$.)

18 Definition

The preceding proposition says that ideals in $\mathcal{O}_K$ have $\mathbb{Z}$-bases, so the discriminant of any such ideal can be well-defined up to a unit (in $\mathbb{Z}$) as the discriminant of any $\mathbb{Z}$-basis. Precisely, $d(\mathcal{O}_K) = D(\mathcal{O}_K) = \boxed{\mathrm{Disc}(\mathcal{O}_K)}$ is the discriminant of any $\mathbb{Z}$-basis of $\mathcal{O}_K$, which is well-defined up to a sign.

19 Proposition

If $0 \neq I \subset \mathcal{O}_K$, then $\mathcal{O}_K/I$ is finite.

20 Lemma

Let $R \subset S$ be integral domains and let $I \subset S$ be a non-zero ideal. Suppose $0 \neq \alpha \in I$ satisfies a non-zero polynomial $f(x) \in R[x]$. Then $I \cap R \neq 0$.

PROOF WLOG assume $f(0) \neq 0$ by canceling enough powers of x. Consider $f(\alpha) - f(0) \in I$, but $f(\alpha) = 0$, so $0 \neq -f(0) \in R$.

PROOF (of proposition). The lemma implies that $I \cap \mathbb{Z} \neq 0$, so there exists $0 \neq m \in I \cap \mathbb{Z}$, and $\mathcal{O}_K/m\mathcal{O}_K \cong (\mathbb{Z}/m)^n$ (since $\mathcal{O}_K$ is a rank n $\mathbb{Z}$-module), and $\mathcal{O}_K/I$ is a further quotient of this, so is "even more" finite.

21 Definition

The $\boxed{\text{norm}}$ of an ideal I is $\boxed{N(I)} := \#(\mathcal{O}_K/I)$. By the preceding proposition, this is finite.

22 Fact

If $0 \neq x \in \mathcal{O}_K$, then $N(x\mathcal{O}_K) = |N_{K/\mathbb{Q}}(x)|$.

For instance, if the norm of an ideal is prime, then $\mathcal{O}_K/I$ has prime order, so it must be a finite field, so I must be maximal, hence prime.

23 Lemma

If M, N are free $\mathbb{Z}$-modules of rank n and $A\colon M \to N$ is an injective $\mathbb{Z}$-linear map, then $|\det(A)| = \#(N/A(M))$.

PROOF Exercise; also in Osserman's notes.

PROOF Let $M = N = \mathcal{O}_K$, $A = m_x$.

Now we'll "zoom out" a little to the generality of Dedekind domains.

24 Definition

An integral domain R is a $\boxed{\text{Dedekind domain}}$ if

(1) R is Noetherian

(2) Every nonzero prime ideal is maximal

(3) R is integrally closed (in its field of fractions)

(Geometrically, this is essentially saying $\operatorname{Spec} R$ is one-dimensional and regular/normal/non-singular. While fields are precisely zero-dimensional Dedekind domains, they typically satisfy the properties of one-dimensional Dedekind domains trivially.)

25 Proposition

Let R be an integral domain. If R is integrally closed and R/I is finite for all non-zero ideals in R, then R is a Dedekind domain.

In particular, by the previous proposition, rings of integers are Dedekind domains

PROOF Let $\mathfrak{p} \subset R$ be a prime ideal, so $R/\mathfrak{p}$ is a finite integral domain, hence a field, so $\mathfrak{p}$ is maximal. For the Noetherian condition, suppose $0 \neq I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots$ is an ascending chain of ideals. Taking successive quotients gives a sequence of surjections $R/I_0 \twoheadrightarrow R/I_1 \twoheadrightarrow \cdots$, which must eventually stabilize since these quotients have weakly decreasing finite order.

October 5th, 2015: Dedekind Domains, the Group of Fractional Ideals, and Unique Factorization

---

Summary of last class: we introduced Dedekind domains, which are commutative domains R where (1) R is Noetherian, (2) every non-zero prime in R is maximal, and (3) R is integrally closed. Our main source of example of Dedekind domain are rings of integers. (These should be all the Dedekind domains which are finite rank $\mathbb{Z}$-modules that are not fields.)

26 Definition

If R is an integral domain with $K := \mathrm{Frac}(R)$, then a subset $I \subset K$ is a $\boxed{\text{factional ideal}}$ of R if

(i) I is an R-submodule;

(ii) There exists $c \in R$ such that $cI \subset R$.

A fractional ideal I is a $\boxed{\text{principal fractional ideal}}$ if $I = \alpha R$ for some $\alpha \in K$.

(The idea behind (ii) is that the "denominators don't get too large" and can all be canceled simultaneously. "Fractional ideal" naively would suggest a subset of ideals satisfying special properties, but in fact fractional ideals are more general than ideals.)

27 Remark

Dedekind domains are not necessarily UFD's, despite $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ being the first example. For instance, $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ is not a UFD since $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. (This is the standard counterexample).

28 Theorem

Let R be a Dedekind domain. Then

(1) Every ideal of R factors uniquely into prime ideals.

(2) The set of fractional ideals forms a group under multiplication, with identity R.

29 Remark

The product of two fractional ideals I, J is the set of finite sums of pairwise products ij for $i \in I, j \in J$.

(1) says that while Dedekind domains need not be UFD's, their primes at least factor uniquely. If every prime were principal, then we would have unique factorization on the level of elements. Hence (2) says we can measure the failure of unique factorization by considering the "ideal class group" of K, Cl_K, which is the quotient of the fractional ideals by non-zero principal ideals. More on this later.

Proof We follow the proof from Lang, which proves (2) and deduces (1). Neukirch does (1) implies (2); Osserman does (2) implies (1) in a different way.

We first outline the proof of (2) as a series of claims:

30 Definition

If I is an ideal, define $\boxed{I^{-1}} := \{x \in K : xI \subset R\} \subset K$. (This is a generalized ideal quotient.)

(I^{-1} is indeed a factional ideal: let $0 \neq a \in I$, so $(a) \subset I$, so $(a)I^{-1} \subset II^{-1} \subset R$.)

Claim 1: If $I \subset R$ is a nonzero ideal, there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I$.

Claim 2: Every maximal ideal $\mathfrak{p}$ is invertible with inverse $\mathfrak{p}^{-1}$.

Claim 3: Every nonzero ideal is invertible and its inverse is a fractional ideal.

Claim 4: If $0 \neq I \subset R$ is an ideal and $J \subset K$ is an inverse of I, then $J = I^{-1}$.

Assuming the claims, we first prove (2). Claim 3 says every ideal is invertible. To amplify this up to all fractional ideals, suppose I is a fractional ideal with $c \in K$ such that $cI \subset R$. An inverse for I is the product of (c) and an inverse for cI. Claim (4) says inverses are unique.

For claim (1), suppose not. Take a maximal counterexample I (using the Noetherian hypothesis). Since I is not prime, we have $b_1, b_2 \notin I$ such that $b_1 b_2 \in I$. Note that

$$(I + b_1)(I + b_2) \subset I \subsetneq I + (b_i).$$

Since I is a maximal counterexample, $I + (b_i)$ cannot be counterexamples, so they each contain a product of non-zero primes. But then the product of those products of primes is contained in $(I + b_1)(I + b_2)$, hence in I, a contradiction.

For claim (2), from the definition we see that $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset R$ is an ideal. Since $\mathfrak{p}$ is maximal, either $\mathfrak{p}\mathfrak{p}^{-1}$ is either $\mathfrak{p}$ or R. So, assume to the contrary $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. From the finitely generated $\mathbb{Z}$-module definition of integrality above, this says $\mathfrak{p}^{-1} \supset R$ consists of integral elements, so since R is integrally closed, $\mathfrak{p}^{-1} = R$. We next exhibit an element of $\mathfrak{p}^{-1} - R$, giving a contradiction and proving the claim. Pick $0 \neq a \in \mathfrak{p}$. By claim (1), there exist non-zero primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$. Take r minimal with this property. Since $\mathfrak{p}$ is prime, some $\mathfrak{p}_i \subset \mathfrak{p}$, say $i = 1$. Primes are maximal here, so we have $\mathfrak{p}_1 = \mathfrak{p}$. Since r is minimal, $\mathfrak{p}_2, \ldots, \mathfrak{p}_r \not\subset (a)$. Take $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \notin (a)$. Note that $b\mathfrak{p} \subset (a)$, so $ba^{-1} \in \mathfrak{p}^{-1}$ and $ba^{-1} \notin R$. Note also that we have shown $\mathfrak{p}^{-1} \supsetneq R$ in general.

For claim (3), again assume not and take a maximal counterexample I. By claim (2), I is not prime, so $I \subsetneq \mathfrak{p}$ for some prime $\mathfrak{p}$. Now $I \subset I\mathfrak{p}^{-1} \subset R$, and $\mathfrak{p}^{-1}$ has non-integral elements, so $I \neq I\mathfrak{p}^{-1}$. But then $I\mathfrak{p}^{-1}$ has inverse J, so $J\mathfrak{p}$ is an inverse for I.

For claim (4), take $0 \neq I \subset R$ and $J \subset K$ such that $IJ = R$. By definition $J \subset I^{-1}$. On the other hand, for $x \in I^{-1}$, $xI \subset R$, so $xR = xIJ \subset J$, so $x \in J$ and $J = I^{-1}$.

We finally prove unique factorization (1). For existence, assume it fails and take a maximal counterexample I. Obviously I cannot be prime. Let $\mathfrak{p} \supsetneq I$ be a maximal ideal. Now $I \subsetneq I\mathfrak{p}^{-1} \subset R$, so $I\mathfrak{p}^{-1}$ has a prime factorization, and we can multiply it by $\mathfrak{p}$ to get a factorization for I.

For uniqueness, first define:

31 Definition

If $I, J \subset K$ are fractional ideals, say $\boxed{I \mid J}$ if there is an ideal $I' \subset R$ such that $J = II'$. Equivalently (using the existence of inverses), $J \subset I$.

Now assume $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Then $\mathfrak{p}_1 \mid \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Hence $\mathfrak{q}_i \subset \mathfrak{p}_1$ for some i, say $i = 1$. Then $\mathfrak{q}_1 = \mathfrak{p}_1$ may be canceled from both sides, giving the result by induction.

32 Example

Let's return briefly to the motivating question from the first day. Let $n \in \mathbb{Z}$ and pick a prime p. We want to know if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y) \in \mathbb{Z}[\sqrt{-n}]$. Assume for the moment that $\mathbb{Z}[\sqrt{-n}]$ is integrally closed (equivalently, $-n$ is squarefree and $-n \equiv_4 2, 3$). Then $p = x^2 + ny^2$ if and only if $(p) \subset \mathbb{Z}[\sqrt{-n}]$ factors as the product of two principal prime ideals. (They have to be prime since the norm of (p) is p^2, and since norm is multiplicative, the norms of the two factors above are each p, which implies they were prime.) Factoring $(p) \subset \mathbb{Z}[\sqrt{-n}]$ into not-necessarily principal primes is well-understood, but fuguring out when they are principal is not well understood since class groups are complicated.

October 7th, 2015: Dedekind Domains, Localizations, and DVR's

Summary of last time: we proved the theorem above, that in a Dedekind domain R, ideals factor uniquely as a product of prime ideals, and the set of fractional ideals form a group under multiplication with identity R. We also related our recent discussion with the problem of finding primes of a particular "polynomial" form.

Today we'll study localizations of Dedekind domains.

33 Definition

An integral domain R is a $\boxed{\text{discrete valuation ring (DVR)}}$ if it is a local PID.

34 Proposition

If R is an integral domain, then

(i) Assume R is noetherian. Then R is a UFD if and only if every irreducible is prime.

(ii) R is a PID if and only if R is a Dedekind domain and a UFD.

Proof For (i), the $\Rightarrow$ implication is clear. As for $\Leftarrow$, pick $r \in R$. First we claim r factors into irreducibles: for if r is not irreducible, we can write it as the product of non-units, which themselves are either irreducible or can be written as the product of non-units, etc. Abstractly this could result in an infinite recursion, but this process constructs a tower of ideals, and infinite recursion would imply an infinite strictly ascending chain, a contradiction. Uniqueness follows since every irreducible element is prime using the standard fundamental theorem of arithmetic argument.

For (ii), in the $\Rightarrow$ direction, we know that since R is a PID, it is noetherian (having finitely generated ideals) and is a UFD. We've already showed that UFD's are integrally closed in their field of fractions. So, we need only show primes are maximal. Let $(x) = \mathfrak{p} \subset R$ be prime. Since $\mathfrak{p}$ is prime, x is irreducible, from which it follows that $(x) = \mathfrak{p}$ is maximal.

In the $\Leftarrow$ direction for (ii), since R is a Dedekind domain, by the theorem it suffices to prove that every prime ideal is principal. Since $\mathfrak{p} \subset R$, we can pick any non-zero element of $\mathfrak{p}$ and write it as a product of irreducibles, whence we have $x \in \mathfrak{p}$ irreducible. But then $(x) \subset \mathfrak{p}$ is a prime ideal, so $(x) = \mathfrak{p}$ is principal.

35 Corollary

DVR's are Dedekind domains.

Proof DVR's are (local) PID's.

36 Lemma

Any Dedekind domain with only finitely many prime ideals is a PID. In particular, local Dedekind domains are DVR's.

Proof Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals of R and let $\mathfrak{a}$ be some other ideal. By the theorem, we can write $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Choose $\pi_i \in \mathfrak{p}_i - \mathfrak{p}_i^2$. By the Chinese Remainder Theorem, there exists $\alpha \in R$ such that $\alpha \equiv_{\mathfrak{p}_i^{e_i+1}} \pi_i^{e_i}$. Write $(\alpha) = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}$. We claim f_i is the maximal value such that $(\alpha) \subset \mathfrak{p}_i^{f_i}$, from which $f_i = e_i$ follows, so $(\alpha) \subset a$. For the claim, suppose $(\alpha) \subset \mathfrak{p}_1^s$ for $s > f_1$. Then $\mathfrak{p}_1^{f_1 - s}\mathfrak{p}_2^{f_2} \cdots \mathfrak{p}_r^{f_r} \subset R$, however $\mathfrak{p}_1^{f_1-s}$ is a non-integral ideal since $f_1 - s < 0$, which contradicts the fact that we can factor this product uniquely using integral ideals.

37 Proposition

If R is a Dedekind domain and S is a multiplicative subset, then $S^{-1}R$ is a Dedekind domain, and the induced map on fractional ideals $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ is a surjective homomorphism from the group of fractional ideals of R to the group of fractional ideals of $S^{-1}R$. The kernel of this map consists precisely of those fractional ideals which intersect S non-trivially.

Proof Exercise; this will be on homework.

38 Definition

Let R be an integral domain with fraction field $K := \mathrm{Frac}(R)$. Let $I \subset K$ be a fractional ideal and suppose $\mathfrak{p} \subset R$ is a non-zero prime ideal. Then $\boxed{I_\mathfrak{p}} := IR_\mathfrak{p} \subset K$. (Note that we may assume all localizations $S^{-1}R$ are literal subsets of K.)

39 Lemma

In the notation of the preceding definition, $I_\mathfrak{p}$ is a fractional ideal of $R_\mathfrak{p}$ and $I = \cap_\mathfrak{p} I_\mathfrak{p}$.

Proof I is a fractional ideal, so pick $c \in R$ such that $cI \subset R$, so $cI_\mathfrak{p} \subset R_\mathfrak{p}$. It follows that $I_\mathfrak{p}$ is indeed a fractional ideal of $R_\mathfrak{p}$.

For $I = \cap_\mathfrak{p} I_\mathfrak{p}$, the $\subset$ direction is clear, so let $x \in \cap_\mathfrak{p} I_\mathfrak{p} \subset K$ and write $x = a/b$ for $a, b \in R$. Let $J := \{y \in R : ya \in bI\} \subset R$. We claim $J = R$, in which case $1 \in J$ says $a \in bI$, so $a/b \in I$. For the claim, pick $\mathfrak{p}$ prime, so $x \in I_\mathfrak{p}$ says $a/b = c/d$ for some $c \in I$, $d \notin \mathfrak{p}$. Hence $da = bc \in bI$ and $d \in J - \mathfrak{p}$. Therefore $J \not\subset \mathfrak{p}$ for all $\mathfrak{p}$, forcing $J = R$.

40 Remark

Osserman proves the theorem on unique factorization in Dedekind domains by building up the local picture and using this lemma repeatedly.

41 Proposition

Let R be a noetherian integral domain. Then R is a Dedekind domain if and only if $R_\mathfrak{p}$ is a DVR for all primes $\mathfrak{p}$.

Proof In the $\Rightarrow$ direction, 37 shows that $R_\mathfrak{p}$ is a (local) Dedekind domain, hence is a DVR. For $\Leftarrow$, we need to show that non-zero primes are maximal and that R is integrally closed.

If $0 \neq \mathfrak{p} \subset \mathfrak{m} \subset R$, then localize at $\mathfrak{m}$. By assumption, $R_\mathfrak{m}$ is a DVR, so $\mathfrak{p} = \mathfrak{m}$ are both the unique prime in $R_\mathfrak{m}$. Since primes in $R_\mathfrak{m}$ are in bijection with primes in R contained in $\mathfrak{m}$, we have $\mathfrak{p} = \mathfrak{m}$ in R. Now suppose $x \in K$ is integral over R. Then x is integral over $R_\mathfrak{p}$ for all $\mathfrak{p}$. Since $R_\mathfrak{p}$ is a DVR, hence is a UFD, so $x \in R_\mathfrak{p}$ for all $\mathfrak{p}$. By the lemma with $I = R$, $x \in R$.

42 Remark

Let K be a number field with an order $\mathcal{O} \subset K$. The maximal order $\mathcal{O}_K$ is a Dedekind domain, but $\mathcal{O}$ need not be. More details in Neukirch, Chapter 1. We can still talk about fractional ideals with respect to $\mathcal{O}$, but they are not necessarily invertable.

43 Definition

Let $\mathfrak{a} \subset K$ be a fractional ideal of $\mathcal{O}$. Say $\mathfrak{a}$ is invertible if there exists another fractional ideal $\mathfrak{b} \subset K$ of $\mathcal{O}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

If $\mathfrak{a}$ is invertible, then $\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subset \mathcal{O}\}$. This follows from claim (4) in the theorem from last time.

44 Proposition

$\mathfrak{a}$ is invertible if and only if $\mathfrak{a}_\mathfrak{p} := \mathfrak{a}\mathcal{O}_\mathfrak{p}$ is a principal fractional ideal for all $\mathfrak{p}$.

Proof Assume $\mathfrak{a}$ is invertible with $\mathfrak{b} := \mathfrak{a}^{-1}$. Then $1 = \sum_{i=1}^r a_i b_i$ for some $a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$. At least one of the products $a_i b_i \notin \mathfrak{p}$, say with $i = 1$. We claim $\mathfrak{a}_\mathfrak{p} = (a_1)$. Let $x \in \mathfrak{a}_\mathfrak{p}$, so $xb_1 \in \mathfrak{a}_\mathfrak{p}\mathfrak{b} = \mathcal{O}_\mathfrak{p}$. Write $x = (xb_1)(a_1b_1)^{-1}a_1 \in \mathcal{O}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\times a_1$. Ran out of time to finish it off—see Neukirch for the rest.

Hence the failure of invertibility of fractional ideals is intimately related to the failure of localizations being PID's.

October 9th, 2015: The ef Theorem, Ramification, Relative Discriminants

Summary To determine if there exists a solution to $p = x^2 + ny^2$, we want to know how p factors in $\mathbb{Z}[\sqrt{-n}]$. So, the next few days will be concerned with figuring out how (p) factors over rings of integers.

We'll use the following background notation in the next few lectures:

45 Notation
Let $R \subset S$ be Dedekind domains. Suppose S is finitely generated as an R-module. Let $K := \mathrm{Frac}(R), L := \mathrm{Frac}(S)$, where L/K is an extension of degree n.

46 Theorem ("*ef* Theorem")
Let $0 \neq \mathfrak{p} \subset R$ be a prime ideal and let $\mathfrak{p}S = \prod_{i=1}^r \mathfrak{q}_i^{e_i}$ where the $\mathfrak{q}_i$ are distinct non-zero prime ideals, and $e_i \in \mathbb{Z}_{>0}$. Then $S/\mathfrak{q}_i$ is a finite dimensional $R/\mathfrak{p}$-vector space and $n = \sum_{i=1}^r e_i f_i$ where $f_i := \dim_{R/\mathfrak{p}} S/\mathfrak{q}_i$.

47 Proposition
$R_\mathfrak{p}S$ is a free $R_\mathfrak{p}$-module of rank n.

Proof Since S is finitely generated as an R-module, $R_\mathfrak{p}S$ is a finitely generated $R_\mathfrak{p}$-module. Note that $R_\mathfrak{p}S$ has finitely many prime ideals, so is a local Dedekind domain, hence is a PID. Using the structure theorem for finitely generated modules over a PID, we just need to show that $R_\mathfrak{p}S$ is torsion free and of rank n. Since $R_\mathfrak{p}S \subset L$ is a subset of a field, it is obviously torsion-free. As for the rank, let $x_1, \ldots, x_m$ be free generators for $R_\mathfrak{p}S$ over $R_\mathfrak{p}$. Then $x_1, \ldots, x_m$ is also a K-basis for L, essentially by canceling denominators. Hence $m = n$.

Proof of theorem: write $S_\mathfrak{p} := R_\mathfrak{p}S$. Notice that $S/\mathfrak{p}S \cong S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$ and $S_\mathfrak{p} \cong R_\mathfrak{p}^n$ by the proposition, so $S/\mathfrak{p}S$ is an $R/\mathfrak{p}$-vector space of dimension n. By the Chinese Remainder Theorem, $S/\mathfrak{p}S \cong \prod_{i=1}^r S/\mathfrak{q}_i^{e_i}$. Now we need only show $\dim S/\mathfrak{q}_i^{e_i} = e_i f_i$. For any m, $S/\mathfrak{q}_i^m \cong S_{\mathfrak{q}_i}/\mathfrak{q}_i^m S_{\mathfrak{q}_i}$. But $S_{\mathfrak{q}_i}$ is a DVR since S is a Dedekind domain. Then we have

$$S/\mathfrak{q}_i \cong S_{\mathfrak{q}_i}/\mathfrak{q}_i S_{\mathfrak{q}_i} \cong \mathfrak{q}_i/\mathfrak{q}_i^2 S_{\mathfrak{q}_i} \cong \cdots \cong \mathfrak{q}_i^m/\mathfrak{q}_i^{m+1} S_{\mathfrak{q}_i}.$$

The claim now follows by induction and the observation $(S_{\mathfrak{q}_i}/\mathfrak{q}_i^{m+1}S_{\mathfrak{q}_i})/(\mathfrak{q}_i^m/\mathfrak{q}_i^{m+1}S_{\mathfrak{q}_i}) \cong S_{\mathfrak{q}_i}/\mathfrak{q}_i^m S_{\mathfrak{q}_i}$.

48 Definition
We say that a prime ideal $\mathfrak{q} \subset S$ $\boxed{\text{lies above}}$ a prime ideal $\mathfrak{p} \subset R$ if $\mathfrak{q} \cap R = \mathfrak{p}$. (Of course, this is just saying the induced map $\operatorname{Spec} S \to \operatorname{Spec} R$ sends $\mathfrak{q}$ to $\mathfrak{p}$.)

49 Proposition
Every non-zero prime ideal of S lies above a unique non-zero prime ideal of R. The following are equivalent:

a) $\mathfrak{q}$ lies above $\mathfrak{p}$

b) $\mathfrak{p} \subset \mathfrak{q}$ (equivalently, $\mathfrak{p}S \subset \mathfrak{q}$)

c) $\mathfrak{q}$ occurs in the factorization of $\mathfrak{p}S$.

Proof We've already shown $\mathfrak{q} \cap R \neq 0$. If $x, y \in R$ such that $xy \in \mathfrak{q} \cap R$, then since $\mathfrak{q}$ is prime, x or $y \in R$, so x or y is in $\mathfrak{q} \cap R$, so $\mathfrak{q} \cap R$ is prime.

We essentially showed (b) $\Leftrightarrow$ (c) when we defined divisibility of fractional ideals. For (b) $\Rightarrow$ (a), we have $\mathfrak{p} = \mathfrak{p} \cap R \subset \mathfrak{q} \cap R$ is a maximal ideal, so $\mathfrak{p} = \mathfrak{q} \cap R$. Note that (a) $\Rightarrow$ (b) is by definition.

50 Definition

Let $\mathfrak{q}$ be a non-zero prime ideal of S lying over $\mathfrak{p}$, written $\boxed{\mathfrak{q}/\mathfrak{p}}$. Let $e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{p}}$ be e_i, f_i from the theorem. Then

- $\boxed{e_{\mathfrak{q}/\mathfrak{p}}}$ is the $\boxed{\text{ramification index/degree}}$ of $\mathfrak{q}/\mathfrak{p}$
- $\boxed{f_{\mathfrak{q}/\mathfrak{p}}}$ is the $\boxed{\text{inertia degree}}$ of $\mathfrak{q}/\mathfrak{p}$.
- We say that $\mathfrak{p}$ is $\boxed{\text{ramified}}$ in S if $e_{\mathfrak{q}/\mathfrak{p}} > 1$ or $S/\mathfrak{q}$ over $R/\mathfrak{p}$ is inseparable for some $\mathfrak{q}/\mathfrak{p}$. We say $\mathfrak{p}$ is $\boxed{\text{unramified}}$ otherwise.
- We say that $\mathfrak{p}$ is $\boxed{\text{inert}}$ if $\mathfrak{p}$ is unramified and there is a unique prime lying above $\mathfrak{p}$.
- We say $\mathfrak{p}$ $\boxed{\text{splits completely}}$ if it is unramified and the inertia degrees $f_{\mathfrak{q}/\mathfrak{p}}$ are 1 for all $\mathfrak{q}/\mathfrak{p}$.

