# Mathematics 223a. Skeletal Notes for Basics of Algebraic Number Theory.

B. Mazur

September 29, 2008

**Introduction:** In the year-long course for graduate students (Math 223a,b) we will study local and global fields and their properties, the technology of adeles and ideles, global units, regulators, ideal class groups, Galois cohomology, Galois representations, local and global duality, Class Field Theory, duality, zeta-functions and $L$-functions and their related analytic number theory, and various concrete instances of all this theory.

*Algebraic Number Theory* as subject can be approached in various ways.

- For example, the focus might be what I will call *elementary and very classical* where the *algebraic numbers* themselves, one-by-one, are somewhat in the spotlight. For a *very* elementary exposition of this sort, see my draft entitled **algebraic numbers** available in pdf format on the section labeled *Provisional and not yet published* on my web-page:
  http://abel.math.harvard.edu/ mazur/
  (This will appear in the *Princeton Companion to Mathematics* edited by Tim Gowers.) Typical problems within this framework might be:

  1. Show that every finite abelian group is the Galois group of a Galois extension of $\mathbf{Q}$.
  2. For
  $$\mathbf{Q} \subset L = \mathbf{Q}(\zeta_7 + \zeta_7^{-1}) \subset \mathbf{Q}(\zeta_7)$$
  show that $L$ is the splitting field of the polynomial $X^3 + X^2 - 2X - 1$ over $\mathbf{Q}$.
  3. Find a polynomial for which the cubic subfield of $\mathbf{Q}(\zeta_{13})$ is a splitting field over $\mathbf{Q}$.

  and we will be assuming that students enrolled in this course will have the background for, and will be able to do, these problems easily.

  Of course, we will be assuming basic Galois Theory and some familiarity with algebraic integers, and if you have any doubts about whether your background in this regard is sufficient for the course, if you can work out the following exercises from **[F-T]**, then you are OK for that:

  – Exercises 1,3,4, 5, 9,10 for Chapter I (pp. 335-336) noting the typo in Exercise 1,

– Exercises 1,2,4 for Chapter II (pp. 336-337).

- Or, the focus might be what might be called more or less *algebraic geometric* where the objects of study are global and local fields, Dedekind domains, discrete valuation rings and their completions, finite extensions of Dedekind domains with particular attention paid to the fine structure of ramification, and of prime splitting, units, regulators, locally trivial modules, ideal class groups, adele, ideles, and idele class groups. This will, in fact, be one of our foci and for this it will be assumed that students have had at least some brief exposure to standard commutative algebra. In particular, we will only be *recalling* rather than *explaining for the first time* the notion of Spec$A$ for $A$ a commutative ring, of localization $S^{-1}A$ for $S$ a multiplicative system of elements of $A$, of *noetherian rings,* and *integral closure.*

- Or, the focus might be what might be called *analytic algebraic number theory* where one of the problems we will eventually treat is the following type of question. Let $f(X) \in \mathrm{Z}[X]$ be a monic irreducible polynomial of degree $n$. for each prime number $p$ consider the *partition of* $n$, $part_f(p) : n = \sum n_i$ defined by letting $\bar{f}(X) \in \mathrm{Z}/p\mathrm{Z}[X]$ be $f(X)$ reduced mod $p$, and factoring $\bar{f}(X)$ into a product of irreducibles,

$$\bar{f}(X) = \prod_i \bar{f}_i(X) \in \mathrm{Z}/p\mathrm{Z}[X],$$

  and putting $n_i :=$ degree $\bar{f}_i(X)$. The question, then, is to say everything one can say about the statistical distribution

$$p \mapsto part_f(p)).$$

  [E.g., think about this for $f(X) = X^2 - 5$.] We will devote some time to this in our course.