Note that for rings of integers, $S/\mathfrak{q}$ over $R/\mathfrak{p}$ is an extension of finite fields, so is automatically separable, so ramification is controlled entirely by the multiplicity condition.

51 Example

Let $S = \mathbb{Z}[i]$, $R = \mathbb{Z}$. Using the e, f theorem, there are only three possible sums which add up to $n = 2$. Indeed, p is ramified iff $p \equiv_4 2$, p is inert iff $p \equiv_4 3$, and p splits completely iff $p \equiv_4 1$.

52 Proposition

Let $T \subset R \subset S$ be extensions of Dedekind domains. Write $K \subset M \subset L$ for the corresponding tower of fraction fields. Suppose that R is finitely generated as a T-module and S is finitely generated as an R-module. Pick a "tower" of primes $\mathfrak{q} \subset \mathfrak{p} \subset \mathfrak{l}$. Then

$$e_{\mathfrak{l}/\mathfrak{p}} = e_{\mathfrak{l}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} \qquad\qquad f_{\mathfrak{l}/\mathfrak{p}} = f_{\mathfrak{l}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}}.$$

Proof Let $\mathfrak{p} = \prod_{i=1}^r \mathfrak{q}_i^{e_i}$, $\mathfrak{q}_i = \prod_{j=1}^{r_i} \mathfrak{l}_j^{e_{ij}}$, so $\mathfrak{p} = \prod_{i=1}^r (\prod_{j=1}^{r_i} \mathfrak{l}_j^{e_{ij}})^{e_i}$, and distribute. Then use the fact that dimensions of towers of field extensions multiply.

Discriminants help determine when primes are ramified, but e is a relative notion, so we first generalize to relative discriminants.

53 Definition

Consider either of the following setups:

Case 1: Let $R \subset S$ be integral domains with fields of fractions $K \subset L$ with L/K of degree n, where R is integrally closed in K and x is integral over R for all $x \in S$.

Case 2: Let $R \subset S$ where S is free of rank n over R.

The $\boxed{\text{relative discriminant}}$ $\boxed{D_{R/S}}$ $\subset R$ is the ideal generated by

Case 1: $D_{L/K}((x_1, \ldots, x_n))$

Case 2: $D_{S/R}((x_1, \ldots, x_n))$

as (x_i) ranges over tuples of elements of S.

Recall that $D_{R/S}(x_1, \ldots, x_n) = \det(\mathrm{Tr}(x_i x_j)) = \det(\mathrm{Tr}(m_{x_i x_j}))$, so the traces are in R and the determinant is indeed in R in case (2). In case (1), the traces are in K and are integral over R, hence are in R, so the determinant is again in R.

54 Remark

1) The two definitions agree when they both apply.

2) If S is free over R then $D_{S/R}$ is a principal ideal generated by $D_{S/R}(x_1, \ldots, x_n)$ where (x_i) is any R-basis for S.

3) If L is a number field, then $D_{\mathcal{O}_L/\mathbb{Z}} = \langle D_L \rangle$.

Proof The two discriminants in fact agree for all tuples, giving (1). For (2), use the change of basis proposition for discriminants above. Hence (3) follows from (2) using the definition of D_L.

October 12th, 2015: Discriminant Criterion for Ramification

Summary Last time we defined relative discriminants in two contexts: A) when S/R was free of rank n, and B) when $R \subset S$ was a domain with fields of fractions $K \subset L$ of degree n, where R is integrally closed in K and for all $x \in S$, x is integral over R.

Our main goal today is to prove a standard result relating ramification and relative discriminants.

(The "B" context was originally stated without the two integral hypotheses, but then isn't not clear the result is an ideal in R. The additional hypotheses have been incorporated into the previous lecture's notes.)

55 Notation

Today, S and R will be as in cases A) or B) above. Again write $S_{\mathfrak{p}} := R_{\mathfrak{p}} S$.

56 Lemma

Let S_1, S_2 be free R-modules of finite rank and let $S = S_1 \oplus S_2$. Then $D_{S/R} = D_{S_1/R} D_{S_2/R}$.

Proof Note that $xy = 0$ for all $x \in S_1, y \in S_2$. Hence $m_{x,S} \colon S \to S$ given by $(s_1, s_2) \mapsto (xs_1, 0)$ is essentially m_{x,S_1}, and similarly with y. It follows that if $z_1, z_2 \in S_1 \cup S_2$, then

$$\mathrm{Tr}(z_1 z_2) = \begin{cases} 0 & \text{if } z_i \in S_1,\ z_j \in S_2 \\ \mathrm{Tr}_{S_1}(z_i z_j) & \text{if } z_i, z_j \in S_1 \\ \mathrm{Tr}_{S_2}(z_i z_j) & \text{if } z_i, z_j \in S_2 \end{cases}$$

Since S is a free R-module, $D_{S/R}$ is a principal ideal generated by $D_{S/R}((z_1, \ldots, z_n))$ for any R-basis for S. The resulting matrix of traces is block diagonal, and the result follows.

57 Lemma (Case B.)

If R is a field and $\mathrm{Nil}(S) \neq 0$*, then $D_{S/R} = 0$.*

Proof Let $0 \neq x \in \mathrm{Nil}(S)$ and let $y \in S$. Consider m_{xy} and let $z \in S$ be an eigenvector of m_{xy} with eigenvalue λ. Then

$$0 = x^n y^n z = (xy)^n z = m_{xy}^n(z) = \lambda^n z$$

for sufficiently large n. Hence $\lambda^n = 0$, so $\lambda = 0$. While there may be no eigenvectors in S itself, we may pass to an algebraic closure and deduce that the minimal polynomial of m_{xy} is of the form t^k, so that $\mathrm{Tr}(xy) = 0$ for all $y \in S$. Since R is a field, there exists a basis containing x, so that $D_{S/R} = 0$.

58 Lemma (Case A.)

Let $I \subset R$ be an ideal. Then

$$D_{(S/IS)/(R/I)} \equiv D_{S/R} \text{ mod } I.$$

Proof If $x_1, \ldots, x_n$ is an R-basis for S, then $\overline{x}_1, \ldots, \overline{x}_n$ is an R/I-basis for S/IS. The result now follows from the definitions.

59 Lemma (Case B.)

Let $\mathfrak{p} \subset R$ be a prime ideal. Then $D_{S_\mathfrak{p}/R_\mathfrak{p}} = R_\mathfrak{p} D_{S/R}$.

Proof $\supset$ is clear from the definitions, since computing discriminants of tuples of elements in S can be done either before or after localizing without affecting the answer. For the $\subset$ inclusion, let $x_i = y_i/z_i \in S_\mathfrak{p}$, so $y_i \in S$ and $1/z_i \in R_\mathfrak{p}$. Then using the change of basis formula gives

$$\mathrm{Disc}((x_i)) = \mathrm{Disc}((y_i/z_i)) = \left(\prod_i \frac{1}{z_i^2}\right) \mathrm{Disc}((y_i)) \in R_\mathfrak{p} D_{S/R}.$$

60 Theorem

Let $R \subset S$ be a finitely generated extension of Dedekind domains. Then $\mathfrak{p} \subset R$ is ramified in S if and only if $\mathfrak{p} \mid D_{S/R}$.

Proof Our rough strategy is to localize and use the last lemma to allow us to use the previous lemmas.

Let $\mathfrak{p}S = \prod_{i=1}^m q_i^{e_i}$. Claim:

$$D_{S/R} \subset \mathfrak{p} \Leftrightarrow \mathfrak{p} \mid D_{S/R} \Leftrightarrow D_{(S/q_i^{e_i})/(R/\mathfrak{p})} = 0 \text{ for some } i.$$

Recall that $(S/\mathfrak{p}S)/(R/\mathfrak{p})$ falls in Case A since $R/\mathfrak{p}$ is a field. Likewise $S_\mathfrak{p} \supset R_\mathfrak{p}$ falls in Case A by the proposition from last lecture. By the Chinese Remainder Theorem, $S/\mathfrak{p}S \cong \oplus S/\mathfrak{q}_i^{e_i}$, so by the first lemma, the final clause of the claim occurs iff $D_{(S/\mathfrak{p}S)/(R/\mathfrak{p})} = 0$. Using the third lemma, this occurs iff $D_{S_\mathfrak{p}/R_\mathfrak{p}} \subset \mathfrak{p}$ in $R_\mathfrak{p}$. Using the fourth lemma, this final condition is the same as saying $\mathfrak{p} \mid D_{S/R}$, giving the claim.

Now suppose $\mathfrak{p}$ is unramified. Then $e_i = 1$ and $S/\mathfrak{q}_i$ is a separable field extension of $R/\mathfrak{p}$. Hence $\mathrm{Disc}_{(S/\mathfrak{q}_i)/(R/\mathfrak{p})}(\text{any basis}) \neq 0$ for all i, so $p \nmid D_{S/R}$.

If $\mathfrak{p}$ is ramified, then either $e_i > 1$, so $S/\mathfrak{q}_i^{e_i}$ over $R/\mathfrak{p}$ is an extension with nilpotents, so the discriminant of the quotient is zero, or $e_i = 1$ and $S/\mathfrak{q}_i$ is an inseparable field extension. But we already showed the discriminant of any inseparable field extension is zero. Hence $\mathfrak{p} \mid D_{S/R}$.

61 Corollary

Under the assumptions of the theorem, if L/K is separable, then only finitely many prime ideals ramify in S/R.

Next we discuss factoring ideals in extensions of Dedekind domains.

62 Notation

We now return to the notation from last class, namely $R \subset S$ is a finitely generated extension of Dedekind domains, and the corresponding extension of fields of fractions $K \subset L$ is of degree N.

63 Lemma

Let $\alpha \in S$. Assume that $K(\alpha) = L$ and let $f(x)$ be the minimal polynomial of α. Then $\mathrm{Disc}(f(x)) \in$ *$D_{S/R}$.*

Proof We showed in an earlier lemma that $\mathrm{Disc}(f(x)) = \mathrm{Disc}_{L/K}((1, \alpha, \ldots, \alpha^{n-1}))$. This latter quantity is in $D_{S/R}$ since each α^i is in S.

The next theorem allows us to often determine how a prime factors in an extension (and more) using factorization over finite fields.

64 Theorem

Let $\mathfrak{p} \subset R$ be a non-zero prime ideal. Assume there exists $\alpha \in S$ such that $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$. Let $f(x)$ be the minimal polynomial of α over R. If $f(x)$ factors as $\prod_{i=1}^m \overline{f}_i(x)^{e_i}$ in $(R/\mathfrak{p})[x]$ with the $\overline{f}_i$ distinct and separable, then

1) $\mathfrak{p}S = \prod_{i=1}^m \mathfrak{q}_i^{e_i}$ with $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg \overline{f}_i$.

2) $\mathfrak{q}_i = \mathfrak{p} + (\widetilde{f}_i(\alpha))$ where $\widetilde{f}_i(x) \in R[x]$ is any lift of $\overline{f}_i(x)$.

Furthermore, if $\alpha \in S$ is such that $\mathrm{Disc}(f_\alpha)D_{S/R}^{-1} \not\subset \mathfrak{p}$, then $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$.

65 Corollary

Assume there exists $\alpha \in S$ such that $L = K(\alpha)$. If $\mathfrak{p} \subset R$ is such that $f(x)$ mod $\mathfrak{p}$ is separable, then properties 1) and 2) hold.

Proof Next time!

October 14th, 2015: Draft

We first recall the theorem from the end of last class.

66 Notation

As before, let $R \subset S$ be a finitely generated extension of Dedekind domains. Let $K \subset L$ be the resulting extension of fields of fractions, of degree n. Set $S_\mathfrak{p} := R_\mathfrak{p}S$.

67 Theorem

Given $\mathfrak{p} \subset R$ nonzero, assume there exists $\alpha \in S$ such that $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$. Let $f(x)$ be the minimal polynomial of α over R. If $f(x) = \prod_{i=1}^m \overline{f}_i^{e_i}(x)$ in $(R/\mathfrak{p})[x]$ with $\overline{f}_i$ distinct and irreducible, then

1) $\mathfrak{p}S = \prod_{i=1}^m \mathfrak{q}_i^{e_i}$ and $f_{\mathfrak{q}/\mathfrak{p}} = \deg \overline{f}_i$, and

2) $\mathfrak{q}_i = \mathfrak{p} + \widetilde{f}_i(\alpha)$ where $\widetilde{f}_i$ is any lift of $\overline{f}_i$ to $R[x]$.

Further, if $\alpha \in S$ is such that $\mathrm{Disc}(f_\alpha)D_{S/R}{-}1 \not\subset \mathfrak{p}$, then $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$.

Proof Let $\mathfrak{p}S = \prod_{i=1}^{m'} \mathfrak{q}_i^{e'_i}$. Note that

$$\prod_{i=1}^{m'} S/\mathfrak{q}_i^{e'_i} \cong S/\mathfrak{p}S \cong S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p} \cong R_\mathfrak{p}[\alpha]/\mathfrak{p}S_\mathfrak{p} \cong \prod_{i=1}^{m} (R/\mathfrak{p})[x]/\overline{f}_i(x)^{e_i}.$$

Hence we essentially need to match up terms. From earlier, $S_\mathfrak{p}$ is a PID, so we may apply the structure theorem to do the matching; Osserman does this step more "by hand"; we won't take the time to write out either approach. Hence $m = m'$, $e_i = e'_i$, and $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg \overline{f}_i$.

For the last claim, we already know $\mathrm{Disc}(f_\alpha) \subset D_{S/R}$, so $(\mathrm{Disc}\, f_\alpha)D_{S/R}^{-1} \subset R$. We also know that $R_\mathfrak{p}D_{S/R} = D_{S_\mathfrak{p}/R_\mathfrak{p}}$ by a lemma from last time. If $\mathrm{Disc}(f_\alpha)D_{S/R}^{-1} \not\subset \mathfrak{p}$, then $R_\mathfrak{p}\,\mathrm{Disc}(f_\alpha) = D_{S_\mathfrak{p}/R_\mathfrak{p}}$. Note that $D_{S_\mathfrak{p}/R_\mathfrak{p}}$ is principal. Hence $R_\mathfrak{p}(\mathrm{Disc}(f_\alpha)) = \langle \mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1}) \rangle$, so $1, \alpha, \ldots, \alpha^{n-1}$ is an $R_\mathfrak{p}$-basis for $S_\mathfrak{p}$, since otherwise the ideal would be zero.

Next we turn to factorization in Galois extensions.

68 Notation

We now assume $K \subset L$ is a Galois extension.

69 Proposition

Let $\mathfrak{p} \subset R$ be non-zero and suppose $\mathfrak{p}S = \prod_{i=1}^{m} \mathfrak{q}_i^{e_i}$. Then $\mathrm{Gal}(L/K)$ acts transitively on $\mathfrak{q}_i$, and for all i, j, we have $e_i = e_j$ and $f_i = f_j$. In particular, $n = mef$.

In this context, we write $\boxed{e_\mathfrak{p}} := e_{\mathfrak{q}/\mathfrak{p}}$ and $\boxed{f_\mathfrak{p}} := f_{\mathfrak{q}/\mathfrak{p}}$ for any $\mathfrak{q} = \mathfrak{q}_i$.

70 Lemma

S is the integral closure of R in L and so σ induces an automorphism of S for all $\sigma \in \mathrm{Gal}(L/K)$.

Proof Not difficult; can see it in Osserman; fine exercise.

Proof of proposition: take $\sigma \in \mathrm{Gal}(L/K)$. Can check that $\sigma(\mathfrak{q}_i)$ is a prime ideal directly. Also, $\sigma(\mathfrak{q}_i) \cap R = \sigma(\mathfrak{q}_i \cap R) = \sigma(\mathfrak{p}) = \mathfrak{p}$, which says that $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$ for some j. Applying σ to the factorization shows that $e_i = e_j$ and σ induces an isomorphism $S/\mathfrak{q}_i \cong S/\mathfrak{q}_j$, so $f_i = f_j$. Hence the full statement follows from transitivity, which we now turn to.

Suppose $\mathfrak{q}_j$ is a prime lying over $\mathfrak{p}$ outside of the orbit of $\mathfrak{q}_1$. By the Chinese Remainder Theorem, there exists $x \in S$ such that $x \in \mathfrak{q}_j$, $x \notin \mathfrak{q}_i$ for all $\mathfrak{q}_i$ in the orbit of $\mathfrak{q}_1$. Consider

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x) \qquad\qquad \sigma_i \in \mathrm{Gal}(L/K).$$

This is a product of integral elements in R, so is itself in R. Also, it is in $\mathfrak{q}_j$ (since the identity is in $\mathrm{Gal}(L/K)$), but the product is not in $\mathfrak{q}_1$ since by assumption none of the factors is in $\mathfrak{q}_1$. But since $\mathfrak{q}_j \cap R = \mathfrak{p} = \mathfrak{q}_1 \cap R$, this is a contradiction.

71 Definition

Let $\mathfrak{p} \subset R$ be a non-zero prime ideal, $\mathfrak{q} \subset S$ lying over $\mathfrak{p}$. The $\boxed{\text{decomposition group}}$ of $\mathfrak{q}/\mathfrak{p}$ is $\boxed{D_{\mathfrak{q}/\mathfrak{p}}} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$ and the $\boxed{\text{inertia group}}$ of $\mathfrak{q}/\mathfrak{p}$ is $\boxed{I_{\mathfrak{q}/\mathfrak{p}}} := \{\sigma \in D_{\mathfrak{q}/\mathfrak{p}} : \sigma(x) \equiv_\mathfrak{q} x, \forall x \in S\}$.

72 Theorem

Let $L_{D,\mathfrak{q}}$ denote the fixed field of $D_{\mathfrak{q}/\mathfrak{p}}$ and let $L_{I,\mathfrak{q}}$ denote the fixed field of $I_{\mathfrak{q}/\mathfrak{p}}$. Further write $S_{D,\mathfrak{q}} := S \cap L_{D,\mathfrak{q}}$ and $S_{I,\mathfrak{q}} := L_{I,\mathfrak{q}} \cap S$. Diagrammatically, we have

$$\begin{tikzcd}
\mathfrak{q} \arrow[r, hook] & S \arrow[r, hook] & L \\
\mathfrak{q}_1 \arrow[r, hook] & S_{I,\mathfrak{q}} \arrow[r, hook] & L_{I,\mathfrak{q}} \arrow[u, hook] \\
\mathfrak{q}_0 \arrow[r, hook] & S_{D,\mathfrak{q}} \arrow[r, hook] & L_{D,\mathfrak{q}} \arrow[u, hook] \\
\mathfrak{p} \arrow[r, hook] & R \arrow[r, hook] & K \arrow[u, hook]
\end{tikzcd}$$

Then

(i) $L_{D,\mathfrak{q}}$ is the minimal subfield of L containing K such that $\mathfrak{q}$ is the unique prime lying over $\mathfrak{q}_0$. Further $e_{\mathfrak{q}_0} = e_\mathfrak{p}$, $f_{\mathfrak{q}_0} = f_\mathfrak{p}$, and $[L : L_{D,\mathfrak{q}}] = e_\mathfrak{p} f_\mathfrak{p}$.

(ii) Assume that $S/\mathfrak{q}$ is separable over $R/\mathfrak{p}$. Then there is a short exact sequence

$$0 \to I_{\mathfrak{q}/\mathfrak{p}} \to D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}((S/\mathfrak{q})/(R/\mathfrak{p})) \to 0.$$

In particular, $\#I_{\mathfrak{q}/\mathfrak{p}} = e_\mathfrak{p}$ and $\#D_{\mathfrak{q}/\mathfrak{p}} = f_\mathfrak{p} e_\mathfrak{p}$.

(iii) $L_{I,\mathfrak{q}}$ is the minimal subfield of L containing K such that $\mathfrak{q}_1$ is totally ramified. Further, $e_{\mathfrak{q}_1} = e_\mathfrak{p}$ and $f_{\mathfrak{q}_1} = 1$. (Totally ramified means $\mathfrak{q}$ is a power of i, and the interia degree is always 1. Double check.) ($[L : L_{I,\mathfrak{q}}] = e_\mathfrak{p} = e_{\mathfrak{q}_1}$, $f_{\mathfrak{q}_1} = 1$.)

More intuitively, there is no splitting in $L/L_{D,\mathfrak{q}}$, $[L_{I,\mathfrak{q}} : L_{D,\mathfrak{q}}] = f_\mathfrak{p}$, $[L : L_{I,\mathfrak{q}}] = e_\mathfrak{p}$. The topmost extension is totally ramified, the middle is inert, and the extensions involving the top three fields are all Galois. However, $L_{D,\mathfrak{q}}/K$ is not necessarily Galois.

Proof We begin with (i). By definition, $\mathrm{Gal}(L/L_{D,\mathfrak{q}}) = D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma : \sigma(\mathfrak{q}) = \mathfrak{q}\}$. Hence the orbit of $\mathfrak{q}$ under the Galois group is just $\mathfrak{q}$, but from the previous proposition the Galois group acts transitively on primes lying over $\mathfrak{q}_0$, so $\mathfrak{q}$ is the unique prime over $\mathfrak{q}_0$.

Now assume there were some $K \subset E \subset L_{D/\mathfrak{q}}$ with $\mathfrak{q}$ the unique minimal prime above $\mathfrak{q} \cap E$. Then $\mathrm{Gal}(L/E) \subset D_{L,\mathfrak{q}}$. Cardinality count gives equality.

We know that $\#D_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}_0} f_{\mathfrak{q}_0}$. We also know that $[L : k] = m e_\mathfrak{p} f_\mathfrak{p} = (\#D_{\mathfrak{q}/\mathfrak{p}}) \cdot \#$ of cosets. The number of cosets is just the number of primes lying above $\mathfrak{p}$, which is m by definition. Hence $e_\mathfrak{p} f_\mathfrak{p} = e_{\mathfrak{q}_0} f_{\mathfrak{q}_0}$. We also know that inertia degrees and ramification indexes multiply in towers, so $e_{\mathfrak{q}_0} e_{\mathfrak{q}/\mathfrak{p}} = e_\mathfrak{p}$ and likewise with f's. These three equations imply $e_\mathfrak{p} = e_{\mathfrak{q}_0}$ and $f_\mathfrak{p} = f_{\mathfrak{q}_0}$.

October 16th, 2015: Draft

We continue the proof of the theorem from last time. Recall that $R \subset S$ was a finitely generated extension of Dedekind domains with fields of fractions $K \subset L$ of degree n.

Proof (Continued.) The following lemma essentially assures us that subextensions of Dedekind domains preserve our background hypotheses.

73 Lemma

Let E be a subfield extension of L/K (i.e. $L/E/K$). Set $T := S \cap E$. Then T is a Dedekind domain with $\mathrm{Frac}(T) = E$. Further, T is a finitely generated R-module and S is a finitely generated T-module.

Proof That $\mathrm{Frac}(T) = E$ is a straightforward verification. It is clear that T is integrally closed in E. That T is noetherian and a finitely generated R-module follows since R is noetherian and S is a finitely generated R-module. S is a finitely generated T-module since it is a finitely generated module over $R \subset T$. To see that every non-zero prime in T is maximal, apply the going up theorem holds for S/T.

The lemma completes the proof of (i). Now we turn to (ii). We must show $S/\mathfrak{q}$ is normal in $R/\mathfrak{p}$. Pick $\overline{\alpha} \in S/fq$ and consider the minimal polynomial $\overline{f} \in R/\mathfrak{p}[x]$. Lift $\overline{\alpha}$ to $\alpha \in S$ and let $f \in R[x]$ be its minimal polynomial. Since L/K is Galois, L, and therefore S, contains all roots of f. Viewing these in $S/\mathfrak{q}$, it follows that $S/\mathfrak{q}$ contains all roots of f mod $\mathfrak{q}$, which $\overline{f}$ divides, so we have all roots of $\overline{f}$. Since we're assuming separability, $S/\mathfrak{q}$ is Galois over $R/\mathfrak{p}$.

Recall $D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$. This definition gives a map $D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}((S/\mathfrak{q})/(R/\mathfrak{p}))$ whose kernel by definition is $I_{\mathfrak{q}/\mathfrak{p}}$. Hence we need only show surjectivity. Since $S/\mathfrak{q}$ is separable over

$R?\mathfrak{p}$, there exists a primitive element $\overline{\alpha} \in S/\mathfrak{q}$. For $\tau \in \mathrm{Gal}((S/\mathfrak{q})/(R/\mathfrak{p}))$, let $\overline{\beta}$ be such that $\tau(\overline{\alpha}) = \overline{\beta}$. We can lift $\overline{\alpha}, \overline{\beta}$ to $\alpha, \beta \in S$ where f is the minimal polynomial of α and β is a root of f. By transitivity of the Galois group, there is some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$. We claim σ fixes $\mathfrak{q}$—this gap will be filled in later, and it's in Osserman's notes. This proves surjectivity, giving the short exact sequence. From (i), we have $\#D_{\mathfrak{q}/\mathfrak{p}} = e_\mathfrak{p} f_\mathfrak{p}$. By definition, $\#\,\mathrm{Gal}((S/\mathfrak{q})/(R/\mathfrak{p})) = f_\mathfrak{p}$. Hence $\#I_{\mathfrak{q}/\mathfrak{p}} = e_\mathfrak{p}$.

We turn to (iii). By definition of totally ramified and (i), $L_{I,\mathfrak{q}} \supseteq L_{D,\mathfrak{q}}$. From (ii), $[L : L_{I,\mathfrak{q}}] = e_\mathfrak{q}$. Suppose there were another field $E \subset L_{I,\mathfrak{q}}$ such that $\mathfrak{q}' := \mathfrak{q} \cap E$ were totally ramified. Then we could apply (i) and (ii) to L/E instead of L/K. Notice $E \supseteq L_{D/\mathfrak{q}}$. Hence we have

$$\underbrace{L_{D,\mathfrak{q}} \subset E = L_{D,\mathfrak{q}/\mathfrak{q}'} \subset}_{f_\mathfrak{p}} \underbrace{L_{I,\mathfrak{q}} \subset L}_{e_\mathfrak{p}}.$$

Note that $E \subset L_{I,\mathfrak{q}}$ corresponds to $\mathrm{Gal}((S/\mathfrak{q})/(R_E/\mathfrak{q}'))$ which is 1 by the totally ramified assumption and the preceding two observations, so $E = L_{I,\mathfrak{q}}$ is indeed minimal.

Note that if $\mathfrak{q}_1, \mathfrak{q}_2 \subset S$ lying over $\mathfrak{p} \subset R$, then $D_{\mathfrak{q}_1/\mathfrak{p}} = \sigma^{-1} D_{\mathfrak{q}_2/\mathfrak{p}} \sigma$ where $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$, $I_{\mathfrak{q}_1/\mathfrak{p}} = \sigma^{-1} I_{\mathfrak{q}_2/\mathfrak{p}} \sigma$. In particaular, if $\mathrm{Gal}(L/K)$ is abelian, then $D_{\mathfrak{q}/\mathfrak{p}}$ and $I_{\mathfrak{q}/\mathfrak{p}}$ is independent of $\mathfrak{q}$. In particular:

74 Theorem

If $\mathrm{Gal}(L/K)$ is abelian, then $L_{D,\mathfrak{p}}$ is the maximal subextension of L/K where $\mathfrak{p}$ splits completely, and $L_{I,\mathfrak{p}}$ is the maximal subextension where $\mathfrak{p}$ is unramified.

Proof We begin with

75 Proposition

If E, E' are Galois subextensions of L/K and $\mathfrak{p}$ is unramified in E and E', the $\mathfrak{p}$ is unramified in EE'.

Proof The extensions involving E and E' satisfy our background hypotheses by the lemma. We'll prove this in more generality later, so we skip the proof of this special case, though we have been assured it can be filled in non-circularly.

Claim for $L_{D,\mathfrak{p}}$: need to show for all $\mathfrak{q}_0$ lying over $\mathfrak{p}$ that $e_{\mathfrak{q}_0} = f_{\mathfrak{q}_0} = 1$. Since e and f are multiplicative in towers and $e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}/\mathfrak{q}_0}$ and $f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{q}_0}$ for all $\mathfrak{q}$, we have $e_{\mathfrak{q}_0/\mathfrak{p}} = f_{\mathfrak{q}_0/\mathfrak{p}} = 1$.

Claim for $L_{I,\mathfrak{p}}$: can use the same argument; Osserman gives another.

76 Notation

In addition to our background assumptions, further assume $R/\mathfrak{p}$ is finite for all non-zero prime ideals. This holds for rings of integers.

77 Corollary

$D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}}$ is cyclic and generated by a lift of the Frobenius map.

Proof The Galois group in this case is cyclically generated by the Frobenius map.

78 Definition

Suppose $\mathfrak{q}$ is lying over $\mathfrak{p}$ with $e_\mathfrak{p} = 1$. Then $\boxed{\mathrm{Fr}(\mathfrak{q}/\mathfrak{p})}$ is the unique element of the decomposition group $D_{\mathfrak{q}/\mathfrak{p}}$ that maps to the Frobenius map. If L/K is abelian, write $\mathrm{Fr}(\mathfrak{p})$ for any $\mathrm{Fr}(\mathfrak{q}/\mathfrak{p})$.

The Frobenius element will show up again in class field theory.

October 19th, 2015: Draft

Bianca is away for two lectures. We'll discuss cyclotomic fields and essentially have a series of extended examples.

79 Outline

(1) Cyclotomic fields, namely $\boxed{\mathbb{Q}(\zeta)/\mathbb{Q}}$

  (a) Show $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$

  (b) Consider decomposition of primes

(2) Application: proving Fermat's Last Theorem for regular primes, of which there are conjecturally infinitely many

80 Notation

Fix a primitive nth root of unity $\zeta := \zeta_n = e^{2\pi i/n}$. Let ℓ be a prime and suppose $n = \ell^\nu$. Write $K := \mathbb{Q}(\zeta)$.

81 Proposition

Set $\lambda := 1 - \zeta$.

- *(λ) is a prime ideal of $\mathcal{O}_K$ with interia degree $f = 1$*
- *$\ell\mathcal{O}_K = (\lambda)^{\phi(n)}$ where ϕ is Euler's totient function, $\phi(\ell^\nu) = \ell^{\nu-1}(\ell - 1) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$.*

Proof The minimal polynomial of ζ over $\mathbb{Q}$ is classically the nth $\boxed{\text{cyclotomic polynomial}}$ $\boxed{\Phi_n(x)}$, namely

$$\Phi_n(x) = \prod_{\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta^\sigma) = \frac{(x^{\ell^{\nu-1}})^\ell - 1}{x^{\ell^{\nu-1}} - 1} = (x^{\ell^{\nu-1}})^{\ell-1} + \cdots + x^{\ell^{\nu-1}} + 1.$$

Since there are ℓ factors, plugging in $x = 1$ gives $\ell = \prod_{\sigma\in(\mathbb{Z}/n\mathbb{Z})^\times}(1 - \zeta^\sigma)$. Now fix $\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$ and write $1 - \zeta^\sigma = (1 - \zeta^\sigma)/(1 - \zeta)\lambda$. We claim the fraction is a unit in the ring of integers. Using the geometric series and the fact that ζ is in $\mathcal{O}_K$, the fraction is also in $\mathcal{O}_K$. To show that its inverse is as well, pick $\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma\tau \equiv_n 1$. Then its inverse is

$$\frac{1 - \zeta}{1 - \zeta^\sigma} = \frac{1 - (\zeta^\sigma)^\tau}{1 - \zeta^\sigma} \in \mathcal{O}_K.$$

Now $\ell = (\text{units})\lambda^{\phi(n)}$, so $\ell\mathcal{O}_K = (\lambda)^{\phi(n)} = (\lambda_1 \cdots \lambda_r)^{\phi(n)}$. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$, from our earlier theorem we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \sum e_i f_i = (\#\text{ primes}) \cdot e \cdot f$, and we've already accounted for $\phi(n)$ factors, we must have $r = 1, f = 1, e = \phi(n)$, so λ is prime with $f = 1$.

82 Notation

Let $\mathcal{B} := \{1, \zeta, \zeta^2, \ldots, \zeta^{\phi(n)-1}\}$ be the usual $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$. We continue to have $n = \ell^\nu$.

83 Proposition

$\operatorname{Disc}\mathcal{B} = \pm\ell^\mu$.

Proof Let $\zeta_1, \ldots, \zeta_{\phi(n)}$ be the $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$-conjugates of ζ and again write $\Phi_n(x) = \prod_{i=1}^{\phi(n)}(x - \zeta_i)$. From our earlier lemma, up to a unit we have $\operatorname{Disc}\mathcal{B}$ is the Vandermonde determinant $\prod_{i\neq j}(\zeta_i - \zeta_j)$. If we apply the product rule, we find

$$\Phi_n'(x) = \sum_i \prod_{j\neq i}(x - \zeta_j),$$

so that

$$\pm\operatorname{Disc}\mathcal{B} = \prod_{i\neq j}(\zeta_i - \zeta_j) = \prod_{i=1}^{\phi(n)} \Phi_n'(\zeta_i) = N_{K/\mathbb{Q}}(\Phi_n'(\zeta)).$$

On the other hand, $(x^{\ell^\nu - 1})\Phi_n(x) = x^{\ell^\nu} - 1$, so differentiating gives

$$\Phi_n'(\zeta) = \frac{\ell^\nu \cdot \zeta^{-1}}{\zeta^{\ell^{\nu-1}} - 1}.$$

Since the norm is multiplicative, we consider each piece. Note that $N_{K/\mathbb{Q}} = \pm\ell$ since the constant term of $\Phi_n(1-\lambda)$ is $\Phi_n(1) = \ell$. Similarly, if we replace ν with $\nu - s$, then

$$N_{\mathbb{Q}(\zeta_{\ell^s})/\mathbb{Q}}(1 - \zeta^{\ell^s}) = \pm\ell.$$

We know that $N_{M/K} = N_{L/K} \circ N_{M/L}$ and that $N_{M/L}(\alpha) = \alpha$ for $\alpha \in L$. Putting it all together, $N_{K/\mathbb{Q}}(1 - \zeta^{\ell^s}) = \pm\ell^m$, so that $\operatorname{Disc}\mathcal{B} = \pm\ell^\mu$.

84 Remark

$[\mathcal{O}_K : \mathbb{Z}[\zeta]] = \ell^m$. Hence $\ell^{m'}\mathcal{O}_K \subset \mathbb{Z}[\zeta]$ for m' large enough. Note that $\operatorname{Disc}(\mathcal{O}_K/\mathbb{Z})[\mathcal{O}_K : \mathbb{Z}(\zeta)]^2 = \operatorname{Disc}\mathcal{B}$.

85 Theorem

If $K = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\ell^\nu})$, then $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Proof Again let $\lambda := 1 - \zeta$. Since $f = 1$, $[\mathcal{O}_K/\lambda\mathcal{O}_K : \mathbb{F}_\ell] = 1$, so $\mathcal{O}_K/\lambda\mathcal{O}_K \cong \mathbb{Z}/\ell\mathbb{Z}$. Hence $\mathcal{O}_K = \mathbb{Z} + \lambda\mathcal{O}_K$, so $\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda\mathcal{O}_K$. Multiply this last expression by λ and substitute the resulting right-hand side in for $\lambda\mathcal{O}_K$ in this last expression to get $\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda\mathbb{Z}[\zeta] + \lambda^2\mathcal{O}_K$. We can of course ignore the middle term. Iterating this computation, we find

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda^t\mathcal{O}_K \qquad t \geq 1.$$

If we use the observation in the remark, if $\ell\mathcal{O}_K = (\lambda)^{\phi(n)}$, letting $t = \phi(n)m'$ gives $\mathcal{O}_K = \mathbb{Z}[\zeta] + \ell^{m'}\mathcal{O}_K = \mathbb{Z}[\zeta]$.

86 Notation

We now consider general n, so write $n := \ell_1^{\nu_1} \cdots \ell_s^{\nu_s}$. For notational convenience, write $\zeta_i := \zeta_n^{n/\ell_i^{\nu_i}}$ and let $\mathcal{B}_i := \{1, \zeta_i, \ldots\}$ be the corresponding basis.

87 Remark

Notice that $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1) \cdots \mathbb{Q}(\zeta_s)$ since the ℓ_i's are coprime, and $\mathbb{Q}(\zeta_1) \cdots \mathbb{Q}(\zeta_i) \cap \mathbb{Q}(\zeta_{i+1}) = \mathbb{Q}$. (For the intersection identity, suppose $p \neq q$ are two primes and consider $K \subset \mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q)$. Consider those subfields in which p and q are totally ramified–the result will follow immediately.)

We have $\operatorname{Disc}\mathcal{B}_i = \pm\ell_i^{\mu_i}$ are pairewise coprime. A technical lemma (Neukirch, 2-11) says that in this situation $\zeta_1^{\alpha_1} \cdots \zeta_s^{\alpha_s}$ as $\alpha_i \in \mathbb{Z}$ varies forms a $\mathbb{Z}$-basis for the ring of integers of the product $\mathbb{Q}(\zeta)$. Hence if $\alpha \in \mathcal{O}_K$, $\alpha = f(\zeta)$ for $f \in \mathbb{Z}[x]$. Now $\deg f \leq \phi(n) - 1$, which says $\{1, \zeta, \ldots, \zeta^{\phi(n)-1}\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{\mathbb{Q}(\zeta)}$.

October 21st, 2015: Draft

Francesca will continue lecturing today on cyclotomic extensions, the splitting behavior of their primes, and Fermat's Last Theorem.

88 Theorem

Let $n = \prod_p p^{\nu_p}$. For each p let f_p be the smallest positive integer such that $p^{f_p} \equiv_{n/p^{\nu_p}} 1$. Then

$$p\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \left(\prod_{i=1}^{r} \mathfrak{p}_i\right)^{\phi(p^{\nu_p})}$$

where $r := \phi(n/p^{\nu_p})/f_p$.

Proof Last time, we saw $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, so trivially $[\mathcal{O}_{\mathbb{Q}(\zeta_n)} : \mathbb{Z}[\zeta_n]]$. By (what is sometimes called) Dedekind-Kummer, study $\Phi_n(x)$ mod p. Fix p and let $n = p^{\nu_p}u$ for $(p, u) = 1$. Since $\zeta^n = 1 = \zeta^{p^{\nu_p}u}$ let $\zeta_u := \zeta^{p^{\nu_p}}$, which is a primitive uth root of unity. Likewise set $\zeta_{p^{\nu_p}} := \zeta^u$, which is a p^{ν_p}th root of unity.

We know that $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_u)\mathbb{Q}(\zeta_{p^{\nu_p}})$, if we consider $\zeta_u^i \cdot \zeta_{p^{\nu_p}}^j$ for $i \in (\mathbb{Z}/u\mathbb{Z})^\times$, $j \in (\mathbb{Z}/p^{\nu_p}\mathbb{Z})^\times$ varying, we get all the primitive roots of unity. Therefore

$$\Phi_n(x) = \prod_{\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta^\sigma) = \prod_{i \in (\mathbb{Z}/u\mathbb{Z})^\times} \prod_{j \in (\mathbb{Z}/p^{\nu_p}\mathbb{Z})^\times} (x - \zeta_u^i \cdot \zeta_{p^{\nu_p}}^j).$$

Note that $x^{p^{\nu_p}} - 1 \equiv_p (x-1)^{p^{\nu_p}}$. Hence $\zeta_{p^{\nu_p}}^j \equiv_p 1$. Moreover, this remains true for any $\mathfrak{p} \mid (p)$. Using this observation in the above expression gives

$$\Phi_n(x) \equiv_p \left(\prod_{i \in (\mathbb{Z}/u\mathbb{Z})^\times} (x - \zeta_u^i) \right)^{\phi(p^{\nu_p})} \equiv_p \Phi_u(x)^{\phi(p^{\nu_p})}.$$

So, we reduce to studying how $\Phi_u(x)$ splits mod p.

Now let $\mathcal{O} := \mathcal{O}_{\mathbb{Q}(\zeta_u)}$, and note that $p = \operatorname{char} \mathcal{O}/\mathfrak{p} \nmid u$ for any $\mathfrak{p}$ lying over (p). Hence the derivative of $x^u - 1$ is ux^{u-1} which has roots only at 0, so $x^u - 1$ has distinct linear factors over $\mathcal{O}/\mathfrak{p}$. It follows that if ζ_u is a primitive uth root of unity, then so is $\overline{\zeta}_u \in \mathcal{O}/\mathfrak{p}$, and moreover the quotient map induces a bijection between primitive uth roots of unity of either ring. We claim that the smallest subextension of $(\mathcal{O}/\mathfrak{p})/\mathbb{F}_p$ containing $\overline{\zeta}_u$ is $\mathbb{F}_{p^{f_p}}$. (Recall that $\mathbb{F}_{p^{f_p}}^\times$ is cyclic of order $p^{f_p} - 1$.) It follows that $\mathbb{F}_{p^{f_p}}/\mathbb{F}_p$ is the splitting field of $\overline{\Phi_u(x) \bmod p}$. We also know that $\Phi_u(x) \mid x^u - 1$, so both are separable over $\mathbb{F}_p$. Hence we can write $\Phi_u(x) = \overline{f}_1(x) \cdots \overline{f}_k(x)$ over $\mathbb{F}_p$ using distinct irreducible factors. Each factor must then be a minimal polynomial over $\mathbb{F}_p$ of some $\overline{\zeta}_u$. But the largest field in which $\overline{\zeta}_u$ is defined is a degree f_p extension, so $\deg \overline{f}_i = f_p$, completing the proof.

(An alternative argument: if $p \nmid u$, then p is unramified, so $e = 1 = \#I_p$. There is a short exact sequence $1 \to I_p \to D_p \to \operatorname{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p) \to 1$, where $\mathbb{F}_\mathfrak{p} := \mathcal{O}/\mathfrak{p}$. Hence the kernel is trivial, so the Galoi group is isomorphic to D_p. The Galois group is of course cyclically generated by the Frobenius map σ. By $p^f \equiv_u 1$, we have $|\sigma| = f$.)

89 Corollary

Let $p \neq 2$. Then

- *p is ramified in $\mathbb{Q}(\zeta_n)$ if and only if $n \equiv_p 0$.*
- *p is totally split in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv_n 1$.*

90 Remark

Note that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an *abelian* extension of $\mathbb{Q}$. Class field theory vastly generalizes these congruence condition-style results for abelian extensions. Similarly, recall $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv_4 1$, and $\left(\frac{-1}{p}\right) = -1$ iff $p \equiv_4 3$, which is another manifestation of these congruence results.

91 Theorem (Gauss' Reciprocity Law)

Let $l \neq p$ be odd primes. Then

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

92 Proposition

Proof *Let ℓ, p be as above. Then p is totally split in $\mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell})$ if and only if p can be decomposed into an even number of primes in $\mathbb{Q}(\zeta_\ell)$.*

Proof It is “easy to see” that $\mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell}) \subset \mathbb{Q}(\zeta_\ell)$.

For ⇒, suppose p is totally split in the smaller field. Roughly, consider the primes above p in the smaller field, and then consider the primes above those primes in the larger field. It is quite easy to see that there exists an automorphism $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_\ell))$ sending any prime $\mathfrak{p}_1$ lying over p to any other prime $\mathfrak{p}_2$ which also sends the primes lying over $\mathfrak{p}_1$ bijectively onto those lying over $\mathfrak{p}_2$, so the number of such primes is the same. In particular, there are an even number of primes lying over p.

For ⇐, let r be the number of primes in $\mathbb{Q}(\zeta_\ell)$ lying above p. Assume r is even. Then by the Fundamental Theorem of Galois Theory,

$$[\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)) : D_p] = [\mathbb{Q}(\zeta_\ell)_p^D : \mathbb{Q}]$$

is even. But ℓ is a prime, so $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$ is cyclic. This gives rise to a tower of extensions

$$\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_\ell)^{D_p}/\mathbb{Q},$$

where the second degree is even. It follows that $\mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell}) \subset \mathbb{Q}(\zeta_\ell)^{D_p}$. Now looking at any $\mathfrak{p}$ over p, $\mathfrak{p} \cap \mathbb{Q}(\zeta_\ell)^{D_p}$ has inertia degree 1, so $\mathfrak{p} \cap \mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell})$ also has inertia degree 1. Therefore p is totally split in $\mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell})$.

The rest of the proof is left as an exercise–it's a sequence of equivalences. It is also in Neukirch.

No time for Fermat's Last Theorem, though it's in Osserman.

October 23rd, 2015: Draft

We've essentially finished chapters 1-3 in Osserman. We'll start in on chapter 4. Recall that our main motivation was finding primes of the form $p = x^2 + ny^2$, and more generally for related equations. We saw we need to determine (1) how (p) factors in $\mathcal{O}_K$ (or $\mathcal{O} \subset \mathcal{O}_K$), particularly when (p) factors into principal ideals of some form, and (2) the unit group $\mathcal{O}_K^\times$ (or $\mathcal{O}^\times$). Our previous results were typically quite general, but in this chapter we'll restrict to number fields and rings of integers.

93 Notation
Let K be a number field and let $\mathcal{O}_K$ be its ring of integers.

94 Definition
Let $\boxed{I_K}$ denote the set of fractional ideals of $\mathcal{O}_K$ and let $\boxed{P_K}$ denote the set of principal practional ideals of $\mathcal{O}_K$. We saw already that I_K is a(n abelian) group, and P_K is a subgroup. Define the $\boxed{\text{class group}}$ of K as

$$\boxed{\mathrm{Cl}_K} := I_K/P_K.$$

Write $\boxed{r_1}$ for the number of real embeddings $K \hookrightarrow \mathbb{R}$, and write $\boxed{r_2}$ for half the number of complex embeddings $K \hookrightarrow \mathbb{C}$ (where a complex embedding does not factor through $\mathbb{R} \hookrightarrow \mathbb{C}$). Note $[K : \mathbb{Q}] = n = r_1 + 2r_2$.

Our focus will now be on proving the following two main theorems:

95 Theorem (Finiteness of the Class Group)
Cl_K *is finite.*

96 Theorem (Dirichlet's Unit Theorem)
$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1}$, *where* $\mu_K := \{x \in K : x^m = 1$ *for some* $m\}$ *(which is finite).*

The following is perhaps the "most general" thing we know about the class group, of which finiteness of the class group is a corollary:

97 Theorem (Minkowski)
Let $I \in I_K$*. Then there exists* $z \in K^\times$ *such that* $zI \subset \mathcal{O}_K$ *and*

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

98 Remark
To show finiteness of Cl_K from here, it suffices to show there are finitely many integral ideals of norm m. For that, let $J \subset \mathcal{O}_K$ be an integral ideal and suppose $N(J) = m$. Write the prime factorization $J = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$. Note that $N(J) = \#\mathcal{O}_K/J$ and $\mathcal{O}_K/J \cong \prod_i \mathcal{O}_K/\mathfrak{p}_i^{e_i}$, so $N(J) = \prod_i N(\mathfrak{p}_i^{e_i}) = \prod_i p_i^{e_i f_i} = m$. (Note the p_i's may not be distinct if two of the $\mathfrak{p}_i$'s lie over the same rational prime). Hence there are only finitely many choices of p_i, e_i, f_i, and finitely many $\mathfrak{p}_i$ lie over those finitely many p_i, giving the result.

Note: you can slightly generalize this argument to show $N(IJ) = N(I)N(J)$, which we will use.

We will deduce Minkowski's theorem from the following:

99 Theorem
Let $J \subset \mathcal{O}_K$ *be an integral ideal. Then there exists* $x \in J$ *such that*

$$|N_{K/\mathbb{Q}}(x)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} N(J)|D_K|^{1/2}.$$

100 Remark
To deduce Minkowski's theorem, let $I \in I_K$ and let $x \in I$. Then $xI^{-1} \subset \mathcal{O}_K$, do spply the theorem to get $y \in xI^{-1}$ such that

$$|N_{K/\mathbb{Q}}(y)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} N(xI^{-1})|D_K|^{1/2}$$

. Since $y \in xI^{-1}$, $\frac{y}{x}I \subset \mathcal{O}_K$ is integral, and

$$N(\frac{y}{x}I) = N(y(xI^{-1})^{-1}) = |N_{K/\mathbb{Q}}(y)|/N(xI^{-1}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |D_K|^{1/2}.$$

We will deduce Theorem 99 by a sequence of arguments involving lattices and convex subsets of $\mathbb{R}^n$.

101 Definition
Define an embedding $\boxed{\phi \colon K \to \mathbb{R}^n}$ by $\phi \colon K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ followed by the identification $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$.

Let $L \subset \mathbb{R}^n$ be a full rank lattice and let $\mathcal{F}_L$ be a fundamental domain. More precisely, if $v_1, \ldots, v_n$ is an integral basis for L, then $\mathcal{F}_L := \{\sum_i a_i v_i : 0 \leq a_i < 1\}$.

102 Theorem
If $I \subset \mathcal{O}_K$ *is an integral ideal, then* $\phi(I)$ *is a rank* n *lattice in* $\mathbb{R}^n$*, and* $\mathrm{vol}\,\mathcal{F}_{\phi(I)} = 2^{-r_2} N(I)|D_K|^{1/2}$.

103 Theorem

Let $t \in \mathbb{R}_{>0}$. Then there exists a compact convex region $R_t \subset \mathbb{R}^n$ that is symmetric about the origin such that

$$\mathrm{vol}(R_t) = 2^{r_1 - r_2} \pi^{r_2} \frac{t^n}{n!}.$$

Moreover, for all $x \in K$ with $\phi(x) \in R_t$,

$$|N_{K/\mathbb{Q}}(x)| \leq \frac{t^n}{n^n}.$$

(Minor note: there is a typo in Osserman's notes, which says $<$ instead of $\leq$.)

104 Theorem (Minkowski, again)

Let $R \subset \mathbb{R}^n$ be a compact convex region that is symmetric about the origin and let $L \subset \mathbb{R}^n$ be a lattice of full rank. If $\mathrm{vol}(R) \geq 2^n \mathrm{vol}(\mathcal{F}_L)$, then R contains a non-zero lattice point of L.

105 Remark

Theorems 102, 103, 104 imply Theorem 99:

Proof Let $J \subset \mathcal{O}_K$ and set $t := (n! \left(\frac{4}{\pi}\right)^{r_2} N(J)|D_K|^{1/2})^{1/n}$. By Theorem 102, $\phi(J)$ is a lattice of full rank. By Theorem 103, we have R_t where

$$\begin{aligned}\mathrm{vol}(R_t) &= 2^{r_1 - r_2}\pi^{r_2}\left(\frac{4}{\pi}\right)^{r_2} N(J)|D_K|^{1/2} \\ &= 2^{r_1+r_2} N(J)|D_K|^{1/2} \\ &= (2^n)(2^{-r_2}N(J)|D_K|^{1/2}) \\ &= 2^n \,\mathrm{vol}(\mathcal{F}_{\phi(J)})\end{aligned}$$

where the last equality used Theorem 102. Now Theorem 104 gives a non-zero element of $\phi(J) \cap R_t$. Then Theorem 103 says that for the corresponding $x \in J$, $N(x) < \frac{t^n}{n^n}$.

Next week will be devoted to proving Theorems 102, 103, 104.