- Or, the focus might be on the structure of the Galois groups in question; for example, the *global Galois groups*: $G_{\mathrm{Q}} := \mathrm{Gal}(\bar{\mathrm{Q}}/\mathrm{Q})$, the Galois group of an algebraic closure of Q, or the more refined quotients of $G_{\mathrm{Q}}$ that take local behavior into account, as in $G_{\mathrm{Q},S} :=$ the Galois group of the maximal subextension in $\bar{\mathrm{Q}}$ that is unramified outside the set $S$ of places of Q. These topological groups pack an enormous amount of information about our subject, and we will try to understand them in various ways, e.g. cohomological. Even the local analogues of these Galois groups have a deep structure, and we can't yet claim to have a fully satisfactory, and exhaustive, understanding of them. But we do have local and global class field theory. We will devote lots of time to this in our course.

What follows are skeletal notes to the introductory lectures.

# Contents

**1 Spectra and Localization.** **4**

**2 Discrete Valuation Rings.** **5**

2.1 The mechanics of valuations. . . . . 6

2.2 Examples . . . . . 7

2.3 Non-examples . . . . . 7

2.4 Discrete Valuation Rings and Integral Closure. . . . . 8

2.5 Examples from algebraic geometry . . . . . 10

**3 Dedekind Domains.** **10**

3.1 Rings of integers in number fields, and function field analogues. . . . . 11

3.2 The group of fractional ideals in a Dedekind domain . . . . . 13

3.3 The full formalism of the norm . . . . . 15

3.4 Extensions of Dedekind domains. . . . . 16

3.5 Decomposition of primes in an extension . . . . . 16

3.6 Monogenic extensions . . . . . 17

3.7 Examples . . . . . 18

3.8 Monogenicity of finite extensions of discrete valuations rings with separable residual field extensions . . . . . 19

**4 Local Fields** **19**

4.1 Normalized Absolute Values . . . . . 19

4.2 The category of profinite groups . . . . . 20

4.3 Completion and topologies of fields . . . . . 24

4.4 Unramified extensions of Local Fields . . . . . 25

4.5 Tamely ramified extensions . . . . . 26

**5 Adeles and Ideles** **26**

**6 The Ideal Class Group and the Dirichlet Unit theorem** **27**

6.1 Sketch of some elements that enter into the proof of the finiteness of the ideal class group and the Dirichlet Unit Theorem. . . . . 27

6.2 On the finiteness of the ideal class group . . . . . 27

6.3 Comments on the Dirichlet Unit Theorem. . . . . 29

**7 Comments on Function fields** **30**

# 1 Spectra and Localization.

Rings, unless otherwise signaled, will be commutative rings with unit element, and homomorphism of rings will be assumed to preserve the unit element. If $A$ is a ring, Spec $A$, its *spectrum* is—as a set—the set of prime ideals of $A$. If $f : A \to B$ is a ring-homomorphism, the pullback, i.e., full inverse image, of any prime ideal of $B$ under the homomorphism $f$ is a prime ideal of $A$. This gives us a map on spectra Spec$B \to$ Spec$A$ that we will denote by Spec$(f)$ (or, sometimes, by just $f$ again) allowing us to consider Spec as a contravariant functor from the category of commutative rings to the category of sets. If $f : A \to B$ is a *surjective* ring-homomorphism, then

$$\mathrm{Spec}(f) : \mathrm{Spec}B \to \mathrm{Spec}A$$

is an injection.

Define the Zariski topology on spectra as follows: If $A$ is a ring, the open sets on Spec$A$ is given by the complements of the injective mappings Spec$(\phi)$ : Spec$B \to$ Spec$A$ where $\phi$ runs through all surjective ring-homomorphisms with domain $A$. A base for the open sets is given by the images of the mappings Spec$(S_f^{-1}A) \to$ Spec$A$ for $f \in A$, where $S_f = \{1, f, f^2, \ldots\}$ is the multiplicative set generated by $f$.

Any homomorphism $f$ of rings induces a *continuous map* Spec$f$ of spectra.

If $A$ is a ring, and $S \subset A$ is a subset containing the identity element of $A$ and closed under multiplication, the localization of $A$ with respect to $S$ is a ring with homomorphism from $A$, $\iota_S : A \to S^{-1}A$ to a ring (denoted $S^{-1}A$) where the image of elements of $S$ are all units in the ring $S^{-1}A$, and moreover, $A \to S^{-1}A$ is universal with respect to the problem of inverting $S$, i.e., for

any ring-homomorphism $j : A \to A'$ where the image of elements of $S$ are all units in the ring $A'$, there is a unique homomorphism $h : S^{-1}A \to A'$ such that $j = h \cdot \iota_S$.