October 26th, 2015: Draft

Summary Recall Theorem 102 from last time, that if $I \subset \mathcal{O}_K$ is a non-zero ideal, then $\phi(I)$ is a lattice of full rank and $\mathrm{vol}(\mathcal{F}_{\phi(I)}) = 2^{-r_2}N(I)|D_K|^{1/2}$. We turn to its proof.

We maintain all the notation from last time.

Proof (Of Theorem 102) Recall that I is a free $\mathbb{Z}$-module of rank n, where $D(I) = \mathrm{Disc}_{K/\mathbb{Q}}((x_i))$ where x_i is a $\mathbb{Z}$-basis for I. That $\phi(I)$ is a lattice of full rank then follows by standard theory, so we need only compute the volume.

106 Lemma

Let $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ and let $\phi_{\mathbf{x}}$ be the $n \times n$ matrix with real entries whose rows are $\phi(x_i)$. Then

$$D_{K/\mathbb{Q}}((x_i)) = (-4)^{r_2}(\det \phi_{\mathbf{x}})^2.$$

In particular, the sign of $D_{K/\mathbb{Q}}$ is independent of $\curvearrowleft$ and depends only on r_2.

Proof Consider $\sigma_{\mathbf{x}} \in M_n(\mathbb{C})$ whose ith row is

$$(\sigma_1(x_i), \ldots, \sigma_{r_1}(x_i), \sigma_{r_1+1}(x_i), \overline{\sigma_{r_1+1}(x_i)}, \overline{\sigma_{r_1+2}(x_i)}, \ldots, \overline{\sigma_{r_1+r_2}(x_i)}).$$

We know that $D_{K/\mathbb{Q}}((x_i)) = (\det(\sigma_{\mathbf{x}}))^2$. Consider the j and $j+1$ columns of $\phi_{\mathbf{x}}$ and $\sigma_{\mathbf{x}}$:

$$\begin{pmatrix} a_1 & b_1 \\ \vdots & \vdots \\ a_n & b_n \end{pmatrix} \qquad \begin{pmatrix} a_1 + ib_1 & a_1 - ib_1 \\ \vdots & \vdots \\ a_n + ib_n & a_n - ib_n. \end{pmatrix}$$

The determinant of $\phi_{\mathbf{x}}$ agrees with that obtained from

$$\begin{pmatrix} a_1 + ib_1 & b_1 \\ \vdots & \vdots \\ a_n + ib_n & b_n \end{pmatrix}$$

and to go to the determinant of $\sigma_{\mathbf{x}}$ we multiply this determinant by $(-2i)^{r_2}$. Hence

$$(\det \phi_{\mathbf{x}})^2(-4)^{r_2} = (\det \sigma_{\mathbf{x}})^2.$$

Continuing the proof of the theorem, we have

$$\operatorname{vol}(\mathcal{F}_{\phi(I)}) = |\det \phi_{\mathbf{x}}| = 2^{-r_2}|D(I)|^{/1/2}$$

where $\mathbf{x}$ is a $\mathbb{Z}$-basis for I; the first equality uses standard multivariable calculus, and the second uses the lemma. By definition, $N(I)$ is the index of $I \subset \mathcal{O}_K$. Now $D(I) = N(I)^2 D(\mathcal{O}_K)$, from which the result follows.

Summary Recall Theorem 103, that if $t \in \mathbb{R}_{>0}$, then there exists $R_t \subset \mathbb{R}^n$ that is compact, convex, and symmetric about the origin such that

(1) $\operatorname{vol}(R_i) = 2^{r_1 - r_2}\pi^{r_2} t^n/n!$

(2) For all $x \in K$ such that $\phi(x) \in R_t$, $N_{K/\mathbb{Q}}(x)| \leq t^n/n^n$.

Proof We claim that

$$R_t := \left\{ \mathbf{x} \in \mathbb{R}^n : |x_1| + \cdots + |x_{r_1}| + 2\sqrt{x_{r_1+1}^2 + x_{r_1+2}^2} + \cdots + 2\sqrt{x_{n-1}^2 + x_n^2} \right\}$$

has the desired properties. Compactness and symmetry are clear. For convexity, write $||\mathbf{x}||$ for the quantity above and let $\mathbf{y}, \mathbf{z} \in R_t$ with $0 \leq \lambda \leq 1$. We see that $\lambda\mathbf{y} + (1-\lambda)\mathbf{z} \in R_t$ since

$$||\lambda\mathbf{y} + (1-\lambda)\mathbf{z}|| \leq ||\lambda\mathbf{y}|| + ||(1-\lambda)\mathbf{z}|| \leq t(\lambda + (1-\lambda)) = t.$$

For the second point, recall that

$$|N_{K/\mathbb{Q}}(\mathbf{x})| = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r_1} |\sigma_i(\mathbf{x})| \prod_{j=1}^{r_2} |\sigma_j(x)|^2.$$

From the arithmetic-geometric mean inequality, we find

$$(N_{K/\mathbb{Q}}(\mathbf{x}))^{1/n} \leq \frac{\sum_{i=1}^{r_1} |\sigma_i(x)|}{n} + 2\sum_{j=r_1+1}^{r_2} |\sigma_j(\mathbf{x})| \leq \frac{||x||}{n} \leq \frac{t}{n}.$$

Finally, for the volume computation, see Lang, page 117, which integrates in polar.

Summary Recall Theorem 104, where if $R \subset \mathbb{R}^n$ is a compact convex region symmetric about the origin and $L \subset \mathbb{R}^n$ is a lattice of full rank, and if $\operatorname{vol}(R) \geq 2^n \operatorname{vol}(\mathcal{F}_L)$, then R contains a non-zero lattice point of L.

Note: we can modify the theorem statement by replacing "compact" with "bounded" at the cost of using strict inequality and get the same result.

Proof (Of Theorem 104) We begin with...

107 Lemma

Let R be a bounded region and let $L \subset \mathbb{R}^n$ be a lattice of full rank. If all translates of R under L are disjoint, then $\mathrm{vol}(R) \leq \mathrm{vol}(\mathcal{F}_L)$.

Proof (Minor note: "volume" of an arbitrary region isn't well-defined, though our regions are incredibly nice–compact sets, or the open set of points $< \epsilon$ from such a set. So, we will be a bit vague in measure-theoretic details.) Recall the partition $\mathbb{R}^n = \coprod_{v \in L} \mathcal{F}_L + v$. Hence

$$\begin{aligned} R &= \coprod_{v \in L} (R \cap (\mathcal{F}_L + v)) \\ &= \cup_{v \in L}((R - v) \cap \mathcal{F}_L) + v. \end{aligned}$$

Since $(R + w) \cap (R + w') = \varnothing$ for all $w \neq w' \in L$ by assumption, so this latter union is actually a disjoint union as well. Hence

$$\mathrm{vol}(R) = \mathrm{vol}(\cup_{v \in L}((R - v) \cap \mathcal{F}_L)) \leq \mathrm{vol}(\mathcal{F}_L).$$

We now prove the modified version of the theorem, which we will use to deduce the stated version. Since $\frac{1}{2^n} \mathrm{vol}(R) > \mathrm{vol}(\mathcal{F}_L)$, by the lemma we have $v \neq w \in L$ such that $(\frac{1}{2}R + v) \cap (\frac{1}{2}R + w) \neq \varnothing$. Let x belong to the intersection, so that $x - v, x - w \in \frac{1}{2}R$. By symmetry and convexity, $\frac{(x-v)-(x-w)}{2} \in \frac{1}{2}R$, so $w - v \in R$ is the desired non-zero lattice point.

We will defer the proof of Theorem 104 as stated from this modified version till next class. (Osserman's is a bit complicated and has a typo.)

October 29th, 2015: Draft

---

108 Aside

There was a mistake on HW2, problem 1. "kernel consists of ideals that meet S" should say "kernel is generated by integral ideals that meet S".

Also, Neukirch gives a somewhat different bound than the above, but it is always worse than the bound we obtained. Neukirch also outlines our proof in the exercises.

109 Definition

A subset $L \subset \mathbb{R}^n$ is called a $\boxed{\text{discrete subgroup}}$ if

1) it is a subgroup under pointwise addition

2) there exists $\epsilon > 0$ such that for all $v \in L$, $B_\epsilon(v) \cap L = \{v\}$.

(As it turns out, the order of the quantifiers in 2) can be switched.)

A $\boxed{\text{lattice}}$ in $\mathbb{R}^n$ is the $\mathbb{Z}$-span of a set of $\mathbb{R}$-linearly independent vectors.

110 Lemma

Let $L \subset \mathbb{R}^n$. Then L is a lattice if and only if L is a discrete subgroup.

Proof See homework.

Last time we proved a modified version of Theorem 104. Namely, if R is bounded, convex, and symmetric about the origin and if L is a lattice of full rank, and if $\mathrm{vol}(R) > 2^n \mathrm{vol}(\mathcal{F}_L)$, then R contains a non-zero lattice point. Now we wish to deduce Theorem 104 itself, namely, if R is compact, convex, and symmetric about the origin and $\mathrm{vol}(R) \geq 2^n \mathrm{vol}(\mathcal{F}_L)$, then R contains a non-zero lattice point.

Proof (Of THeorem 104) For all $\epsilon > 0$, $\mathrm{vol}((1+\epsilon)R) > 2^n \mathrm{vol}(\mathcal{F}_L)$, so $(1+\epsilon)R$ contains a non-zero lattice point v_ϵ. We also know that $2R$ is bounded, so since L is a discrete subgroup, there are finitely many lattice points in $2R$ by compactness and condition (2). Hence the v_ϵ must hit some particular non-zero lattice point infinitely often as $\epsilon \to 0$, which is then in $\cap_{\epsilon>0}(1+\epsilon)R = R$ (using compactness at the end).

Having proven finiteness of the class group, our next goal is:

111 Theorem (Dirichlet's Unit Group Theorem)

Let $\mathcal{O} \subset \mathcal{O}_K$ be an order of a ring of integers. Then

$$\mathcal{O}^\times \cong \mu_{\mathcal{O}} \times \mathbb{Z}^{r_1+r_2-1},$$

where $\mu_{\mathcal{O}} := \{x \in \mathcal{O} : x^n = 1 \text{ for some } n\}$ is a finite cyclic group.

To prove this, we'll again use lattices. This time we'll consider

$$\begin{aligned}&\psi\colon K^\times \to \mathbb{R}^{r_1+r_2}\\ &x \mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, 2\log|\sigma_{r_1+1}|, \ldots, 2\log|\sigma_{r_1+r_2}|)\end{aligned}$$

We will deduce Dirichlet from the following result:

112 Proposition

The image $\psi(\mathcal{O}^\times)$ is a lattice of rank r_1+r_2-1, and it spans the hyperplane H given by $x_1+\cdots+x_{r_1+r_2} = 0$.

Proof (Of Dirichlet, Theorem 111) This proposition implies that $\mathcal{O}^\times / \ker\psi|_{\mathcal{O}^\times} \cong \mathbb{Z}^{r_1+r_2-1}$. Let $x \in \ker\psi|_{\mathcal{O}^\times}$. Then $|\sigma_i(x)| = 1$ for all i implies $|\sigma_i(x^j)| = 1$ for all i, j, so $\psi(\{x^j\}_{j\in\mathbb{N}})$ lies in a bounded region. Using the embedding $\phi\colon K \hookrightarrow \mathbb{R}^n$ from the above arguments, $\phi(\mathcal{O}_K)$ is a lattice, so $\phi(\{x^j\})$ must be a finite set, so $\{x^j\}$ is a finite set since ϕ is injective, so $x^n = 1$ for some n. Since $[K : \mathbb{Q}]$ is finite, it follows that $\mu_{\mathcal{O}}$ is finite (we could alternatively expand the set $\{x^j\}$ in the above). That it is cylic is a standard result:

113 Lemma

Every finite subgroup G of $F^\times$ for a field F is cyclic.

Proof There are many arguments. Let m be the least common multiple of $x \in G$ Them $m \mid |G|$. On the other hand, every $x \in G$ is a root of $T^m - 1$, so $|G| \leq m$, so $|G| = m$. One may produce an element of order m by an inductive argument, or by using the classification of finitely generated abelian groups, or the Sylow theorems.

Proof (Of Proposition) Obviously $\mathcal{O}^\times \subset \mathcal{O}_K^\times$. So, for all $x \in \mathcal{O}^x\times$,

$$1 = |N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \prod_{j=1}^{r_2} |\sigma_{j+r_1}(x)|^2.$$

Take log of both sides to get $\sum(\psi(x)_i) = 0$, so the image lies in the suggested hyperplane. We want to show that in any bounded region, $\psi(\mathcal{O}^\times)$ has finitely many points. Assuming this, we then have that $\psi(\mathcal{O}^\times)$ is a discrete subgroup (using the fact that ψ is a group homomorphism).

For the claim, let R be a bounded region. Then there exists $c_1, \ldots, c_{r_1+r_2}$ such that for every $x = \psi(y) \in \psi(\mathcal{O}^\times) \cap R$, $\log|\sigma_i(y)| \leq c_i$. Hence $\sigma_i(y)| \leq e^{c_i}$, so $\phi(y)$ is contained in a bounded region. But $\phi(y) \in \phi(\mathcal{O}_K)$ is a lattice, so all $\phi(y)$ are contained in a finite set, so again since ϕ is an embedding, all y are contained in a finite set.

As an aside, we now have the machinery to define:

114 Definition

The $\boxed{\text{regulator}}$ of $\mathcal{O}$ is

$$\mathrm{vol}(\mathcal{F}_{\psi(\mathcal{O}^\times)} \subset H).$$

We likely won't use the regular in this class, though it comes up, especially in analytic studies of number fields. (When $r_1 + r_2 - 1 = 0$, the regular is defined to be 1.)

All that remains is that $\psi(\mathcal{O}^\times)$ spans H. For that, we show

115 Lemma

(1) $\phi(\mathcal{O})$ is a lattice of full rank

(2) $\mathcal{O}/I$ is finite for any ideal $0 \neq I \subset \mathcal{O}$

(3) $\mathcal{O}$ is noetherian and every non-zero prime ideal is maximal

(4) For all $0 \neq x \in \mathcal{O}$, there exist only finitely many ideals containing x.

Proof Each is straightforward and typically follows from an earlier argument where we showed the corresponding property for the ring of integers.

We'll finish the proof next time.

October 30th, 2015: Draft

We were finishing a proof at the end of last lecture, the remaining part of which is encapsulated in the following proposition:

116 Proposition

The image $\psi(\mathcal{O}^\times)$ spans the hyperplane $x_1 + \cdots + x_{r_1+r_2} = 0$.

117 Notation

To be clear, $\sigma_1, \ldots, \sigma_{r_1}$ are the r_1 real embeddings of K, $\sigma_{r_1+1}, \ldots, \sigma_{r_2}$ are r_2 fo the $2r_2$ complex embeddings, and $\sigma_i = \overline{\sigma_j}$. We had defined

$$\begin{tikzcd}
\phi\colon K \arrow[r] \arrow[dr, "(\sigma_i)"'] & \mathbb{R}^n \\
& \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \arrow[u, "\sim"]
\end{tikzcd}$$

and

$$\begin{aligned}
\psi\colon K^\times &\to \mathbb{R}^{r_1+r_2} \\
x &\mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, 2\log|\sigma_{r_1+1}(x)|, \ldots, 2\log|\sigma_{r_1+r_2}(x)|).
\end{aligned}$$

We will further define a multiplication $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ induced by coordinate-wise multiplication on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Also define the norm map

$$\begin{aligned} N \colon \mathbb{R}^n &\to \mathbb{R}_{\geq 0} \\ (x_1, \ldots, x_n) &\mapsto \prod_{i=1}^{r_1} |x_i| \prod_{j=1}^{r_2} |x_{r_1+2j-1}^2 + x_{r_1+2j}^2| \end{aligned}$$

and also define

$$\begin{aligned} \chi \colon \mathbb{R}^n &\to \mathbb{R}^{r_1+r_2} \\ (x_1, \ldots, x_n) &\mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, 2\log|\sigma_{r_1+1}(x)|, \ldots, 2\log|\sigma_{r_1+r_2}(x)|) \end{aligned}$$

Note that

$$\begin{aligned} \psi &= \chi \circ \phi, \\ \phi(xy) &= \phi(x) \cdot \phi(y) \\ \chi(x \cdot y) = \chi(x) + \chi(y) \\ N(x \cdot y) &= N(x)N(y) \\ \log N(x) &= \sum_{i=1}^{r_1+r_2} (\chi(x))_i. \end{aligned}$$

118 Lemma

If $L \subset \mathbb{R}^m$ is a lattice, then L is full rank if and only if there exists a bounded region $S \subset \mathbb{R}^m$ such that $S + L$ covers $\mathbb{R}^m$.

Proof In the $\Rightarrow$ direction, we have $L = \mathbb{Z}v_! + \cdots + \mathbb{Z}v_m$ where the v_i are $\mathbb{R}$-linearly independent. Then set $S := \{\sum_{i=1}^m a_i v_i : 0 \leq a_i < 1\}$.

If L is not full rank, then $\mathrm{Span}(L) =: V \subsetneq \mathbb{R}^m$. So for any $D > 0$, there exists $v \in \mathbb{R}^m$ such that the distance from r to V is $> D$, so no such S exists.

Proof (Of Proposition) By the lemma, we want to construct a bounded set $S \subset H$ such that $S + \psi(\mathcal{O}^\times)$ covers H. We will take $S = \chi(\widetilde{S})$ for some $\widetilde{S} \subset \mathbb{R}^n$. Let $U \subset \mathbb{R}^n$ where $U := \{x \in \mathbb{R}^n : N(x) = 1\}$. Note that $\chi(U) = H$, so $\widetilde{S} \subset U$.

Claim 1: if $\widetilde{S}$ is bounded, then S is bounded. To see the implication, suppose that for all $x \in \widetilde{S}$, $|x_i| \leq C_i$. Then we have component-wise bounds $(\chi(x))_j \leq C'_j$ for some C'_j. Since $\chi(\widetilde{S}) \subset \chi(U) = H$, this implies that $\chi(x)_j \geq C''_j$ for some C''_j. (The converse also holds.)

Claim 2: if for all $v \in U$ there exists $x \in \mathcal{O}^\times$ such that $\phi(x) \cdot v \in \widetilde{S}$, then $S + L$ covers H. To see this, let $y \in H$. We want to show that there exists $w \in L$ such that $y - w \in S = \chi(\widetilde{S})$, which is $\chi(v) + \psi(x)$. Note that $\chi(v \cdot \phi(x)) = \chi(v) + \chi(\phi(x))$.

Hence it suffices to construct $\widetilde{S}$ with the properties in the claim.

119 Lemma

Given $c \in \mathbb{R}_{>0}^{r_1+r_2}$, set

$$S_c := \left\{ (x_i) \in \mathbb{R}^n : \begin{cases} |x_i| \leq c_i & 1 \leq i \leq r_1 \\ x_{2_i+r_1-1}^2 + x_{2i+r_1}^2 \leq c_i & r_1 + 1 \leq i \leq r_2 \end{cases} \right\}.$$

Then S_c is compact, convex, symmetric about the origin, and has volume

$$\mathrm{vol}(S_c) = 2^{r_1}\pi^{r_2} \prod_{i=1}^{r_1+r_2} c_i.$$

Proof Compactness, convexity, and symmetry are routine or immediate. For the volume, we have r_1 intervals of length $2c_i$ and r_2 discs of radius $\sqrt{c_i}$, so it is also essentially routine.

Now we construct $\widetilde{S}$. Let $V = \mathrm{vol}(\mathcal{F}_{\phi(\mathcal{O})})$. Let $c \in \mathbb{R}^n_{>0}$ such that $C = \prod c_i > (4/\pi)^{r_2} V$. Let $\alpha_1, \ldots, \alpha_m$ be generators for all of the principal ideals of $\mathcal{O}$ of norm $\leq C$. Then set

$$\widetilde{S} := U \cap (\cup_{i=1}^m (\phi(\alpha_i^{-1}) \cdot S_c))$$

Notice that

$$\mathrm{vol}(S_c) = 2^{r_1} \pi^{r_2} \prod c_i = 2^{r_1} \pi^{r_2} C > 2^n V,$$

which is exactly the condition needed to have a non-zero lattice point. For any $y \in U$, $N(y) = 1$, so $\mathrm{vol}(y \cdot \mathcal{F}_{\phi(\mathcal{O})}) = \mathrm{vol}(\mathcal{F}_{\phi(\mathcal{O})}) = V$. Hence for any $y \in U$, there exists a non-zero lattice point of $y \cdot \phi(\mathcal{O})$ in S_c, call it $\phi(\alpha_y)$. Consider

$$|N_{K/\mathbb{Q}}(\alpha_y)| = N(\phi(\alpha_y)) \leq \prod c_i = C,$$

so $(\alpha_y) = (\alpha_1)$ (say), so $\alpha_y = \epsilon \alpha_1$ for some $\epsilon \in \mathcal{O}^\times$. We know that $y \cdot \phi(\alpha_y) \in S_c$, which is $y \cdot \phi(\epsilon) \cdot \phi(\alpha_i)$, so $y \cdot \phi(\epsilon) \in (\phi(\alpha_1^{-1}) S_c) \cap U \subset \widetilde{S}$, giving the second claim and completing the proof and theorem.

120 Aside

Why do we care about finiteness of the class group? For one example, set $h_p := \#\,\mathrm{Cl}(\mathbb{Q}(\zeta_p))$. If $p \nmid h_p$, then Fermat's Last Theorem holds for exponent p. (The proof is in Osserman.)

In another direction, let S be a finite set of primes, and define $\mathcal{O}_{K,S} := S^{-1}\mathcal{O}_K$ (where we are inverting all primes in S rather than localizing at them in any sense). The finiteness of $\mathrm{Cl}(\mathcal{O}_K)$ implies that for any finite set S_0 of primes, there exists a finite set $S \supset S_0$ such that $\mathcal{O}_{K,S}$ is a UFD. This fact is used very often in number theory, but it fails in more generality since class groups of Dedekind domains need not be finite.

One can generalize Dirichlet's unit theorem to get $\mathcal{O}_{K,S}^\times \cong \mu_m \times \mathbb{Z}^{r_1 + r_2 + \#S - 1}$. It's perhaps not as widely used as the finiteness of the class group, though it is certainly fundamental.

November 2nd, 2015: Draft

Summary We'll now switch the focus of our discussion to local fields. We'll begin with a review of p-adics.

121 Notation

Fix a prime p.

122 Definition

The $\boxed{p\text{-adic valuation}}$

$$\begin{aligned} \boxed{v_p} &: \mathbb{Q} \to \mathbb{Q} \cup \{\infty\} \\ & 0 \mapsto 0 \\ p^k \frac{a}{b} = r \neq 0 &\mapsto k \qquad (p \nmid ab) \end{aligned}$$

The $\boxed{p\text{-adic absolute value}}$ is

$$\begin{aligned} \boxed{||\cdot||_p} : \mathbb{Q} &\to \mathbb{R}_{\geq 0} \\ 0 &\mapsto 0 \\ r &\mapsto p^{-v_p(r)}. \end{aligned}$$

123 Lemma

Let $z_1, z_2 \in \mathbb{Q}$. Then

(1) $v_p(\pm 1) = 0$*;*
$|| \pm 1||_p = 1$

(2) $v_p(z_1 z_2) = v_p(z_1) + v_p(z_2)$*;* $||z_! z_2||_p = ||z_1||_p ||z_2||_p$

(3) $v_p(z_1 + z_2) \geq \min(v_p(z_1), v_p(z_2))$ *with equality if* $v_p(z_1) \neq v_p(z_2)$*;* $||z_1 + z_2||_p \leq \max(||z_1||_p, ||z_2||_p$ *with equality if* $||z_1||_p \neq ||z_2||_p$

Proof (1) and (2) are immediate from the definitions. As for (3), assume $z_1 z_2 \neq 0$ and write $z_i = p^{k_i} a_i / b_i$ for $p \nmid a_i b_i$. Then if $m := \min(v_p(z_1), v_p(z_2))$,

$$z_1 + z_2 = \frac{p^{k_1} a_1 b_2 + p^{k)_2} a_2 b_1}{b_1 b_2} = p^m \frac{p^{k_1 - m} a_1 b_2 + p^{k_2 - m} a_2 b_1}{b_1 b_2}.$$

Note that $p \nmid b_1 b_2$ by assumption, and if, say, $k_1 < k_2$, then the numerator is of the form $a_1 b_2 + p^{\cdot} a_2 b_1$ where $\cdot > 0$, giving the result.

We next give three essentially equivalent definitions:

124 Definition

The set of $\boxed{p\text{-adic integers}}$ is the set of formal power series

$$\boxed{\mathbb{Z}_p} := \{\sum_{i=0}^{\infty} a_i p^i : 0 \leq a_i < p\},$$

with the usual addition and multiplication.

125 Definition

Alternatively, we may define $\mathbb{Z}_p$ categorically as an inverse limit,

$$\begin{aligned} \mathbb{Z}_p &:= \varprojlim \mathbb{Z}/p^i\mathbb{Z} \qquad \text{maps are usual quotients} \\ &= \{(a_0, a_1, a_2, \ldots) : a_i \in \mathbb{Z}/p^{i+1}\mathbb{Z}, a_{i+1} \equiv_{p^{i+1}} a_i\} \end{aligned}$$

which inherits a ring structure from the components.

126 Definition

Finally, we may define $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ with respect to $|| \cdot ||_p$.

127 Proposition

There is a set bijection between any two of these definitions, and the additional structures are preserved.

128 Remark

Refer to definition 124 as (1), definition 125 as (2), and 126 as (3).

Definition (2) inherits a topology from components (the discrete topology on each). Definition (3) has a ring structure.

Proof For (1) $\Rightarrow$ (2), use

$$\sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{j} a_i p^i \bmod p^{j+1} \right)_{j=0}^{\infty}.$$

To go the other way, use $(a_i) \mapsto \sum_{j=0}^{\infty} b_j pj$ where the b_j's are defined recursively and uniquely by the condition $\sum_{j=0}^{i} b_j p^j \equiv_{p^{i+1}} a_i$. We can essentially divide by p^i to solve this equation for b_i. That these are mutual inverses is clear.

For (2) $\Rightarrow$ (3), send $(a_i) \mapsto (\widetilde{a}_i)$ for any lifts $\widetilde{a}_i \in \mathbb{Z}$ of a. Any two lifts differ by a Cauchy sequence converging to zero since $\widetilde{a}_i \equiv_{p^i} a_{i+1}$, so in the completion such choices are equal. For (3) $\Rightarrow$ (2), let (b_i) be a Cauchy sequence. Then for all j there exists $n \gg 0$ such that $b_m \equiv_{p^{j+1}} b_{m'}$ for all $m, m' > n$. Set $a_j := b_m \bmod p^{j+1}$ for all $m > n_j$. One may easily check this is well-defined.

129 Remark

$\mathbb{Z}_p$ is an integral domain, from (2). So, we may set $\boxed{\mathbb{Q}_p}$ as its field of fractions. (Alternatively, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|| \cdot ||_p$.)

130 Exercise

Show that

(1) $\sqrt{-1} \in \mathbb{Z}_p$ for all $p \equiv_4 1$

(2) $\sqrt{a} \in \mathbb{Z}_p$ for all p such that $\left(\frac{a}{p}\right) = 1$, using the Legendre symbol, i.e. if and only if a is a non-zero square mod p.

Indeed, we have several natural inclusions,

$$\begin{tikzcd} \mathbb{Q} \arrow[r, hook] & \mathbb{Q}_p \end{tikzcd}$$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook] \arrow[dr, hook] & \mathbb{Z}_p \\ & \mathbb{Z}_{(p)} \arrow[u, hook] \end{tikzcd}$$

131 Definition (Ad-hoc)

A $\boxed{\text{local field}}$ is either $\mathbb{R}$, $\mathbb{C}$, a finite extension of $\mathbb{Q}_p$, or a finite extension of $\mathbb{F}_q((t))$.

At present this is unmotivated (to put it mildly), so we'll give another definition and come back to this one later.

132 Definition

Let K be a field. An $\boxed{\text{absolute value}}$ on K is

$$\boxed{|\cdot|} \colon K \to \mathbb{R}_{\geq 0}$$

such that

(i) For all $x \in K$, $|x| = 0$ if and only if $x = 0$

(ii) $|xy| = |x||y|$

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

133 Example

On $\mathbb{Q}$, set

$$\boxed{|x|_\infty} := \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

We can also use $\boxed{|x|_p} := p^{-v_p(x)}$. Moreover, for any field K, we may use the $\boxed{\text{trivial absolute value}}$ $|x| = 1$ for $x \neq 0$ with $|0| = 0$.

134 Definition

Two absolute values $|\cdot|_1, |\cdot|_2$ on a field K are $\boxed{\text{equivalent absolute values}}$ if and only if the underlying topology is the same.

135 Proposition

$|\cdot|_1 \sim |\cdot|_2$ *if and only if there exists* $s \in \mathbb{R}_{>0}$ *such that* $|x|_1 = |x|_2^s$ *for all* $x \in K$.

136 Remark

The $\Leftarrow$ direction assumes both $|x|_1$ and $|x|_2$ are in fact absolute values. In general we may have to restrict the possible s's, since for instance squaring the Euclidean distance does not preserve the triangle inequality.

Proof The $\Leftarrow$ direction is clear, so consider $\Rightarrow$ and assume $|\cdot|_1 \sim |\cdot|_2$. Let $x \in K$. Note that $|x| < 1$ if and only if $\{x^n\}$ converges to 0, so $|x|_1 < 1$ if and only if $|x|_2 < 1$. Without loss of generality, assume $|\cdot|_1$ is non-trivial. Pick $y \in K$ such that $|y|_1 > 1$. For any $x \in K$, there exists $\alpha = \alpha(x)$ such that $|x|_1 = |y|_1^\alpha$. Take a sequence of rational numbers m_i/n_i converging to α from above. Hence

$$|x|_1 = |y|_1^\alpha \leq |y|_1^{m_i/n_i} \qquad \forall i$$

so by multiplicativity $|x^{n_i}/y^{m_i}|_1 \leq 1$ for all i. By the opening observation, $|x^{n_i}/y^{m_i}|_2 \leq 1$. So $|x|_2 \leq |y|_2^{m_i/n_i}$, meaning $|x|_2 \leq |y|_2^\alpha$. Similarly if we take m_i/n_i converging to α from below instead, we find $|x|_2 \geq |y|_2^\alpha$, so $|x|_2 = |y|_2^\alpha$. So

$$\frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2} = s$$

for s independent of x.

Since $|y|_1 > 1$ implies $|y|_2 > 1$, we find $s > 0$.

Next time, we will classify absolute values on $\mathbb{Q}$:

137 Proposition

Let $|\cdot|$ *be a non-trivial absolute value on* $\mathbb{Q}$. *Then* $|\cdot| \sim ||\cdot||_p$ *for some prime* p, *or* $|\cdot| \sim |\cdot|_\infty$.

November 4th, 2015: Draft

Let K be a field.

138 Theorem (Approximation)

Let $|\cdot|_1, \ldots, |\cdot|_n$ *be inequivalent non-trivial absolute values on* K, *and pick* $a_1, \ldots, a_n \in K$. *Then for all* $\epsilon > 0$, *there exists* $x \in K$ *such that* $|x - a_i|_i < \epsilon$.

(The conclusion may fail if the absolute values are trivial or inequivalent.)

Proof From the characterization of equivalent absolute values, there exist $\alpha, \beta \in K$ such that $|\alpha|_1 < 1, |\beta|_1 > 1$, and $|\alpha|_2 > 1, |\beta|_2 < 1$.

Claim: there exists $z \in K$ such that $|z|_1 > 1$ and $|z|_j < 1$ for all $j \geq 2$. We'll prove this by induction; the previous observation gives the $n = 2$ case. Suppose $z \in K$ such that $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n-1$. If $|z|_n < 1$, then we're done. Assume $|z|_n \leq 1$. Set $y := \alpha/\beta$ and consider $z^m y$ for $m \gg 0$. Now $|z^m y|_1 > 1$ since $|z|_1 \geq 1$ and $z^m y|_j < 1$ for $j = 2, \ldots, n-1$. In addition, since $|y|_n < 1$, $|z^m y|_n < 1$ for all m. So for $m \gg 0$, $z^m y$ satisfies claim.

Then consider $|z^m/(1+z^m)|_\cdot$; this is going to 1 where $\cdot = 1, n$ and 0 for $\cdot = 2, \ldots, n-1$. Then $yz^m/(1+z^m)$ has the desired properties.

[There are some minor mistakes in the above–clean it up as an exercise.]

Now set $w_m = z^m/(1+z^m)$; note

$$|w_m|_j \to \begin{cases} 1 & j = 1 \\ 0 & j > 1 \end{cases}.$$

Let $x_1 = w_m$, $m \gg 0$, and define $x_2, \ldots, x_n$ similarly after exchanging 1 with j, so

$$|x_j|_i \to \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}.$$

Now set $x := a_1 x_1 + \cdots + a_n x_n$, so that

$$|x - a_i|_i \leq |a_i(x_i - 1)|_i + \sum_{j \neq i} |a_j x_j|_i,$$

which will be appropriately small.

There are roughly two types of absolute values—the real absolute value we're used to from grade school, and absolute values similar to the p-adic case above. We give a pair of ad-hoc definitions distinguishing between these:

139 Definition (Ad-Hoc)

$|\cdot|$ on K is archimidean if it is non-trivial and the completion of K with respect to $|\cdot|$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. It is called nonarchimidean otherwise. (In particular, the trivial absolute value on $\mathbb{R}$ or $\mathbb{C}$ is nonarchimidean.)

Alternatively, $|\cdot|$ is nonarchimedean if $|n|$ is bounded for all $n \in \mathbb{N}$ and archimidean otherwise. (This condition is unchanged for positive characteristic; the condition is just trivial then.)

140 Proposition

$|\cdot|$ is nonarchimedean if and only if it satisfies the "strong triangle inequality"

$$|x + y| \leq \max\{|x|, |y|\}.$$

Proof For ($\Leftarrow$), note that $|n| = |1 + \cdots + 1| \leq \max|1|$ is evidently bounded. For ($\Rightarrow$), assume $|n| < M$ for all n. Let $x, y \in K$, and take $|x| \geq |y|$. Then $|x|^\nu |y|^{n-\nu} \leq |x|^n$ and

$$|x + y|^n \leq \sum_{\nu=0}^{n} \left| \binom{n}{\nu} x^\nu y^{n-\nu} \right| \leq (n+1)M|x|^n.$$

Taking nth roots of both sides,

$$|x + y| \leq (n+1)^{1/n} M^{1/n} |x|.$$

Take the limit as $n \to \infty$ to get $|x + y| \leq |x| = \max(|x|, |y|)$.

141 Remark

If for all $x, y \in K$, $|x+y| \leq \max(|x|, |y|)$, then in fact $|x| \neq |y|$ implies $|x+y| = \max(|x|, |y|)$.

Proof Suppose $|x| > |y|$. Then

$$|x+y| \leq |x| = |x+y-y| \leq \max |x+y|, |y| = |x+y|$$

where the last step follows from $|y| < |x|$. We had obtained this stronger triangle inequality above.

142 Proposition ((“Little”) Ostrowski)

Let $|\cdot|$ be a nontrivial absolute value on $\mathbb{Q}$. Then $|\cdot| \sim ||\cdot||_p$ for some p, or $|\cdot| \sim ||\cdot||_\infty$.

Proof Assume $|\cdot|_p$ is nonarchimedean. Then $|n| \leq 1$. Since $|\cdot|$ is nontrivial, there exists n with $|n| < 1$, so by unique factorization in integers, there exists a prime p with $|p| < 1$. Set $\mathfrak{a} := \{a \in \mathbb{Z} : |a| < 1\}$. This is an ideal and $p\mathbb{Z} \subset \mathfrak{a} \subsetneq \mathbb{Z}$, so $\mathfrak{a} = p\mathbb{Z}$. Hence $|n| = |p|^k$ for $p^k || n$ (where p^k exactly divides n). But this says precisely $|n| = ||n||_p^{-\log|p|/\log p}$, which says $|\cdot| \sim ||\cdot||_p$.

Now assume $|\cdot|_p$ is archimedean. Pick $m, n \in \mathbb{N}$ and write m in base n as $m = a_0 + a_1 n + \cdots + a_r n^r$ for $0 \leq a_i \leq n-1$. Now $n^r \leq m$, so $r \leq \log m / \log n$, and $|a_i| \leq a_i \leq n$. Hence

$$|m| \leq \sum_{i=0}^{r} |a_i||n^i| \leq \sum_{i=0}^{r} |n^r| = (r+1)n|n|^r \leq (\log m/\log n + 1)n|n|^{\log m/\log n}.$$

Set $m = (m')^k$ and take kth roots of both sides to get

$$|m'| \leq (k \log m'/\log n + 1)^{1/k} n^{1/k} |n|^{\log m'/\log n}.$$

Take the limit as $k \to \infty$ to get $|m'| \leq |n|^{\log m'/\log n}$. Now set $m \mapsto n^k$ and $n \mapsto m'$ to get $|n| \leq |m'|^{\log n/\log m'}$. This gives $|n|^{1/\log n} = |m|^{1/\log m}$. Setting $s := \log |m'|/\log m'$, one finds $|m| = ||m||_\infty^s$ for all $m \in \mathbb{Z}$, so for all $m \in \mathbb{Q}$.

143 Theorem ((“Big”) Ostrowski)

If K is a field which is complete with respect to an archimidean absolute value $|\cdot|$, then there exists a field isomorphism $\sigma\colon K \to \mathbb{R}$ or $\mathbb{C}$ such that $|a| = ||\sigma(a)||_\infty^s$ for all $a \in K$.

Proof Outline: archimedean absolute value implies K is characteristic 0, giving $\mathbb{Q} \hookrightarrow K$, so the restriction of $|\cdot|$ to $\mathbb{Q}$ is equivalent to $||\cdot||_\infty$. Since K is complete, it contains the completion of $\mathbb{Q}$ under $||\cdot||_\infty$, namely $\mathbb{R}$. Hence one must show K is either this $\mathbb{R}$ or $\mathbb{C}$. Then one can show that for all $a \in K$, a satisfies a quadratic relation over $\mathbb{R}$—take $x \in K$ and consider $f\colon \mathbb{C} \to \mathbb{R}$ given by $z \mapsto ||x^2 - (z+\overline{z})x + z\overline{z}||_\infty$, which one may show has minimum zero.

November 6th, 2015: Draft

Last time we classified the fields which are complete with respect to an archimedean absolute value. Today we'll focus on non-archimedean absolute values $|\cdot|\colon K \to \mathbb{R}_{\geq}$. We can define an associated (non-archimedean) valuation.

144 Definition

A $\boxed{\text{valuation}}$ is a map $v\colon K \to \mathbb{R} \cup \{\infty\}$ such that

(1) $v(x) = \infty$ if and only if $x = 0$

(2) $v(xy) = v(x) + v(y)$

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

145 Remark

If $|\cdot|$ is a non-archimedean absolute value, its associated valuation is defined by $v_{|\cdot|}(0) := \infty$, $v_{|\cdot|}(x) := -\log|x|$. In the other direction, we may choose any $a \in \mathbb{R}_{>1}$ and construct a non-archimedean absolute value from a valuation by setting $|x|_v := a^{-v(x)}$.

We also have the trivial valuation, $|\cdot| := 0$ for all $x \neq 0$.

146 Definition

Two valuations v_1, v_2 are $\boxed{\text{equivalant valuations}}$ if there exists $s > 0$ such that $v_1(x) = sv_2(x)$ for all $x \in K$.

147 Proposition

Let v be a valuation on K. Define $\mathcal{O} := \{x \in K : v(x) \geq 0\}$. This is a ring with a unique maximal ideal $\mathfrak{p} := \{x \in K : v(x) > 0\}$ and the units are precisely $\mathcal{O}^\times = \{x \in K : v(x) = 0\}$.

Proof $\mathcal{O}$ is a ring from properties (1) through (3). Let $\mathfrak{m} \subset \mathcal{O}$ be an ideal. If there exists $x \in \mathfrak{m}$ such that $v(x) = 0$, then $1/x \in \mathcal{O}$ because $v(1/x) = -v(x) = 0 \geq 0$, so $1/x \cdot x \in \mathfrak{m}$, so $\mathfrak{m} = \mathcal{O}$. Hence any proper idea is contained in $\mathfrak{p}$, which is an ideal by properties (1) through (3). Since $\mathcal{O}$ is a local ring, its complement is the set of units.

The ring $\mathcal{O}$ satisfies the following abstract condition:

148 Definition

An integral domain $\mathcal{O}$ is a $\boxed{\text{valuation ring}}$ if for all $x \in \operatorname{Frac}(\mathcal{O})$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. Any valuation ring has a unique maximal ideal $\mathfrak{p} := \{x \in \mathcal{O} : x^{-1} \notin \mathcal{O}\}$. The $\boxed{\text{residue field}}$ of $\mathcal{O}$ is $\kappa := \mathcal{O}/\mathfrak{p}$.

Nathan says a version of the converse (going from these abstract conditions to a valuation with values in a certain abelian group) is done in Atiyah-Macdonald.

149 Lemma

A valuation ring is integrally closed.

Proof Let $x \in \operatorname{Frac}(\mathcal{O})$ and assume that x satisfies a monic polynomial in $\mathcal{O}[x]$, so there exists $a_i \in \mathcal{O}$ such that

$$x^{-(n-1)}(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = 0$$

so that

$$x = -a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0(x^{-1})^{n-1}.$$

If $x^{-1} \in \mathcal{O}$, the the right-hand side is in $\mathcal{O}$, so in either case $x \in \mathcal{O}$.

150 Definition

A valuation v is a $\boxed{\text{discrete valuation}}$ if $\operatorname{im}(v)$ has a minimum positive element, which says $v(K^\times)$ is a lattice in $\mathbb{R}$. A $\boxed{\text{normalized discrete valuation}}$ is one where $v(K^\times) = \mathbb{Z}$.

Given a discrete valuation, we can choose $\pi \in \mathcal{O}$ with minimal valuation. Then for all $x \in K = \operatorname{Frac}(\mathcal{O})$, $x = u\pi^m$ for some unique unit u and $m \in \mathbb{Z}$. Such an element is called a $\boxed{\text{uniformizer}}$, which is not itself unique.

151 Proposition

If v is a discrete valuation of K, then the corresponding valuation ring $\mathcal{O} = \mathcal{O}_K$ is a DVR. If v is normalized and π is a uniformizer, then all ideals of $\mathcal{O}$ are of the form

$$\mathfrak{p}^n = \pi^n \mathcal{O} = \{\mathcal{O} : v(x) \geq n\}.$$

Further, $\mathcal{O}/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$ for all n.

Proof $\mathcal{O}$ is local, noetherian, and integrally closed, so it satisfies our earlier DVR definition, so it's principal. The ideal structure is then clear (and it's easy to prove directly). As for the isomorphism, define a map $\mathfrak{p}^n \to \mathcal{O}/\mathfrak{p}$ by $x = a\pi^n \mapsto (x/\pi^n) = a \bmod \mathfrak{p}$. The kernel of this map is precisely $\mathfrak{p}^{m+1}$.

We have a basis for neighborhoods of 0 and 1. For 0 we have

$$\mathcal{O} \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \cdots \supset (0)$$

and for 1 we have

$$\mathcal{O}^\times \supset U^{(1)} \supset U^{(2)} \supset \cdots \supset (1)$$

where

$$U^{(n)} := 1 + \mathfrak{p}^n = \{x \in K : |1-x|_v < 1/q^{n-1}\} \qquad\qquad q := |\pi|^{-1}.$$

152 Proposition

$\mathcal{O}^\times/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^\times$ and $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$ for all n.

Proof Use maps $u \mapsto u \bmod \mathfrak{p}^n$ and $u = 1 + a\pi^n \mapsto (u-1)/\pi^n \bmod \mathfrak{p}$.

The following is Bianca's favorite fact about valuations. It has many variations.

153 Theorem (Hensel's Lemma)

Let K be complete with respect to a non-trivial valuation v, with valuation ring $\mathcal{O}$. Let $f(x) \in \mathcal{O}[x]$ be a primitive polynomial, meaning $f(x) \not\equiv_\mathfrak{p} 0$. If $f(x) \equiv_\mathfrak{p} \overline{g}\overline{h}$ with $\overline{g}, \overline{h}$ relatively prime, then there exist $g, h \in \mathcal{O}[x]$ such that

1. $\deg g = \deg \overline{g}$
2. $g \equiv_\mathfrak{p} \overline{g}$ *and* $h \equiv_\mathfrak{p} \overline{h}$
3. $f = gh$

Proof Let $d := \deg f$, $m := \deg \overline{G}$. Then $d - m \geq \deg \overline{h}$. Let $g_0, h_0 \in \mathcal{O}[x]$ be any lift of $\overline{g}$ and $\overline{h}$ for which $\deg g_0 = \deg \overline{g}$ and $\deg h_0 \leq d - m$. Since $\overline{g}, \overline{h}$ are relatively prime in $\kappa[x]$, there exist $a(x), b(x) \in \mathcal{O}[x]$ such that $ag_0 + bh_0 - 1 \equiv_\mathfrak{p} 0$. We also have $f - g_0h_0 \equiv_\mathfrak{p} 0$. Let π be a coefficient of $ag_0 + bh_0 - 1$ or $f - g_0h_0$ with minimum valuation ($v(\pi) > 0$). We want to find $g_n, h_n \in \mathcal{O}[x]$ such that

(1) $\deg(g_n) = m$, $\deg(h_n) \leq d - m$, and the leading coefficients of g_n and g_0 agree;

(2) $g_n \equiv_{\pi^n} g_{n-1}$ and $h_n \equiv_{\pi^n} h_{n-1}$;

(3) $f \equiv_{\pi^{n+1}} g_nh_n$.

We've already exhibited such elements for $n = 0$, so suppose we have such a g_{n-1} and h_{n-1}. Then we'll construct

$$\begin{aligned} g_n &= g_{n-1} + \pi^n p_n && \text{for some } \deg p_n < m \\ h_n &= h_{n-1} + \pi^n q_n && \text{for some } \deg q_n \leq d - m. \end{aligned}$$

That is,

$$f - g_nh_n = f - g_{n-1}h_{n-1} - \pi^n(g_{n-1}q_n + h_{n-1}p_n + \pi^n p_nq_n) \equiv_{\pi^{n+1}} 0.$$

Set

$$f_n = (f - g_{n-1}h_{n-1})/\pi^n \equiv_\pi (g_{n-1}q_n + h_{n-1}p_n) \equiv_\pi (g_0q_n + h_0p_n).$$

Recall we have $g_0a + bh_0 \equiv_\pi 1$, so use the Extended Euclidean Algorithm to get

$$f_nb = qg_0 + r(x) \qquad \text{with } \deg r(x) < \deg g_0 = m$$

Then

$$g_0f_na + f_nbh_0 = g_0(f_na + h_0q) + h_0r(x) \equiv_\pi f_n.$$

We can set $p_n := r(x)$ which has degree $< d$ and $q_n := f_na + h_0q$ which has degree m.

November 9th, 2015: Draft

Last time, we ended with:

154 Theorem (Hensel's Lemma)
Let K be complete with respect to a non-trivial nonarchimedean valuation with valuation ring $\mathcal{O}$ with (unique) maximal ideal $\mathfrak{p}$ and residue field κ, where $f(x) \not\equiv_{\mathfrak{p}} 0$. If there exists $\overline{g}, \overline{h} \in \kappa[x]$ relatively prime such that f mod $\mathfrak{p} = \overline{g}\overline{h}$. Then there exists $g, h \in \mathcal{O}[x]$ such that

(1) $g \equiv_{\mathfrak{p}} \overline{g}$, $h \equiv_{\mathfrak{p}} \overline{h}$

(2) $\deg g = \deg \overline{g}$

(3) $f = gh$ *in* $\mathcal{O}[x]$

155 Corollary
Let K be complete with respect to a non-trivial (nonarchimedean?) valuation. Suppose $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ is irreducible with $a_0 a_n \neq 0$. Then $|f| : \max\{|a_i|\} = \max(|a_0|, |a_n|)$. In particular, if $a_n = 1$ and $a_0 \in \mathcal{O}$, then $a_i \in \mathcal{O}$ for all i.

Proof After scaling by the least possible amount, we may assume $f(x) \in \mathcal{O}[x]$ such that $|f| = 1$. Let r be minimal such that $|a_r| = 1$. Then $f(x)$ mod $\mathfrak{p} = x^r(a_r + \cdots + a_n x^{n-r})$ where $a_r \neq 0$. If $0 < r < n$, then by Hensel's lemma, there exists a non-trivial factorization of f, which is irreducible. It follows that $r = 0$ or $r = n$, giving the result.

156 Theorem
Let K be complete with respect to $|\cdot|$ and suppose L/K is an algebraic extension. Then there exists a unique extension of $|\cdot|$ to L. If L/K is finite of degree n, then

$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|} \qquad \forall \alpha \in L,$$

and L is complete.

Proof If $|\cdot|$ is archimedean, then this follows from the classification using $\mathbb{R}$ or $\mathbb{C}$. So, assume $|\cdot|$ is nonarchimedean. Since an algebraic extension is just the union of all finite sub-extensions, we may assume that L/K is finite.

For existence using the formula above: $|\alpha| = 0 \Leftrightarrow \alpha = 0$ is clear, and multiplicativity is also clear. Claim: $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$ for all $\alpha, \beta \in L$ if and only if ($|\alpha| \leq 1 \Rightarrow |\alpha + 1| \leq 1$). (For $\Leftarrow$, roughly, divide by an element of maximal absolute value.)

Now let $\alpha \in L$ have $|\alpha| \leq 1$. Then $|N_{L/K}(\alpha)| \leq 1$, so the minimal polynomial of α has integral constant term, so α is integral by the preceding corollary, i.e. $\{\alpha \in L : |\alpha| \leq 1\} = \mathcal{O}_L$. But $\alpha \in \mathcal{O}_L$ implies $\alpha + 1 \in \mathcal{O}_L$, so $|\alpha + 1| \leq 1$.

For uniqueness, suppose $\widetilde{|\cdot|}$ is another extension of $|\cdot|$ to L. Let $\widetilde{\mathcal{O}}_L$ be the valuation ring of $\widetilde{|\cdot|}$. Note that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L. Claim: $\mathcal{O}_L \subset \widetilde{\mathcal{O}}_L$. Proof: let $\alpha \in \mathcal{O}_L$ and $f = \sum_{i=0}^{d} a_i x^i$ be the minimal polynomial, with $\alpha_d = 1$. Hence $f(\alpha) = 0$ says $1 = -a_{d-1}\alpha^{-1} - a_{d-2}\alpha^{-2} - \cdots - a_0\alpha^{-d}$. If $\alpha \notin \widetilde{\mathcal{O}}_L$, then $\alpha^{-1} \in \widetilde{\mathfrak{p}}$, but then the right-hand side is in $\widetilde{\mathfrak{p}}$, so $1 \in \widetilde{\mathfrak{p}}$, a contradiction.

Since $\mathcal{O}_L \subset \widetilde{\mathcal{O}}_L$, we have $|\alpha| \leq 1$ implies $\widetilde{|\alpha|} \leq 1$, which implies $|\cdot| \sim \widetilde{|\cdot|}$. Since $|\cdot| = \widetilde{|\cdot|}$ on K, we have $|\cdot| = \widetilde{|\cdot|}$.