This operation is indeed a *localization* operation for on the level of spectra we have that the map induced by $\iota_S$, i.e.,

$$\mathrm{Spec}(\iota_S) : \mathrm{Spec}S^{-1}A \to \mathrm{Spec}A$$

is injective, and its image is the complement of

$$\{P \in \mathrm{Spec}A \mid P \cap S \neq \text{the empty set}\}.$$

Here are some important special cases of localization:

- Let $A$ be an integral domain, and suppose that the multiplicative system $S \subset A$ doesn't contain $0 \in A$. In this case, if $K$ is the field of fractions of $A$ ($K$ being the localization of $A$ relative to the multiplicative system $A - \{0\}$), then
$$S^{-1}A = \{a/s \in K \mid a \in A, s \in S\};$$
- Suppose $S$, as a multiplicative system, is generated by finitely many elements $f_1, f_2, \ldots, f_m$ of $A$. In this case put $f = \prod_i f_i$ and you can take $S^{-1}A$ to be the ring $A[1/f] = A[X]/(fX - 1)$ with $A \to S^{-1}$ the natural homomorphism $A \to A[1/f]$. Denoting $X := \mathrm{Spec}A$ and $X_f := \mathrm{Spec}S^{-1}A$ we have that $X_f \subset X$ is the open subset consisting of of the complement of all primes $P$ in $A$ that contain the element $f$; visually: "the complement of the locus of zeroes of $f$."
- For a prime ideal $P \subset A$ take $S = A - P$. Then we usually denote $S^{-1}A$ as $A_P$ (*the localization of $A$ at $P$*). We have that $A_P$ is a local ring, with maximal ideal equal to $PA_P \subset A_P$, and with residue field $A_P/PA_P =$ the field of fractions of the integral domain $A/P$. The set of prime ideals of $A_P$ pull back to the set of prime ideals of $A$ contained in $P$.

## 2 Discrete Valuation Rings.

A ring is a **DVR** if it is a principal ideal domain and has precisely one nonzero prime ideal. If $A$ is a DVR then its nonzero prime ideal, $m(A) \subset A$ is visibly its only maximal ideal; so $A$ is a local ring, and $A/m(A)$ is its residue field. Any element not contained in $m(A)$ is a unit in $A$; i.e., $A^* = A - m(A)$. Any generator $z$ of the ideal $m(A)$ is called a *uniformizer*, the uniformizers being the *irreducible* elements of $A$. Fix a uniformizer $z$. For any nonzero element $\alpha \in A$ there is a maximal integer ($\geq 0$) $n$ such that $\alpha$ is divisible by $z^n$ in $A$, and for such an $n$ we have that $\alpha = uz^n$ for a unit $u \in A^*$ (proof: $A$ is a PID so a UFD and has only one irreducible element up to multiplication by a unit, namely $z$). Call $n$ the *order* or the *valuation,* $v(\alpha)$, of $\alpha$. If $K$ is the field of fractions of the DVR $A$, then any nonzero element $\phi$ of $K$ can be written uniquely as $uz^m$ for $m \in \mathrm{Z}$ and for $u \in A^*$, where, again, $v(\phi) \in \mathrm{Z}$ is called the valuation of $\phi$. We have an exact sequence

$$0 \to A^* \to K^* \to \mathrm{Z} \to 0$$

independent of the choice of uniformizer where the surjective homomorphism $K^* \to \mathrm{Z}$ is the valuation.

## 2.1 The mechanics of valuations.

Let $A$ be a DVR, with $K$ its field of fractions, and $m \subset A$ its maximal ideal. For reasons that should be evident, we convene that the *valuation* of the zero element is $\infty$. The rules that the valuation $v : K \to \mathrm{Z} \cup \{\infty\}$ satisfy are the following:

1. $v(x) = \infty \iff x = 0$
2. $v(x \cdot y) = v(x) + v(y)$
3. $v(x_1 + x_2 + \ldots + x_s) \geq \min\{v(x_1), v(x_2), \ldots, v(x_s)\}$ with equality if there is a unique summand $x_j$ $(1 \leq j \leq s)$ achieving the above minimal valuation.