It remains to show that L is complete.

157 Proposition

Let K be complete with respect to $|\cdot|$ and let V be an n-dimensional normed K-vector space. Suppose $v_1, \dots, v_n$ is a K-basis for V. Then the max norm

$$|x_1 v_1 + \cdots + x_n v_n| := \max\{|x_1|, \dots, |x_n|\}$$

is equivalent to the given norm on V. In particular, $K^n \to V$ is a homeomorphism and V is complete.

PROOF One may check that if there exists $\rho, \rho' > 0$ such that

$$\rho||x|| \leq |x| \leq \rho'||x|| \qquad \forall x \in V$$

then $|\cdot| \sim ||\cdot||$ and $K^n \to V$ given by $e_i \mapsto v_i$ is a homeomorphism. By the triangle inequality, we have

$$|x| \leq |x_1||v_1| + \cdots + |x_n||v_n| \leq ||x||(|v_1| + \cdots + |v_n|) =: ||x||\rho'.$$

To construct ρ, we induct. If $n = 1$, set $\rho = |v_1|$. Now $V_i := \operatorname{Span}\{v_1, \dots, \widehat{v_i}, \dots, v_n\}$ has $V = V_i + Kv_i$. By induction, V_i is complete, so it is closed in V, so $V_i + v_i$ is closed. Since $0 \notin \cup_i V_i + v_i$, there exists a neighborhood of 0 disjoint from all $V_i + v_i$, i.e. there exists $\rho > 0$ such that $|w_i + v_i| \geq \rho$ for all $w_i \in V_i$. Then

$$\frac{|x|}{||x||} = \left|\sum_{i=1}^n \frac{x_i}{x_r} v_i\right| = \left|v_r + \sum_{i \neq r} \frac{x_i}{x_r v_i}\right| \geq \rho.$$

We now have enough machinery to give a nicer definition of local fields.

158 Theorem

Let K be a locally compact field with a non-trivial absolute value. Then $(K, |\cdot|)$ is isomorphic to one of the following:

- $\mathbb{R}$
- $\mathbb{C}$
- *A finite extension of $\mathbb{Q}_p$*
- *A finite extension of $\mathbb{F}_p((t))$*

where the valuation in each case is the obvious one. The first two are the archimedean ones, the third are the characteristic zero non-archimedean ones, and the fourth are the positive characteristic non-archimedean ones.

PROOF We will avoid a lengthy digression by assuming the following fact:

159 Lemma

Let $(F, |\cdot|)$ be a locally compact field with a non-trivial absolute value and suppose V is a valued F-vector space. Then V is locally compact if and only if $\dim_F V < \infty$.

The archimedean case follows from Ostrowski's theorem, so assume $|\cdot|$ is nonarchimedean. Suppose K has characteristic 0, so $\mathbb{Q} \hookrightarrow K$ and $|\cdot|$ restricts to a nonarchimedean absolute value of $\mathbb{Q}$, which must be non-trivial by a brief argument. So without loss of generality we may assume $|\cdot|_{\mathbb{Q}} = |\cdot|_p$, meaning $\mathbb{Q}_p \hookrightarrow K$. Now apply the lemma with base field $\mathbb{Q}_p$.

Now suppose K has characteristic p, so $\mathbb{F}_p \hookrightarrow K$. Note that $|\cdot|_{\mathbb{F}_p}$ is trivial (indeed, any valuation on a finite field is trivial), but $|\cdot|$ on K is nontrivial, so we have some $t \in K$ such that $|t| < 1$. Hence $|\cdot|$ restricted to $\mathbb{F}_p(t)$ is equivalent to the standard valuation. Hence $\mathbb{F}_p((t)) \hookrightarrow$, so we may again apply the lemma.

November 13th, 2015: Draft

Bianca will be out of town on Monday, so class is cancelled.

Last time we showed that every locally compact non-discrete valued field is one of four types. For completeness, we now prove the reverse, that these possibilities are in fact locally compact non-discrete valued fields. This is clear for $\mathbb{R}$ and $\mathbb{C}$. (A note on terminology: Neukirch says just "local field" for "non-archimedean local field".)

160 Proposition

Let K be a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ equipped with the unique extension of the natural valuation. Then K is locally compact and the valuation ring $\mathcal{O}$ is compact.

161 Lemma

With K as above, we have $\mathcal{O} \cong \varprojlim_n \mathcal{O}/\mathfrak{p}^n$, both as rings and as topological spaces.

Proof The map is induced by $x \mapsto x \bmod \mathfrak{p}^n$. The overall kernel is then $\cap_n \mathfrak{p}^n = \{x : v(x) > s \cdot n\} = \{0\}$. For surjectivity, let $(x_n) \in \varprojlim \mathcal{O}/\mathfrak{p}^n$, and choose lifts $\widetilde{x}_i \in \mathcal{O}$. By completeness, there exists $x \in \mathcal{O}$ such that $\widetilde{x}_n \to x$.

The topological statement (where $\mathcal{O}/\mathfrak{p}^n$ is given the discrete topology) is straightforward and a good exercise in the definitions.

Proof (of Proposition) $\mathcal{O} \cong \varprojlim \mathcal{O}/\mathfrak{p}^n$ is a closed subset of $\prod \mathcal{O}/\mathfrak{p}^n$, which is compact by Tychonoff's theorem, so $\mathcal{O}$ is compact. If $a \in K$, then $a + \mathcal{O}$ is a compact neighborhood of a.

162 Proposition

Let K be a non-archimedean local field. Set $\mathcal{O}$ for its valuation ring, $\mathfrak{p}$ for the maximal ideal in $\mathcal{O}$, and κ for the residue field $\mathcal{O}/\mathfrak{p}$. Further suppose $q = \#\mathcal{O}/\mathfrak{p}$ and that $\pi \in \mathcal{O}$ is any uniformizer. Then we have

$$K^\times = \langle \pi \rangle \times \mu_{q-1} \times U^{(1)}$$

where $\boxed{U^{(1)}} := \{x \in \mathcal{O} : x \equiv_{\mathfrak{p}} 1\}$.

Proof Note that $x^{q-1} - 1$ factors into distinct linear factors in κ, so by Hensel's lemma, it factors into distinct linear factors in K. Then $\mu_{q-1} \subset \mathcal{O} \subset K$. Note $\mu_{q-1} \to (\mathcal{O}/\mathfrak{p})^\times$ given by $x \mapsto x \bmod \mathfrak{p}$ is an isomorphism, so $\mathcal{O}^\times = \mu_{q-1} \times U^{(1)}$. Since $K^\times = \langle \pi \rangle \times \mathcal{O}^\times$, this completes the proof.

Note: this describes $K^\times$ both as a group and topologically.

163 Proposition

Let K be a characteristic 0 non-archimedean local field (i.e. a finite extension of $\mathbb{Q}_p$). Then there exists a continuous homomorphism $\boxed{\log}: K^\times \to K$ which is uniquely determined by the following properties:

(1) If $p = \operatorname{char}(\kappa)$, then $\log p = 0$

(2) On $U^{(1)}$, $\log(1+x) = x - x^2/2 + x^3/3 - x^4/4 + \cdots$

Proof First we show that $x - x^2/2 + x^3/3 - \cdots$ converges for $x \in \mathfrak{p}$. Let v be the valuation on K such that $v|_{\mathbb{Q}_p} = v_p$. Then for $\nu \in \mathbb{N}$,

$$v(x^\nu/\nu) = \nu v(x) - v(\nu) \geq \nu \frac{\ln p^{\nu(x)}}{\ln p} - \frac{\ln \nu}{\ln p} = \frac{\ln(p^{\nu(x)}/\nu)}{\ln p} \to \infty \qquad \text{as } \nu \to \infty.$$

Now tet λ be any homomorphism that satisfies (1) and (2). Since $K^\times = \langle \pi \rangle \times \mu_{q-1} \times U^{(1)}$, for any $x \in K^\times$, write $x = \pi^{n(x)}\zeta_\pi(x)u_\pi(x)$, so that

$$\lambda(x) = n(x)\lambda(\pi) + \lambda(\zeta_\pi(x)) + \lambda(u_\pi(x)).$$

Note that $\lambda(\mu_\pi(x)) = \log u_\pi(x)$. Also note that $\lambda(\zeta_\pi(x)) = \frac{1}{q-1}\lambda(\zeta_\pi(x)^{q-1}) = \frac{1}{q-1}\lambda(1) = 0$, so the middle term cancels. For the first term $n(x)\lambda(\pi)$, we know that $p = \pi^e\zeta_\pi(p)u_\pi(p)$, so that

$$0 = \lambda(p) = e\lambda(\pi) + \lambda(\mu_\pi(p)) = e\lambda(\pi) + \log(u_\pi(p)),$$

so that $\lambda(\pi) = -\log(u_\pi(p))/e$.

164 Proposition

Let K be a non-archimedean characteristic zero local field with valuation v extending v_p on $\mathbb{Q}_p$. Let $e := 1/v(\pi) \in \mathbb{Z}$ for some uniformizer π. Then for any $n > e/(p-1)$,

$$\begin{aligned} \mathfrak{p}^n &\cong U^{(n)} \qquad \textit{algebraically and topologically} \\ \log(1+x) &\leftarrow 1+x \\ x &\mapsto \exp(x) := 1 + x + x^2/2 + x^3/3! + \cdots \end{aligned}$$

(Here $\boxed{U^{(n)}} := \{x \in \mathcal{O} : x \equiv_{\mathfrak{p}} n\}$.)

Proof It suffices to show that for all $x \in \mathfrak{p}^n$,

(1) $\exp(x)$ converges

(2) $\exp(x) \in U^{(n)}$

(3) $\log(1+x) \in \mathfrak{p}^n$

165 Lemma

If $\nu \in \mathbb{N}$ is written mod p as $\nu = \sum_{i=0}^r a_ip^i$ for $0 \le a_i < p$, then

$$\nu_p(\nu!) = \frac{1}{p-1}\sum_{i=0}^r a_i(p^i - 1).$$

Proof Counting factors of p coming from multiples of p, p^2, ..., we find

$$\begin{aligned} v_p(\nu!) &= \lfloor \nu/p \rfloor + \lfloor \nu/p^2 \rfloor + \cdots + \lfloor \nu/p^r \rfloor \\ &= \sum_{i=1}^r a_ip^{i-1} + \sum_{i=2}^r a_ip^{i-2} + \cdots + \sum_{i=r}^r a_ip^{i-r}. \end{aligned}$$

Rearrange this last expression to get the above formula.

Returning to the proof of the proposition, we turn to (3). Let z be such that $v(z) > 1/(p-1) = e/(p-1)v(\pi)$, i.e. $z \in \mathfrak{p}^n = \pi^n\mathcal{O} = \{x \in \mathcal{O} : v(x) \ge nv(\pi)\}$ for $n > e/(p-1)$. We want to show $\log(1+z) \in \mathfrak{p}^n$; we want $v(z^\nu/\nu) - v(z) > 0$ for $\nu > 1$. We compute

$$\begin{aligned} v(z^\nu/\nu) - v(z) &= (\nu-1)v(z) - v(\nu) \\ &> (\nu - 1)\left(\frac{1}{p-1} - \frac{v(\nu)}{\nu - 1}\right), \end{aligned}$$

where we want to show the final term in parentheses is > 0. Write $\nu = p^a\nu_0$ and note

$$v(\nu)/(\nu-1) = a/(\nu-1) \le a/(p^a - 1) = 1/(p-1)(a/(1+p+\cdots+p^{a-1})) < 1/(p-1).$$

We will skip the arguments for (1) and (2), which Bianca believes are also in Osserman's notes.

166 Proposition

Let K be a characteristic 0 non-archimedean local field with $q = \#\kappa = p^f$. Then

$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1) \times \mathbb{Z}/p^a \times \mathbb{Z}_p^d \qquad \textit{algebraically and topologically}$$

for some $a \geq 0$, where $d := [K : \mathbb{Q}_p]$.

167 Aside

If K is a characteristic p non-archimedean local field, then analogously $K^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1) \times \mathbb{Z}_p^{\mathbb{N}}$. We won't prove this version though.

Proof ((Sketch)) We have $\langle \pi \rangle \cong \mathbb{Z}$ and $u_{q-1} \cong \mathbb{Z}/(q-1)$, so we're essentially claiming $U^{(1)} \cong \mathbb{Z}/p^a \times \mathbb{Z}_p^d$. Now $U^{(1)}$ is a $\mathbb{Z}_p$-module, so by the classification of such finitely generated modules, we need only compute the torsion of $U^{(1)}$, namely $\mu_{p^\infty}(K)$. This uses the facts that $\mathfrak{p} \cong \pi^n \mathcal{O} \cong \mathcal{O}$, $\operatorname{rank} U^{(1)} = \operatorname{rank} U^{(n)}$.

November 18th, 2015: Draft

Today we'll do a quick introduction to Newton polygons. A more modern multivariable generalization we won't discuss at all is through tropical geometry.

168 Notation

Let K be a field, be v a valuation on K, and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$.

169 Definition

The $\boxed{\text{Newton polygon}}$ of $f(x)$, $\boxed{\mathrm{NP}(f)}$, is the lower convex hull in $\mathbb{R}^2$ of $\{(i, v(a_i))\}$. More precisely, for each x-value, the corresponding y-value is the pointwise minimum of all y-values of all line segments between two vertices. This is one-dimensional, though one can imagine it being a polygon by adding extra edges in several ways.

170 Proposition

Let ω be an extension of v to the splitting field L of f over K. If $(r, v(a_r)) \leftrightarrow (s, v(a_s))$ is a line segment of $\mathrm{NP}(f)$, then $f(x)$ has $s - r$ roots of valuation equal to $-m$ where m is the slope of the segment.

If K is complete, then $g_m(x) := \prod_\alpha (x - \alpha) \in K[x]$ where the product is over $\alpha \in L$ where $f(\alpha) = 0$ and $v(\alpha) = -m$.

Proof Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$, repeated according to multiplicity. Write v for ω for this half. Order them so that $v(\alpha_i) \leq v(\alpha_j)$ for $i \geq j$. Let $(r, v(a_r))$ be maximal such that $v(\alpha_r) = v(\alpha_1)$. We first claim a_r is the right endpoint of the first line segment of the Newton polygon, i.e.

$$\frac{v(a_s) - v(a_0)}{s} > \frac{v(a_r) - v(a_0)}{r} \qquad \text{if } s > r.$$

The rough idea is that we can group roots according to their valuations, and we can express the coefficients as certain sums of products of roots, i.e. if $a_n = 1$, then

$$\begin{aligned} a_0 &= \prod \alpha_i \\ a_1 &= \sum_j \prod_{i \neq j} \alpha_i \\ a_2 &= \sum_{j,k} \prod_{i \neq j,k} \alpha_i \end{aligned} \qquad \vdots$$

Note that if $|I| < r$, then $v(\prod_{i\in I} \alpha_i) < |I|v(\alpha_1)$. Now we can compute the valuations of $a_0, a_1, \ldots$ in terms of the given data using the strong triangle inequality and the fact that the α_i are constant in groups to give the first claim; the rest of the details are left as an exercise.

For the second claim, let $\sigma \in \mathrm{Gal}(L/K)$. Then $(\sigma\omega)(\alpha) = \omega(\sigma^{-1}(\alpha))$ is a valuation that agrees with v when restricted to K. Since K is complete, there is a unique extension of v to L, so $\sigma\omega = \omega$. If α_i is a root of $f(x)$ with $\omega(\alpha_i) = -m$, then $\sigma^{-1}(\alpha_i)$ is a root of $f(x)$ and

$$\omega(\sigma(\alpha_i)) = (\sigma\omega)(\alpha_i) = \omega(\alpha_i) = -m.$$

Recall that if $f(x) \in K[x]$ is irreducible and monic, and $a_0 \in \mathcal{O}$, then $f(x) \in \mathcal{O}[x]$. We can use the Newton polygon to deduce a stronger version of this result for complete fields by analyzing the slope between the 0th and nth vertices.

171 Notation

Let L/K be an extension of non-archimedean local fields. (From the classification of such fields, the extension must be finite.) Let v be a valuation on K with unique extension w to L (where $w(\alpha) = \frac{1}{n}v(N_{L/K}(\alpha))$).

Recall the inertia degree of $[L : K]$ is $[\lambda : \kappa] =: f$ where λ is the residue field of L and κ is the residue field of K. Similarly the ramification index e is such that $\mathfrak{q}^e = \mathfrak{p}\mathcal{O}_K$. In fact, $e = [w(L^\times) : v(K^\times)]$. Recall that $[L : K] = ef$ (see a remark in Neukirch on page 151 for the positive characteristic case). We say L/K is unramified if $e = 1$.

172 Theorem

Continuing the notation above, let L/K be an unramified extension of degree f. Set $q := \#\kappa$. Then $L = K(\mu_{q^f-1})$. Conversely, given any $f \in \mathbb{Z}_{>0}$, $K(\mu_{q^f-1})$ is an unramified extension of L of degree f. In particular, there exists a unique unramified extension of any degree and it is Galois.

Proof Note that $\#\lambda = q^f$. We know that $L \supset \mu_{q^f-1}$, which we saw when we determined the multiplicative structure of such fields, which used Hensel's lemma. Consider the tower of fields

$$\overbrace{L \supset \underbrace{K(\mu_{q^f-1}) \supset K}_{\geq f}}^{f}$$

where $\geq f$ occurs since $[\kappa(\mu_{q^f-1}) : \kappa)] = f$. It remains to show that $K(\mu_{q^f-1})$ is unramified over K. This is the splitting field of $\Phi_{q^p-1}(x)$ over K, which is irreducible over κ and preserves degree when viewed over κ. It follows that $ef = [K(\mu_{q^f-1}) : K] = [\kappa(\mu_{q^f-1}) : \kappa] = f$, so $e = 1$.

173 Proposition

If L, K' are extensions of K and $L' = K'L$ is their compositum, and if L/K is unramified, then L'/K' is unramified.

Proof Since L/K is unramified, $[L : K] = [\lambda : \kappa]$. Let $\overline{\alpha} \in \lambda$ be a primitive element and let $\alpha \in L$ be a lift of $\overline{\alpha}$, which exists by Hensel's lemma (though we can get away without Hensel here). Then $L = K(\alpha)$ by degree considerations. So $L' = K'(\alpha)$ and $\lambda' = \kappa'(\alpha)$. Claim: $m_{K,\alpha}$ has the same degree as $m_{\kappa,\alpha}$ (by Hensel's lemma).

November 20th, 2015: Draft

Summary Last time, we had a diagram of local fields

$$\begin{tikzcd}
& KL \arrow[dl] \arrow[dr] & \\
K \arrow[dr] & & L \arrow[dl] \\
& K &
\end{tikzcd}$$

If L/K is unramified, then LK'/K' is unramified.

174 Corollary

The compositum of any unramified extensions is unramified.

175 Definition

If L/K is an extension of local fields, the $\boxed{\text{maximal unramified subextension}}$ T is the compositum of all unramified subextensions. (By the corollary, this is indeed the maximal subextension with the property of being unramified.)

Last time, we showed the residue field of T is the residue field of L and the value group of T is the value group of K, so in the tower $L/T/K$, T in some sense interpolates between the endpoints.

176 Aside

177 Definition

L/K is $\boxed{\text{tamely ramified}}$ if e is coprime to $p = \mathrm{char}(\kappa)$. One can generalize our discussion to this context to a reasonably large degree, but we will not pursue this.

Upshot: if $n = ef$ is coprime to $p = \mathrm{char}(\kappa)$, then degree n extensions of K are easily characterized.

We next want to relate the theory of extensions of global fields (finite extensions of $\mathbb{Q}$ or $\mathbb{F}_p(t)$) to the theory of extensions of local fields. How do we get from global fields to local fields?

We've already gone from $\mathbb{Q}$ (a global field) to $\mathbb{Q}_p$ (a local field) by taking the completion with respect to $|\cdot|_p$. Let K be a field with an absolute value $|\cdot|$. If $|\cdot|$ is archimedean, then $|\cdot|$ is determined up to equivalence by an embedding $\iota\colon K \to \mathbb{R}$ or $\mathbb{C}$, by Ostrowski's theorem. Let K_ι be the completion of K with respect to this absolute value, which is well-defined on equivalence classes of valuations.

178 Notation

Let K be a field with an absolute value $|\cdot|$. If $|\cdot|$ is archimedean, then let K_ι be the completion with respect ι. If $|\cdot|$ is nonarchimedean, then there exists an associated valuation v, so let K_v be the completion with respect to this valuation.

179 Proposition

Let K be a field with discrete valuation v. Then v extends uniquely to K_v and $v(K_v^\times) = v(K^\times)$ (by the strong triangle inequality). Additionally, if $\mathcal{O}_{K,v} \subset K$ and $\mathcal{O}_v \subset K_v$ are the valuation rings with maximal ideals $\mathfrak{p} \subset K$ and $\mathfrak{p}_v \subset K_v$, then

$$\mathcal{O}_{K,v}/\mathfrak{p}^n \cong \mathcal{O}_v/\mathfrak{p}_v^n \qquad \forall\, n \geq 1.$$

Proof See homework.

180 Proposition

Let $R \subset \mathcal{O}_{K,v}$ be a system of representatives for κ such that $0 \subset R$ and let $\pi \in \mathcal{O}_{K,v}$ be a uniformizer. Then for all $x \in K^\times$ there exists a unique $m \in \mathbb{Z}$ and unique $a_i \in R$ with $a_0 \neq 0$ such that

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots).$$

Proof The argument is exactly the same as for $\mathbb{Z}_p$, so we skip it.

181 Proposition

We have

$$\mathcal{O}_v \xrightarrow{\sim} \varprojlim \mathcal{O}/\mathfrak{p}_v^n \cong \varprojlim \mathcal{O}_{K,v}/\mathfrak{p}^n.$$

Proof This is just combining earlier facts.

182 Notation

Let K be a global field and L/K a finite extension with nontrivial valuation v on K (or an embedding $\iota\colon K \hookrightarrow \mathbb{R}$ or $\mathbb{C}$; we won't belabor this point). Let K_v denote the completion and let $\overline{K_v} := \overline{K_v}$ be the result of completing and then taking the algebraic closure. Note that v extends uniquely to $\overline{K_v}$, say as $\overline{v}$. Choose an embedding $\overline{\iota}\colon L \hookrightarrow \overline{K_v}$. From this we obtain a valuation $w = w_\tau$ on L defined by $w(\alpha) := \overline{v}(\tau(\alpha))$.

Since (by definition of w) τ is continuous, τ extends to an embedding $L_w \hookrightarrow \overline{K_v}$. Diagramattically,

$$\begin{tikzcd}
 & \overline{K_v} & & \\
 & & L_w \arrow[ul] & \\
L \arrow[urr] & & & \\
 & & & K_v \arrow[uul] \\
 & K \arrow[uul] \arrow[urr] & &
\end{tikzcd}$$

Note: w agrees with the unique extension of v (namely $(1/n)v(N_{L_w/K_v})(-)$ where $n = [L_w : K_v]$).

If $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$, then $\sigma \circ \tau$ is another embedding $L \hookrightarrow \overline{K_v}$.

183 Definition

We say τ and $\sigma \circ \tau$ are $\boxed{\text{conjugate embeddings}}$.

From the Newton Polygon proof, we would "morally expect" $w_\tau = w_{\sigma\circ\tau}$ on L_w for all $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$.

184 Theorem (Extension Theorem)

(1) Every valuation w on L extending v on K arises from an embedding $\tau\colon L \hookrightarrow \overline{K_v}$.

(2) Two embeddings τ, τ' give the same valuation if and only if τ is conjugate to τ'.

185 Proposition

Let $L = K[x]/(f(x))$ where $f(x)$ is an irreducible monc polynomial, let v be the valuation. Let $f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}$ be the factorization in K_v. Then there are r valuations of L extending v and the corresponding embeddings are

$$\begin{aligned} \tau_i\colon L &\to \overline{K_v} \\ x &\mapsto \alpha_i \qquad \text{where } \alpha_i \text{ is a root of } f_i(x) \end{aligned}$$

Proof This follows easily from the extension theorem, and is essentially an example. For instance, by the second part, the chosen root of $f_i(x)$ does not matter.

Proof For (1), let w be an extension of v and let L_w be the completion. Since $w|_K = v$, $K_v \hookrightarrow L_w$, and this is in fact finite, so we have $K_v \hookrightarrow L_w \hookrightarrow \overline{K_v}$. Since L_w is complete, there is a unique extension of v to L_w, so w agrees with this unique extension, which agrees with w_τ where $\tau\colon L \hookrightarrow L_w \hookrightarrow \overline{K_v}$.

For (2), consider $\Leftarrow$. Let $\tau' := \sigma \circ \tau$ and consider

$$\begin{tikzcd}
& \overline{K_v} \arrow[dr, "\sigma"] & \\
L \arrow[ur, "\tau"] \arrow[rr, "\tau'"] & & \overline{K_v}
\end{tikzcd}$$

$\overline{v}$ is unique when restricted to any complete subextension of $\overline{K_v}/K_v$, so restrict to the Galois closure of L_w, which is the same as the Galois closure of $L_{w'}$. Then we compute

$$w(alpha) = \bar(v)(\tau(\alpha)) = (\sigma\overline{v})(\alpha) = \overline{v}(\sigma)(\tau(\alpha)) = w'(\alpha).$$

November 23rd, 2015: Draft

186 Notation
Let L/K be a finite extension of global fields and let v be a valuation of K.

187 Theorem (Extension Theorem)
We have:

(1) Every extension w of v to L arises from an embedding $\tau\colon L \hookrightarrow \overline{K_v}$.

(2) Two embeddings τ and τ' are conjugate if and only if $w_\tau := \overline{v} \circ \tau = \overline{v} \circ \tau' =: w_{\tau'}$.

Proof For $\Rightarrow$ in (2), we have $\tau = \sigma^{-1} \circ \tau$ on $\overline{K_v}$ and $\overline{v} = \sigma\overline{v}$, so

$$w_{\tau'} = \overline{v} \circ \tau' = \overline{v} \circ \sigma^{-1} \circ \tau = \sigma\overline{v} \circ \tau = \overline{v} \circ \tau = w_\tau.$$

For $\Leftarrow$ in (2), let $\sigma = \tau' \circ \tau^{-1}\colon \tau L \xrightarrow{\sim} \tau' L$. Note that this is a K-isomorphism. Since τL is dense in $\tau L \cdot K_v$, for all $x \in \tau L \cdot K_v$ there exists $x_n \in L$ such that $x = \varinjlim \tau(x_n)$. Since $\omega_\tau = \omega_{\tau'}$, i.e. $\overline{v} \circ \tau = \overline{v} \circ \tau'$, we have that $(\sigma\tau(x_n)) = (\tau'(x_n))$ also converges. So we can extend $\sigma\colon \tau L \cdot K_v \to \tau' L \cdot K_v$ to a K_v-isomorphism and then choose $\widetilde{\sigma}\colon \overline{K_v} \to \overline{K_v}$ which agrees with σ on $\tau L \cdot K_v$.

188 Proposition
If L/K is separable, then

$$L \otimes_K K_V \to \prod_{w|v} L_w$$

is an isomorphism.

Proof Let $L = K[x]/f(x)$ for an irreducible, separable polynomial $f(x)$. By the Chinese Remainder Theorem,

$$L \otimes_K K_v \cong K_v[x]/f(x) \cong \prod_{w|v} K_v[x]/f_w(x) \cong \prod_{w|v} K_v(\alpha) = L_w$$

using $\tau_w\colon L \to \overline{K_v}$ by $\sum a_i x^i \mapsto \sum a_i \alpha^i$ where α is a root of $f_w(x)$. The composite comes from the map $a \otimes b \mapsto (\tau_w(a)b)$.

189 Corollary

If L/K is separable, then

$$\begin{aligned}[L:K] &= \sum_{w|v}[L_w : K_v] \\ N_{L/K}(\alpha) &= \prod_{w|v} N_{L_w/K_v}(\alpha) \qquad \forall \alpha \in L \\ \mathrm{Tr}_{L/K}(\alpha) &= \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(\alpha) \qquad \forall \alpha \in L.\end{aligned}$$

In particular, the first gives a "fundamental identity" of valuation theory, $[L:K] = \sum_{w|v} e_w f_w$.

Proof The first follows immediately. Notice that $m_{\alpha,L} \otimes K_v = M_{\alpha, L\otimes K_v}$ is similar to a block matrix of m_{α,L_w} and use linear algebra.

190 Remark

What if we apply the preceding theory to the case where L is a number field? What are the absolute values of L, up to equivalence? If $|\cdot|$ is a nonarchimedean valuation v, then $v|_{\mathbb{Q}}$ is a nonarchimedean valuation, so up to equivalence $v|_{\mathbb{Q}} = v_p$. We have bijections

$$\{\text{irreducible factors of } f(x) \text{ over } \mathbb{Q}_p\} \leftrightarrow \{\text{extensions of } v_p\} \leftrightarrow \{\text{embeddings } L \hookrightarrow \overline{\mathbb{Q}_p}\}/\operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$$

One can show that extensions of v_p are in bijection with prime ideals of $\mathcal{O}_L$ lying over p by taking maximal ideals of valuation rings. Assuming $f(x)$ is separable mod p, we can put the primes of $\mathcal{O}_L$ lying over p in bijection with irreducible factors of $f(x)$ over $\mathbb{F}_p$.

What about archimedean absolute values? Then $v_{\mathbb{Q}} = |\cdot|_\infty$. We get a bijection

$$\{\text{extensions of } |\cdot|_\infty \text{ to } L\} \leftrightarrow \{\text{embeddings of } L \hookrightarrow \mathbb{C}\}/\operatorname{Gal}(\mathbb{C}/\mathbb{R}).$$

We now turn to the Galois theory of valuations for number fields.

191 Notation

Let L/K be a Galois extension of number fields. Set $G := \operatorname{Gal}(L/K)$ and let v be a valuation on K.

192 Proposition

$\operatorname{Gal}(L/K)$ acts transitively on extensions w of v to L.

Proof Let w, w' be two extensions of v to L which are not conjugate under G. Then $\{\sigma w : \sigma \in G\}$ and $\{\sigma w' : \sigma \in G\}$ are disjoint, so by the approximation theorem there exists some $x \in L$ such that $|x|_{\sigma w} < 1$ and $|x|_{\sigma w'} > 1$. Then

$$\begin{aligned}|N_{L/K}(x)|_v = \prod_{\sigma\in G} |\sigma x|_w &= \prod_{\sigma \in G} |x|_{\sigma^{-1}w} < 1 \\ = \prod_{\sigma\in G} |\sigma x|_{w'} &= \prod_{\sigma\in G} |x|_{\sigma^{-1}w'} > 1,\end{aligned}$$

a contradiction.

193 Definition

The $\boxed{\text{decomposition group}}$ of $w \mid v$ is

$$\boxed{G_w} := G_w(L/K) := \{\sigma \in \operatorname{Gal}(L/K) : \sigma w = w\}.$$

If v is nonarchimedean, the $\boxed{\text{inertia group}}$ of $w \mid v$ is

$$\boxed{I_w} := I_w(L/K) := \{\sigma \in G_w : w(\sigma(x) - x) > 0, \forall x \in \mathcal{O}_L\}$$

and the $\boxed{\text{ramification group}}$ of $w \mid v$ is

$$\boxed{R_w} := R_w(L/K) := \{\sigma \in G_w : w(\sigma(x)/x - 1) > 0, \forall x \in L^\times\}.$$

Note that $R_w \subset I_w \subset G_w$. The latter two require w to be nonarchimedean.

November 25th, 2015: Draft

194 Notation

Let L/K be a Galois extension of global fields, v be a valuation on K, and w an extension of v to L.

Recall that we had defined the decomposition group G_w (the set of all elements of $\mathrm{Gal}(L/K)$ which fix w), the inertia group I_w (the set of all elements of $\mathrm{Gal}(L/K)$ which fix w and where σ descends to the identity on $\mathcal{O}_L/\mathfrak{p}_w$), and the ramification group R_w (the set of elements of $\mathrm{Gal}(L/K)$ which fix w and where $\sigma(x)/x \equiv_{\mathfrak{p}_w} 1$ for all $x \in \mathcal{O}_L$).

195 Remark

Suppose L'/K' is as L/K and assume there exists $\tau\colon L \hookrightarrow L'$ such that

$$\begin{tikzcd}
 & L' & \\
L \arrow[ur, hook, "\tau"] & & K' \arrow[ul] \\
 & K \arrow[ul] \arrow[ur, hook, "\tau"'] &
\end{tikzcd}$$

we get a homomorphism

$$\tau^*\colon\ \mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$$

defined by

$$\sigma \mapsto \tau^{-1}\sigma\tau.$$

(Note that $\sigma\colon \tau L \to \tau L'$, so τ^{-1} is defined on $\sigma\tau L$.)

196 Proposition

Let v' be a valuation on K', w' an extension of v' to L', so $v = v'|_K, w = w'|_K$. Then τ^* induces homomorphsisms

$$\tau^*\colon G_{w'}(L'/K') \to G_w(L/K)$$
$$\tau^*\colon I_{w'}(L'/K') \to I_w(L/K)$$
$$\tau^*\colon R_{w'}(L'/K') \to R_w(L/K).$$

Proof We just need to show that τ^* restricted to each of these subgroups lands in the appropriate subgroup of the codomain. Let $\sigma \in \mathrm{Gal}(L'/K')$, $x \in L$. If $\sigma \in G_w(L'/K')$, we see

$$(w \circ \tau^*\sigma)(x) = (w \circ \tau^{-1}\sigma\tau)(x) = w'(\sigma\tau(x)) = (w' \circ \sigma)(\tau(x)) = w'(\tau(x)) = w \circ \tau^{-1}(\tau(x)) = w(x).$$

Similarly, if $\sigma \in I_w(L'/K')$, then

$$w(\tau^*\sigma x - x) = w(\tau^{-1}\sigma\tau x - x) = w \circ \tau^{-1}(\sigma\tau x - \tau x) = w'(\sigma(\tau x) - \tau x) > 0.$$

A very similar argument also works for R_w.

197 Remark

If τ and $\tau|_K$ are isomorphisms, then τ^* induces isomorphisms on the respective groups.

198 Corollary

If $L' = L$, $K' = K$, and $\tau, \tau|_K$ are isomorphisms, then $G_{w\circ\tau}(L/K) = \tau^{-1}G_w\tau$, $I_{w\circ\tau}(L/K) = \tau^{-1}I_w\tau$, $R_{w\circ\tau}(L/K) = \tau^{-1}R_w\tau$.

199 Corollary

If $L/M/K$ is a tower of extensions with L/K Galois (so L/M is Galois, but M/K need not be Galois), then

$$\begin{aligned} G_w(L/M) &= G_w(L/K) \cap \mathrm{Gal}(L/M) \\ I_w(L/M) &= I_w(L/K) \cap \mathrm{Gal}(L/M) \\ R_w(L/M) &= R_w(L/K) \cap \mathrm{Gal}(L/M). \end{aligned}$$

Proof Let $L' = L$, $\tau = \mathrm{id}$, $K' = M$. Then τ^* is just the inclusion of $\mathrm{Gal}(L/M)$ into $\mathrm{Gal}(L/K)$. Then $G_w(L/M) \hookrightarrow G_w(L/K)$, where $G_w(L/M) \subset \mathrm{Gal}(L/M)$, $G_w(L/K) \subset \mathrm{Gal}(L/K)$.

200 Corollary

We have

$$\begin{aligned} G_w(L/K) &= \mathrm{Gal}(L_w/K_v) \\ I_w(L/K) &= I_w(L_w/K_v)[= I(L_w/K_v)] \\ R_w(L/K) &= R_w(L_w/K_v)[= R(L_w/K_v)], \end{aligned}$$

where the pieces in brackets are referring to the fact that there is a unique w by completeness.

Proof Use

$$\begin{tikzcd}
 & L_w & \\
L \arrow[ur, hook, "\mathrm{id}"] & & K_v \arrow[ul] \\
 & K \arrow[ul] \arrow[ur, hook, "\mathrm{id}"] &
\end{tikzcd}$$

so that τ^* is just restriction $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(L/K)$.

Claim 1: it suffices to show that $G_w(L/K) = \mathrm{Gal}(L_w/K_v)$, which is straightforward and a nice (small) exercise in the definitions.

Claim 2:

$$G_w(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma \text{ is continuous with respect to } w\}.$$

For this, $\subset$ is clear from the definition, since constant maps are continuous. On the other hand, suppose $\sigma \in \mathrm{Gal}(L/K)$ is continuous with respect to w, so w is equivalent to $w \circ \sigma$ (since the topologies agree). Since $w|_K = w \circ \sigma|_K$, they agree on a non-zero element, so $w \sim w \circ \sigma$ implies $w = w \circ \sigma$ is in $G_w(L/K)$, completing Claim 2.

Now, an element $\sigma \in G_w(L/K)$ extends uniquely to an element $\sigma \in \mathrm{Gal}(L_w/K_v)$, since σ (being continuous) extends uniquely to L_w as the limit of finite extensions, and this fixes K, so also K_v. This completes Claim 1 and the proof.

201 Remark

Fixing an extension w, then G_w controls all extensions of v to L. More precisely,

$$\begin{aligned} G_w\backslash G &\leftrightarrow \{\text{extensions of } v \text{ to } L\} \\ \sigma &\mapsto w \circ \sigma. \end{aligned}$$

This also works for extensions that are not necessarily Galois. That is, suppose $N/L/K$ is a tower of extensions where N/K is Galois, but L/K is not necessarily Galois. Suppose w is a valuation on N extending the valuation v on K. Then

$$\begin{aligned} G_w(N/K)\backslash \operatorname{Gal}(N/K)/\operatorname{Gal}(N/L) &\leftrightarrow \{\text{extensions of } v \text{ to } L\} \\ \sigma &\mapsto w \circ \sigma|_L. \end{aligned}$$

This is well-defined since

$$w \circ (g\sigma h)|_L = (w \circ g) \circ (\sigma h)|_L = w \circ (\sigma h)|_L = w \circ \sigma|_L.$$

202 Notation

Let L/K be Galois, and let w be an extension of v.

203 Definition

The $\boxed{\text{decomposition field}}$ $\boxed{Z_w}$ $:= Z_w(L/K)$ is the fixed field of G_w, the $\boxed{\text{inertia field}}$ $\boxed{T_w}$ $:= T_w(L/K)$ is the fixed field of I_w, and the $\boxed{\text{ramification field}}$ $\boxed{R_w}$ $:= R_w(L/K)$ is the fixed field of R_w.

Note: Z_w, T_w, V_w are not necessarily complete. We have $L \supset V_w \supset T_w \supset Z_w \supset K$.

204 Proposition

We have the following:

(1) The restriction w_z of w to Z_w extends uniquely to L.

(2) w_z has the same value group and residue field as v.

(3) $Z_w = L \cap K_v$ (in the completion L_w)

(4) $1 \to I_w \to G_w \to \operatorname{Gal}(\lambda/\kappa) \to 1$, where λ is the residue field of w, κ is the residue field of v

(5) T_w/Z_w is the maximal unramified subextension of L/Z_w

(6) $1 \to R_w \to I_w \to \chi(L/K) := \operatorname{Hom}(w(L^\times)/v(K^\times)), \lambda^\times) \to 1$

(7) R_w is the unique p-Sylow subgroup of I_w

(8) V_w/Z_w is the maximal tamely ramified subextesnion of L/Z_w.

Proof We skip proving (1)-(5) since you can compare them to our earlier reasoning involving prime ideals instead of valuations. They are relatively straightforward as well. We won't be able to completely prove (6)-(8) both because of time constraints and because they involve some structure theorems for tamely ramified extensions. So, we give a sketch.

For (6), use $I_w \to \chi(L/K)$ given by $\sigma \mapsto (\chi_\sigma : \overline{\delta} \mapsto \sigma(x)/x \bmod \mathfrak{p}$ where $\delta \in w(L^\times)$ is some lift of $\overline{\delta}$ and $x \in L^\times$ is such that $w(x) = \delta$. It is not obvious that this is well-defined, which ends up depending on σ being in I_w (as opposed to, say G_w). It follows that R_w is the kernel, so is normal. It's not clear that this map is surjective.

(8) follows from (7) in part because (7) implies that the degree of L/V_w is prime to p. (7) follows from a cardinality count together with (6). Both of these depend on structure theorems for tamely ramified extensions.

November 30th, 2015: Draft

Today, we'll begin a discussion of Galois cohomology. Today's topics are topological groups and profinite groups. Our main references are Milne's notes on class field theory (chapter II) and Cassels-Frohlich (chapter IV).

205 Definition

A $\boxed{\text{topological group}}$ is a group G together with a topology such that the multiplication and inversion maps $G \times G \to G$ and $G \to G$ are continuous. In this class, we will also assume topological groups are Hausdorff. This is not entirely standard. This is equivalent to the inclusion $e \hookrightarrow G$ being closed.

206 Fact

In a topological group, we have the following:

(1) If $U \ni e$ is an open neighborhood, there exists a $\boxed{\text{symmetric}}$ open neighborhood $U \supset V \ni e$ such that $V = V^{-1}$ and $V \cdot V \subset U$.

(2) If $H \leq G$, then $\overline{H}$ (the closure in the topology) is also a subgroup. Further, if $H \trianglelefteq G$, then $\overline{H} \trianglelefteq G$.

(3) An open subgroup of G is closed and a finite index closed subgroup is open.

(4) An open subgroup of a compact group is finite index.

(1) is mostly technical, though (2) and (3) will come up during proofs frequently enough that we will eventually use them without comment. These are a good exercise if you feel unfamiliar with topological groups.

207 Definition

A $\boxed{\text{profinite group}}$ is a topological group G that is isomorphic to an inverse limit of *discrete* finite groups. The topology on an inverse limit is the coarsest topology such that all of the projection maps are continuous.

208 Example

$\mathbb{Z}_p$; more generally, the valuation ring $\mathcal{O}$ of a nonarchimedean local field, i.e. $\varprojlim \mathcal{O}/\mathfrak{p}^n$. Later, we'll see that if E/K is a Galois extension, then $\mathrm{Gal}(E/K)$ is a profinite group. Any finite group is trivially a profinite group (with the discrete topology).

209 Theorem

A topological group G is profinite if and only if G is compact and totally disconnected.

Proof Omitted; relies on topological facts we don't want to take the time to go through.

210 Corollary

If G is profinite, then $G \cong \varprojlim G/U$ where the limit is taken over all normal open $U \trianglelefteq G$. (Since G is compact, each U is of finite index by fact (4) above, so this makes sense.)

211 Corollary

If $H \trianglelefteq G$ is closed, then

$$H \cong \varprojlim H/(H \cap U),$$

where the limit is over all normal open $U \trianglelefteq G$.

212 Corollary

If $H \trianglelefteq G$ is closed, then G/H is profinite.

213 Proposition

If E/F is any Galois extension (i.e. normal and separable), then

$$\mathrm{Gal}(E/F) \cong \varprojlim \mathrm{Gal}(K/F)$$

where the limit is over all finite Galois subextensions $E \supset K \supset F$ (i.e. $K \supset F$ is finite and Galois).

Proof We define an isomorphism $\rho\colon \operatorname{Gal}(E/F) \to \varprojlim \operatorname{Gal}(K/F)$. Since K/F is a finite Galois subextension, we have a restriction morphism $\operatorname{Gal}(E/F) \to \operatorname{Gal}(K/F)$. Hence we get a homormorphism $\operatorname{Gal}(E/F) \to \prod_{E/K/F} \operatorname{Gal}(K/F)$, and the image is contained in the inverse limit because the restriction maps satisfy the requisite compatibility condition.

We first show that ρ is injective. If $\mathrm{id} \neq \sigma \in \operatorname{Gal}(E/F)$, there exists $x \in E - F$ such that $\sigma(x) \neq x$, so there exists $E/K/F$ with $x \in K$ and K/F finite and Galois (e.g. take K to be the Galois closure of $F[x]$). Now $\sigma|_K \neq \mathrm{id}$, so $\rho(\sigma)$ is not the identity.

For surjectivity, let $(\sigma_K) \in \varprojlim \operatorname{Gal}(K/F)$. Define $\sigma\colon E \to E$ such that $\sigma(x) = \sigma_K(x)$ where K is such that $x \in K$. Assuming this is well-defined, surjectivity is clear, but this follows immediately from the compatibility condition for the inverse limit (that the underlying index set is directed is essential here, i.e. the compositum is used).

214 Theorem (Fundamental Theorem of Galois Theory)
Let E/F be any Galois extension. Then there is an inclusion-reversing bijection

$$\{\text{subfield extensions of } E/F\} \leftrightarrow \{\text{closed subgroups of } \operatorname{Gal}(E/F)\}$$
$$K \mapsto \operatorname{Gal}(E/K)$$
$$E^h := \{x \in E : \sigma(x) = x, \forall \sigma \in H\} \leftarrow H.$$

Proof We'll only discuss the parts which are different in the infinite case than in the finite case. (Note that all subgroups are closed in the finite case.)

Step 1) Claim: $\operatorname{Gal}(E/K)$ is a closed subgroup. Note $K = \cup L_i$, where the union is over all $K \supset L_i \supset F$ where $L_i \supset F$ is finite. Hence $\operatorname{Gal}(E/K) = \cap_i \operatorname{Gal}(E/L_i)$. Each $\operatorname{Gal}(E/L_i)$ is closed for reasons that currently elude us (to be fixed).

Step 2) Claim: $K = E^{\operatorname{Gal}(E/K)}$. The proof is as in the finite case.

Step 3) Claim: let $H' := \operatorname{Gal}(E/E^H)$; then $H' = H$. That $H' \supset H$ is clear. On the other hand, by step 2 we have $E^H = E^{H'}$. Hence at the finite level, we have $H'/U = HU/U$ for all $U \trianglelefteq H$. Hence H is dense in H'. Since H is closed, $H = \overline{H} = H'$. More generally, groups that have the same closure end up mapping to the same field, so you generally just recover the closure of the starting group.

December 2nd, 2015: Draft

There will be no class on Friday.

215 Remark
At the end of last class, we had a Galois extension E/F and a subextension $E/K/K$. We wanted to show that $\operatorname{Gal}(E/K)$ was closed in $\operatorname{Gal}(E/F)$. We wrote $\operatorname{Gal}(E/K) = \cap \operatorname{Gal}(E/L_j)$ where $K/L_j/F$ with L_j/F finite, so we reduced to showing that each $\operatorname{Gal}(E/L_j)$ is closed. Here's essentially Sid's argument to finish this. Write L instead of L_j. It's important to note that L/F is finite but not necessarily Galois. However, $\operatorname{Gal}(E/L) = \{\sigma \in \operatorname{Gal}(E/F) : \sigma|_L = \mathrm{id}\}$ is a subgroup of $\operatorname{Gal}(E/F) = \varprojlim \operatorname{Gal}(K/F)$, so $\operatorname{Gal}(E/L)$ is $\{(\sigma_K) : \sigma_K \text{ fixes } L \cap K, \forall K/F \text{ finite, Galois}\}$ which is $\cap_{K/F} \pi_K^{-1}(\operatorname{Gal}(K/(L \cap K))$. Each term of this last intersection is closed and of finite index (so also open), which gives the result.

216 Definition
Let G be a topological group. A $\boxed{\text{continuous } G\text{-module}}$ M means M is a topological abelian group with a continuous map $G \times M \to M$ such that $g(m + m') = g(m) + g(m')$, $(gg')(m) = g(g'(m))$,

and $1 \cdot m = m$. A $\boxed{\text{homomorphism of } G\text{-modules}}$ $\alpha M \to N$ is a group homomorphism such that $\alpha(gm) = g\alpha(m)$.

217 Remark

If M is a G-module, then the G action extends uniquely to a $\mathbb{Z}[G]$-module.

218 Definition

Let $H \leq G$ be a subgroup and N an H-module. We would like to augment N to make it a G-module. To do so, define

$$\boxed{\operatorname{Ind}_H^G(N)} := \{\text{maps } \phi \colon G \to N \mid \phi(hg) = h\phi(g)\}.$$

We give $\operatorname{Ind}_H^G(N)$ an abelian group structure by pointwise addition, $(\phi + \phi')(x) := \phi(x) + \phi'(x)$, and we defing the G-action by $(g \cdot \phi)(x) := \phi(xg)$.

Note: if $\alpha \colon N \to N'$ is an H-module map, we have an induced map $\operatorname{Ind}_H^G(N) \to \operatorname{Ind}_H^G(N')$ given by $\phi \mapsto \alpha \circ \phi$.

219 Lemma

(1) For all G-modules M and all H-modules N,

$$\operatorname{Hom}_G(M, \operatorname{Ind}_H^G(N)) \cong \operatorname{Hom}_H(M, N)$$

(2) $\operatorname{Ind}_H^G \colon \operatorname{Mod}_H \to \operatorname{Mod}_G$ is an exact functor.

Proof For (1), take $\alpha \in \operatorname{Hom}_G(M, \operatorname{Ind}_H^G(N))$ and define $\beta_\alpha \colon M \to N$ by $m \mapsto (\alpha(m))(1)$. It is easy to check that β_α is a group homomorphism. Now look at the action of $h \in H$:

$$\beta_\alpha(hm) = \alpha(hm)(1) = (h(\alpha(m)))(1) = \alpha(m)(h1) = h(\alpha(m)(1)) = h\beta_\alpha(m).$$

Hence we have a map for (1) in the forward direction. For the backwards direction, let $\beta \in \operatorname{Hom}_H(M, N)$ and define $\alpha_\beta \colon M \to \operatorname{Ind}_H^G(N)$ by $m \mapsto (g \mapsto \beta(gm))$. This evidently a group homomorphism. Now we see

$$\begin{aligned}
\alpha_\beta(g'm) &= (g \mapsto \beta(gg'm)) \\
g'(\alpha_\beta(m)) &= g'(g \mapsto \beta(gm)) \\
&= (g \mapsto \beta((gg')m)),
\end{aligned}$$

so they are indeed equal.

Now we check that they are mutual inverses. Consider $\beta \mapsto \alpha_\beta \mapsto \beta_{(\alpha_\beta)}$, so $\alpha_\beta \colon m \mapsto (g \mapsto \beta(g(m)))$, and $\beta_{(\alpha_\beta)} \colon m \mapsto (\alpha_\beta(m))(1) = \beta(1(m)) = \beta(m)$. Now consider $\alpha \mapsto \beta_\alpha \mapsto \alpha_{(\beta_\alpha)}$. We have $\beta_\alpha \colon m \mapsto \alpha(m)(1)$ and $\alpha_{(\beta_\alpha)} \colon m \mapsto (g \mapsto \beta_\alpha(g(m))) = (g \mapsto \alpha(gm)(1) = \alpha(m)(g)) = \alpha(m)(1)$. This completes (1).

For (2), consider an exact sequence $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$ of H-modules. We must show that

$$0 \to \operatorname{Ind}_H^G(M) \xrightarrow{\iota} \operatorname{Ind}_H^G(N) \xrightarrow{\pi} \operatorname{Ind}_H^G(P) \to 0$$

is exact. We have $\iota \colon \phi \mapsto \alpha \circ \phi$. It follows quickly that it is exact at $\operatorname{Ind}_H^G(M)$. For the middle factor, that the composite of the two maps is 0 is immediate, and the other half of exactness is nearly the same argument as for the left factor. So, the only difficulty is showing exactness at the rightmost factor. We have $\pi \colon \psi \mapsto \beta \circ \psi$.

Pick $\phi \in \operatorname{Ind}_H^G(P)$ and consider "lifting" ϕ. Let s be a right coset representative for H in G and let $n(s) \in N$ be such that $\phi(s) = \beta(n(s))$. Define $\widetilde{\phi}(hs) := h \cdot (n(s))$ and check that $\beta \circ \widetilde{\phi} = \phi$ to complete the proof.

220 Corollary

Let M be a G-module, $H \leq G$ a subgroup. For all H-module homomorphisms $\beta\colon M \to N$, then there exists a unique $\alpha\colon M \to \operatorname{Ind}_H^G(N)$ such that

$$\begin{tikzcd}
M \arrow[d, dashed, "\exists!\alpha"'] \arrow[dr, "\beta"] & \\
\operatorname{Ind}_H^G(N) \arrow[r] & N
\end{tikzcd}$$

where the bottom arrow is given by $\phi \mapsto \phi(1)$.

221 Example

Let $H = \{1\}$. Then H-modules are simply abelian groups. Now

$$\operatorname{Ind}_{\{1\}}^G(M) = \operatorname{Ind}^G(M) = \{\phi\colon G \to M\} = \operatorname{Hom}(\mathbb{Z}[G], M).$$

M' is $\boxed{\text{induced from } H}$ if $M' \cong \operatorname{Ind}_H^G(M)$ for some H-module M. If $H = \{1\}$, we often omit it from the notation.

222 Remark

Let G be a finite group, $H \leq G$ a subgroup.

(a) A G-module M is induced if and only if there exists an abelian group M_0 such that $M = \oplus_{g \in G} gM_0$, in which case $\operatorname{Ind}^G(M_0) \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ by $\phi \mapsto \sum_g g \otimes \phi(g^{-1})$.

(b) Suppose H is a subgroup of G. If M is an induced G-module, then M is an induced H-module.

(c) If M is a G-module, then there exists a surjective homomorphism $\operatorname{Ind}^G(M) \twoheadrightarrow M$ given by $\phi \mapsto \sum_g g\phi(g^{-1})$. In terms of $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0 \to M$, this is $(\sum n_g g) \otimes m \mapsto \sum n_g gm$.

December 7th, 2015: Draft

We'll continue our discussion of cohomology groups.

223 Notation

Let M denote some G-module. Let M^G denote the elements of M which are fixed under the action of G. One may check that $M \to M^G$ is left exact directly. Alternatively, one can note $M \to M^G = \operatorname{Hom}_G(\mathbb{Z}, M)$ where $\mathbb{Z}$ has the trivial action, and $\operatorname{Hom}_G(\mathbb{Z}, -)$ is left exact in general.

224 Definition

We say a G-module I is $\boxed{\text{injective}}$ if $\operatorname{Hom}(-, I)$ is an exact functor.

225 Defitheorem

For every G-module M, there exists an injective G-module$I$ and an injection $M \hookrightarrow I$. This is often phrased by saying "the category of G-modules has $\boxed{\text{enough injectives}}$".

In particular, every G-module M has an injective resolution, i.e. there exists an exact sequence

$$0 \to M \to I^0 \to I^1 \to I^2 \to \cdots$$

where each I^j is an injective G-module. (This arises by taking injections from cokernels.) The rth $\boxed{\text{cohomology group}}$ of G with coefficients in M is

$$\boxed{H^r(G, M)} := \frac{\ker d^r\colon (I^r)^G \to (I^{r+1})^G}{\operatorname{im} d^{r-1}(I^{r-1})^G \to (I^r)^G} \qquad r \geq 0, I^{-1} := 0.$$

This definition is independent of the choice of $I^\bullet$ and gives functors $M \mapsto H^r(G, M)$. (For more details, see the appendix to chapter 2 of Milne's class field theory notes.)

226 Theorem

The functors $M \to H^r(G, M)$ are uniquely determined by the following properties:

(a) $H^0(G, M) = M^G$ for all G-modules M

(b) $H^r(G, I) = 0$ for all $r > 0$ and injective G-modules I

(c) For all short exact sequences of G-modules

$$0 \to M \to N \to P \to 0$$

there exists a long exact sequence

$$\begin{aligned} 0 &\to H^0(G, M) \to H^0(G, N) \to H^0(G, P) \\ &\overset{\delta^1}{\to} H^1(G, M) \to H^1(G, N) \to H^1(G, P) \\ &\overset{\delta^2}{\to} \cdots \end{aligned}$$

The maps δ^r are also uniquely determined.

Proof We'll show the injective resolution definition has (some of) these properties. For (a), we have $0 \to M \to I^0 \to I^1 \to \cdots$, which gives $0 \to M^G \to (I^0)^G \to (I^1)^G$, which is exact. Hence $H^0(G, M)$ is measuring exactness at $0 \to (I^0)^G \to (I^1)^G$, which is $\ker (I^0)^G \to (I^1)^G = \operatorname{im} M^G \to (I^0)^G = M^G$.

For (b), $I^0 = I$, $I^j = 0$ for all $j > 0$ is an injective resolution. Applying the fixed points functor to $0 \to I \to I^0 \to 0$ and computing homology gives the result immediately. We omit (c).

227 Proposition (Shapiro's Lemma)

Let H be a subgroup of G and let M be an H-module. Then for any $r \geq 0$, $H^r(G, \operatorname{Ind}_H^G(N)) \cong H^r(H, N)$. In particular, $H^r(G, \operatorname{Ind}^G(M_0)) = 0$ for all $r > 0$.

Proof Let A be any H-module. We have $A^H \cong \operatorname{Hom}_R(\mathbb{Z}, A) \cong \operatorname{Hom}_G(\mathbb{Z}, \operatorname{Ind}_H^G(A)) \cong \operatorname{Ind}_H^G(A)$. Now let $N \to I^\bullet$ be an injective resolution. Then

$$0 \to \operatorname{Ind}_H^G(N) \to \operatorname{Ind}_H^G(I^\bullet)$$

is injective. In fact, one can check that inducing an injective module preserves injectivity, so $\operatorname{Ind}_H^G(I^j)$ is injective. By the observation at the start of the proof, $0 \to (I^\bullet)^H$ is isomorphic to $0 \to (\operatorname{Ind}_H^G(I^\bullet))^G$, so $H^r(H, N) \cong H^r(G, \operatorname{Ind}_H^G(N))$.

For the final claim, $H^r(G, \operatorname{Ind}^G(M_0)) \cong H^r(\{e\}, M_0) = 0$ for all $r > 0$.

228 Aside

When $r = 0$, this argument is reasonable to do by hand. For higher r, it becomes a pain to compute the relevant isomorphism explicitly because of the need to repeatedly induce the injective resolution.

Shapiro's lemma is used in many ways. We'll explore the case of $\boxed{\text{dimension shifting}}$.

229 Definition

Let M be a G-module. Take $M_* := \operatorname{Ind}_{\{e\}}^G(M)$. From our definition of induced modules, M naturally injects into M_* (as the constant functions), so we have an exact sequence

$$0 \to M \to M_* \to N \to 0.$$

Taking cohomology with coefficients in G gives a long exact sequence

$$\begin{aligned} &0 \to M \to M_* \to N \to 0 \\ &\cdots \\ &\to H^r(M) \to H^r(M_*) \to H^r(N) \\ &\to H^{r+1}(M) \to H^{r+1}(M_*) \to \cdots \end{aligned}$$

This allows for inductive proofs using Shapiro's lemma when enough terms can be shown to cancel.

230 Definition

We next define cohomology via (inhomogenous) $\boxed{\text{cochains}}$. Set $G^0 := \{e\}$, $\boxed{C^r(G, M)} := \{\text{maps } \phi\colon G^r \to M\}$. Define boundary maps

$$\boxed{d^r}\colon C^r(G, M) \to C^{r+1}(G, M)$$

$$\phi \mapsto \left((g_1, \ldots, g_{r+1}) \mapsto g_1\phi(g_2, \ldots, g_{r+1}) + \sum_{j=1}^{r} (-1)^j \phi(g_1, \ldots, g_{r+1}) + (-1)^{r+1})\phi(g_1, \ldots, g_r) \right).$$

The group of r-$\boxed{\text{cocycles}}$ is $\boxed{Z^r(G, M)} := \{\phi \in C^r(G, M) : d^r\phi = 0\}$, and the group of r-$\boxed{\text{coboundaries}}$ is $\boxed{B^r(G, M)} = \operatorname{im} d^{r-1}$.

231 Proposition

$d^r \circ d^{r-1}$ for all r and $H^r(G, M) \cong Z^r(G, M)/B^r(G, M)$.

232 Example

Let $r = 1$, so $Z^1(G, M) = \{\phi\colon G \to M \mid g_1\phi(g_2) - \phi(g_1g_2) + \phi(g_2) = 0\}$. The constraint on ϕ is equivalent to $\phi(g_1g_2) = g_1\phi(g_2) + \phi(g_1)$, and such ϕ are referred to as $\boxed{\text{crossed homomorphisms}}$. Setting $g_1 = g_2 = e$, we still get $\phi(e) = 0$. This is surprisingly amenable to computation.

The coboundaries $B^1(G, M) = \{\phi\colon G \to M \mid \phi(g) = g(m) - m \text{ for some } m \in M\}$. These are called $\boxed{\text{principal crossed homomorphisms}}$. If G acts trivially on M, then $H^1(G, M) = \operatorname{Hom}(G, M)$.

233 Remark

$H^2(G, M)$ classifies extensions of G by M with a fixed action of G on M.

234 Example

Suppose $G = \langle\sigma\rangle$ is a cyclic group. Consider $\phi \in Z^1(G, M)$, so $\phi(\sigma^{i-1}) = \sigma^{i-1}\phi(\sigma) + \phi(\sigma^{i-1})$. Hence ϕ is determined by $\phi(\sigma)$. If $\sigma^n = e$, then

$$\begin{aligned} 0 = \phi(\sigma^n) &= \sigma^{n-1}\phi(\sigma) + \phi(\sigma^{n-1}) = \cdots \\ &= (\sigma^{n-1} + \sigma^{n-2} + \cdots + \sigma + e)\phi(\sigma). \end{aligned}$$

Hence $\phi(\sigma) = m \in \ker N_G$, where N_G denotes the $\boxed{\text{norm map}}$ $m \mapsto (\sigma^{n-1} + \cdots + \sigma + e)(m)$. We then find $H^1(G, M) = \ker N_G/(\sigma - 1)(M)$.

We now define the connecting homomorphisms of long exact sequences in terms of cochains.

235 Definition

Let $0 \to M \to N \to P \to 0$ be a short exact sequence of G-modules. Let $\delta^r\colon H^r(G, P) \to H^{r+1}(G, M)$ be defined as follows. For $\phi \in Z^r(G, P)$, lift it to $\widetilde{\phi} \in C^r(G, N)$. Then $d^r\widetilde{\phi}\colon G^{r+1} \to N$, and in fact we find the image of $d^r\widetilde{\phi}$ is in M. Hence $\phi \mapsto d^r\widetilde{\phi}$.

December 9th, 2015: Draft

Having defined group cohomology in several ways, today we'll discuss its functorial properties.

236 Notation

Let G, G' be groups, M a G-module, M' a G'-module.

237 Definition

We say homomorphisms $\alpha\colon G' \to G$ and $\beta\colon M \to M'$ are $\boxed{\text{compatible homomorphisms}}$ if $\beta(\alpha(g')m) = g'(\beta(m))$. (Here β is just an abelian group homomorphism.) This is precisely saying that viewing M as a G'-module under induced by α, β is a G'-module morphism.

238 Example

If $\alpha = \mathrm{id}$, then this condition reduces precisely to requiring β is a G-module homomorphism.

239 Definition

If (α, β) are compatible, then we obtain a homomorphism of of complexes $C^\bullet(G, M) \to C^\bullet(G', M')$ given by $\phi \mapsto \beta \circ \phi \circ \alpha^r$. This induces (group) homomorphisms $H^r(G, M) \to H^r(G', M')$ for all $r \geq 0$.

240 Example

1. Shapiro's lemma says $H^r(G, \mathrm{Ind}_H^G(M)) \xrightarrow{\sim} H^r(H, M)$. Let $\alpha\colon H \hookrightarrow G$ and $\beta\colon \mathrm{Ind}_H^G(M) \to M$ by $\beta(\phi) := \phi(e)$. These maps are in fact compatible:

$$h(\phi(e)) = \phi(h) = \phi(eh) = (h\phi)(e) = \beta(h\phi).$$

   In fact, the resulting map $H^r(G, M) \to H^r(G', M')$ above is the isomorphism from our proof of Shapiro's lemma. Going the other way is a bit irritating.

2. Let $\alpha\colon H \hookrightarrow G$ and $\beta\colon M \to M$ be the identity. This gives the $\boxed{\text{restriction map}}$

$$\boxed{\mathrm{Res}}\colon H^r(G, M) \to H^r(H, M),$$

   which on cocycles is obtained precisely by restricting the domain. Alternatively, consider $\alpha\colon G \to G$ by the identity and $\beta\colon M \to \mathrm{Ind}_H^G(M)$ by $m \mapsto (g \mapsto g \cdot m)$. This gives a map $H^r(G, M) \to H^r(G, \mathrm{Ind}_H^G(M))$. Composing this with the map from Shapiro's lemma gives

$$\mathrm{Res}\colon H^r(G, M) \to H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(H, M)$$

3. Let $H \trianglelefteq G$, $\alpha\colon G \to G/H$, $\beta\colon M^H \hookrightarrow M$. This gives the $\boxed{\text{inflation map}}$

$$\boxed{\mathrm{Inf}}\colon H^r(G/H, M^H) \to H^r(G, M).$$

4. Fix $g_0 \in G$. Consider $\alpha_{g_0}\colon G \to G$ given by conjugation: $\sigma \mapsto g_0 \sigma g_0^{-1}$. Let $\beta_{g_0}\colon M \to M$ by $m \mapsto g_0^{-1} m$. One can check these two maps are compatible, so they give rise to $H^r(G, M) \to H^r(G, M)$, which is clearly an isomorphism. In fact, this is the identity, which we'll show in a moment.

   As a consequence, α_g, β_g give a G-action on $H^r(H, M)$ for H normal. The induced H-action will be trivial, so the G-action factors through G/H, giving a natural G/H-action on $H^r(H, M)$ for any $H \trianglelefteq G$.

   To see that the induced map is the identity, consider $r = 0$, so $M^G \to M^G$ by $m \mapsto \beta(m) = g_0^{-1} m = m$. Now assume the result is true for $r = n - 1$ and apply dimension shifting to the short exact sequence

$$0 \to M \to \mathrm{Ind}^G(M) \to N \to 0$$

   which yields a morphism of long exact sequences

$$\begin{tikzcd}
H^{r-1}(G, \mathrm{Ind}^G(M)) \arrow[r] \arrow[d, "\mathrm{id}"] & H^{r-1}(G, N) \arrow[r] \arrow[d, "\mathrm{id}"] & H^r(G, M) \arrow[r] \arrow[d, dashed] & 0 \\
H^{r-1}(G, \mathrm{Ind}^G(M)) \arrow[r] & H^{r-1}(G, N) \arrow[r] & H^r(G, M) \arrow[r] & 0
\end{tikzcd}$$

Now $H^r(G, M) \to H^r(G, M)$ must be the identity.

5. Let $H \leq G$ be a subgroup of finite index and let S be a set of left coset representatives. Define a homomorphism $N_{G/H} \colon M^H \to M^G$ given by $m \mapsto \sum_{s \in S} sm$. This is independent of the representatives since M is fixed by H and is well-defined. We can think of this as $N_{G/H} \colon H^0(H, M) \to H^0(G, M)$. As a general yoga, one should be able to extend things from H^0 to all H^r, and we may do so here. Define $\beta \colon \mathrm{Ind}_H^G(M) \to M$ by $\phi \mapsto \sum_{s \in S} s\phi(s^{-1}))$. We claim β is a G-module homomorphism:

$$\begin{aligned}
\beta(g\phi) &= \sum_{s \in S} s(g\phi)(s^{-1}) = \sum_{s \in S} s\phi(s^{-1}g) \\
&= \sum_{s \in S} gg^{-1}s\phi(s^{-1}g) = g \sum_{s \in S} s\phi(s^{-1}) \\
&= g\beta(\phi).
\end{aligned}$$

Hence we get a map $H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(G, M)$. We want a $\boxed{\text{corestriction}}$ map

$$\boxed{\mathrm{Cor}} \colon H^r(H, M) \to H^G, M),$$

so we use Shapiro's lemma:

$$\begin{tikzcd}
H^r(G, \mathrm{Ind}_H^G(M)) \arrow[r] \arrow[d, "\sim"] & H^r(G, M) \\
H^r(H, M) \arrow[ur, dashed, bend right, "\mathrm{Cor}"'] &
\end{tikzcd}$$

Hence corestriction is easy to compute on H^0, but because we have to use the inverse of the Shapiro's lemma map for $r > 0$, it's annoying to compute in general. Geometrically, restriction is roughly like pulling back, and corestriction is like pushing forward.

241 Proposition

Let $H \leq G$, $[G : H] = n$, M a G-module. Then

$$\mathrm{Cor} \circ \mathrm{Res} \colon H^r(G, M) \to H^r(H, M) \to H^r(G, M)$$

is multiplication by $[G : H]$.

242 Corollary

If G has finite order n, then $nH^r(G, M) = 0$ for all $r > 0$.

Proof Multiplication by n factors through $H^r(\{e\}, M) = 0$.

243 Corollary

If G is finite and M is a finitely generated abelian group, then $H^r(G, M)$ for $r > 0$ is finite.

Proof It's annihilated by n by the first corollary, and from cocycles it is clearly finitely generated, so it must in fact be finite.

244 Corollary

If G is finite and G_p is a p-Sylow subgroup, then

$$\mathrm{Res} \colon H^r(G, M) \to H^r(G_p, M)$$

is injective on the p-primary component.

Proof This follows from the fact that $[G : G_p]$ is relatively prime to p.

Proof Consider

$$\begin{tikzcd}
\operatorname{Cor}\circ\operatorname{Res}\colon H^r(G,M) \arrow[r] \arrow[dr, "m\mapsto(g\mapsto gm)"'] & H^r(H,M) \arrow[r] & H^r(G,M) \\
& H^r(G,\operatorname{Ind}_H^G(M)) \arrow[u, "\sim"] \arrow[ur, "\phi\mapsto\sum_{s\in S} s\phi(s^{-1})"'] &
\end{tikzcd}$$

The composite is mercifully nice:

$$\begin{aligned} m \mapsto (\phi_m(g\mapsto gm)) &\mapsto \sum_{s\in S}\phi_m(s^{-1}) \\ &= \sum_{s\in S} ss^{-1}m = \sum_{s\in S} m = [G : H]m. \end{aligned}$$

245 Theorem (Inflation-Restriction Exact Sequence)
Let $H \trianglelefteq G$, M a G-module, $r > 0$. Assume that $H^i(H,M) = 0$ for all $0 < i < r$. Then

$$\begin{tikzcd}
0 \arrow[r] & H^r(G/H,M^H) \arrow[r, "\operatorname{Inf}"] & H^r(G,M) \arrow[r, "\operatorname{Res}"] & (H^r(H,M))^{G/H} \arrow[dll, "\operatorname{Trans}"] \\
& H^{r+1}(G/H,M^H) \arrow[r, "\operatorname{Inf}"] & H^{r+1}(G,M) &
\end{tikzcd}$$

is exact, where $\boxed{\text{Trans}}\colon H^r(H,M)^{G/H} \to H^{r+1}(G/H,M^H)$ *is the* $\boxed{\textit{trangression}}$ *map.*

Proof We will not define the transgression map, which is more involved to define than corestriction. So, we will only prove pieces. Let $r = 1$ and check exactness at $H^1(G,M)$. Let $\phi \in Z^1(G,M)$ be such that $\phi|_H \in B^1(G,M)$, i.e. $\phi(h) = hm_0 - m_0$ for some $m_0 \in M$ independent of h. Define $\phi'(g) := \phi(g) - (gm_0 - m_0)$, so $\phi(h) = 0$ for all $h \in H$. Further define $\widetilde{\phi}\colon G/H \to M^H$ by $\widetilde{\phi}(gH) := \phi'(g)$. This is well-defined using the cocycle condition.

List of Symbols

$B^r(G,M)$	r-coboundaries of G with coefficients in M, page 56
$C^r(G,M)$	r-cochains of G with coefficients in M, page 56
$D_{R/S}$	Relative discriminant, page 12
$D_{\mathfrak{q}/\mathfrak{p}}$	Decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$, page 16
G_w	Decomposition group of a valuation extension, page 47
$H^r(G,M)$	rth cohomology group of G with coefficients in M, page 54
$I \mid J$	I divides J, page 8
I^{-1}	Inverse Fractional Ideal, page 7
I_K	Set of fractional ideals of $\mathcal{O}_K$, page 22
$I_{\mathfrak{p}}$	Localization of a fractional ideal, page 10
I_w	Inertia group of a valuation extension, page 48
$I_{\mathfrak{q}/\mathfrak{p}}$	Inertia group of $\mathfrak{q}/\mathfrak{p}$, page 16
K	A number field, page 5
$N(I)$	Norm of an ideal, page 6
$N_{S/R}(\alpha)$	Norm of an element, page 3
P_K	Set of principal fractional ideals of $\mathcal{O}_K$, page 22
R_w	Ramification group of a valuation extension, page 48
R_w	ramification field, page 50
T_w	inertia field, page 50
$U^{(1)}$	Lifts of 1 in κ, page 40
$U^{(n)}$	Lifts of n in κ, page 41
$Z^r(G,M)$	r-cocycles of G with coefficients in M, page 56
Z_w	decomposition field, page 50
Cl_K	Class Group of K, page 22
Cor	Corestriction, page 58
$\mathrm{Disc}(\mathcal{O}_K)$	Discriminant of a Ring of Integers, page 5
$\mathrm{Disc}_{S/R}(\alpha_1,\ldots,\alpha_n)$	Discriminant of $\alpha_1,\ldots,\alpha_n$, page 3
$\mathrm{Disc}\, f(x)$	Polynomial discriminant, page 5
$\mathrm{Fr}(\mathfrak{q}/\mathfrak{p})$	Frobenius of $\mathfrak{q}/\mathfrak{p}$, page 18
$\mathrm{Ind}_H^G(N)$	Induced G-module, page 53
Inf	Inflation map, page 57
$\mathrm{NP}(f)$	Newton Polygon of f, page 42

$\Phi_n(x)$	nth cyclotomic polynomial, page 19
Res	Restriction map, page 57
$\mathrm{Tr}_{S/R}(\alpha)$	Trace of an element, page 3
Trans	Transgression map, page 59
$\mathbb{Q}(\zeta)/\mathbb{Q}$	Cyclotomic Field, page 19
$\mathbb{Q}_p$	p-adic field, page 32
$\mathbb{Z}_p$	p-adic integers, page 31
$\mathcal{O}$	An order, page 2
$\mathcal{O}_K$	Ring of integers of K, page 2
$\mathfrak{q}/\mathfrak{p}$	The prime $\mathfrak{q}$ lies over $\mathfrak{p}$, page 12
log	Log map, page 40
$\phi\colon K \to \mathbb{R}^n$	Embedding a number field in $\mathbb{R}^n$, page 23
d^r	rth cochain boundary map, page 56
$e_{\mathfrak{p}}$	Galois ramification index, page 16
$e_{\mathfrak{q}/\mathfrak{p}}$	Ramification index/degree of $\mathfrak{q}/\mathfrak{p}$, page 12
$f_{\mathfrak{p}}$	Galois interia degree, page 16
$f_{\mathfrak{q}/\mathfrak{p}}$	Inertia degree of $\mathfrak{q}/\mathfrak{p}$, page 12
r_1	Number of real embeddings, page 22
r_2	Number of pairs of complex embeddings, page 22
v_p	p-adic valuation, page 30

Index

R-order, 2
p-adic absolute value, 31
p-adic integers, 31
p-adic valuation, 30

absolute value, 32
archimidean, 34

class group, 22
coboundaries, 56
cochains, 56
cocycles, 56
cohomology group, 54
compatible homomorphisms, 57
conjugate embeddings, 45
continuous G-module, 52
corestriction, 58
crossed homomorphisms, 56
cyclotomic polynomial, 19

decomposition field, 50
decomposition group, 16, 47
Dedekind domain, 6
dimension shifting, 55
discrete subgroup, 26
discrete valuation, 36
discrete valuation ring (DVR), 9
discriminant, 3
discriminant of S, 3

enough injectives, 54
equivalant valuations, 36
equivalent absolute values, 33

factional ideal, 7

global field, 2

homomorphism of G-modules, 53

induced from H, 54
inert, 12
inertia degree, 12
inertia field, 50
inertia group, 16, 48
inflation map, 57
injective, 54
integral element, 3

lattice, 26
lies above, 11
local field, 32

maximal unramified subextension, 44

Newton polygon, 42
nonarchimidean, 34
norm, 3, 6
norm map, 56
normalized discrete valuation, 36
number field, 2

principal crossed homomorphisms, 56
principal fractional ideal, 7
profinite group, 51

ramification field, 50
ramification group, 48
ramification index/degree, 12
ramified, 12
regulator, 28
relative discriminant, 12
residue field, 36
restriction map, 57
ring of integers, 2

splits completely, 12
symmetric, 51

tamely ramified, 44
topological group, 51
trace, 3
trangression, 59
trivial absolute value, 33

uniformizer, 36
unramified, 12

valuation, 35
valuation ring, 36