**Definition 1** *If $K$ is a field, and $v : K \to \mathrm{Z} \cup \{\infty\}$ is a valuation on $K$ i.e., a mapping satisfying the above three conditions, assumed to be surjective, then we call $(K, v)$ a* **nonarchimedean valued** *field.*

Given a valued field as above, by definition its *ring of integers* $A_v \subset K$ is the subset of elements with nonnegative valuation; this is indeed a subring of $K$ by properties (1),(2), (3) above. Moreover, $A_v$ is a DVR and any element of valuation 1 is a uniformizer.

If, as usual, one replaces this "logarithmic" type function $v$ by exponentiating with respect to some chosen *base* (i.e., real number $c > 1$) to obtain a multiplicative absolute value,

$$|x|_c := c^{-v(x)}$$

we have the corresponding laws:

1. $|x|_c = 0 \iff x = 0$
2. $|x \cdot y|_c = |x|_c \cdot |y|_c$
3. $|x_1 + x_2 + \ldots + x_s|_c \leq \max\{|x_1|_c, |x_2|_c, \ldots, |x_n|_c\}$ with equality if there is a unique summand $x_j$ $(1 \leq j \leq s)$ achieving the above maximal absolute value.

We may view $|\ |_c$ as giving us a metric on $K$, and the underlying topology of this metric is independent of the choice of *base* $c$. The last of the three rules is an ultrametric version of the classical triangle inequality for this metric. As we shall see, there is a particularly good choice of base, in the algebraic number theoretic set-up.

## 2.2 Examples

- **Power series rings in one variable over a field.** The simplest example of a DVR is the ring of power series $A := k[[z]]$ in one variable $z$ over a field $k$. The field $k$ is the residue field, the maximal ideal of our DVR is then the set of multiples of $z$, and the valuation of a nonzero power series is given by the "order of zero at the origin" of the power series. The group of units is the group of power series with nonzero constant term, i.e., of valuation 0. The field of fractions is $K := k((z)) = \cup_{\nu \geq 0} z^{-\nu} k[[z]]$, the field of "finite-tailed" Laurent series in $z$ with coefficients in $k$.

  **Exercise 1** *Let $k$ be a field, $k[t]$ the ring of polynomials in the variable $t$ with coefficients in $k$ and $k(t)$ the fraction field of $k[t]$, i.e., the field of rational functions over $k$ in the variable $t$. If $m \subset k[t]$ is a nonzero maximal ideal, define the valuation $v = v_m : k(t)^* \to \mathrm{Z}$ as usual; i.e., if $\pi(t) \in m \subset k[t]$ is a generator, write $f = \pi(t)^\nu \times \text{unit}$ and put $v(f) = \nu$. Let $k(t)_v$ be the completion of $k(t)$ with respect to the valuation $v$.*

  1. *If $\pi(t) = t - \alpha$ for $\alpha \in k$ show that*

     $$k(t)_v \simeq k((z))$$

     *via an isomorphism that sends $t$ to $z + \alpha$.*
  2. *Think about $k(t)_v$ when $\pi(t)$ is an irreducible polynomial in $k[t]$ of degree $> 1$. For example, $k = \mathbf{R}$ and $\pi(t) = t^2 + 1$.*

  **The $p$-adic integers.** Let $A := \mathrm{Z}_p := \lim_{n \geq 0} \mathrm{Z}/p^n\mathrm{Z}$ which is a PID with field of fractions $K := \mathrm{Q}_p = \mathrm{Z}_p[1/p]$ the *field of $p$-adic numbers.*

  The ring Z is naturally a "dense" subring of $\mathrm{Z}_p$, and the prime number $p$ itself, is uniformizer: $p \in \mathrm{Z} \subset \mathrm{Z}_p$. The group of units $\mathrm{Z}_p^* \subset \mathrm{Z}_p$ consist of the $p$-adic integers that are not congruent to zero modulo $p$. Any nonzero $p$-adic number $z \in \mathrm{Z}_p$ can be written as $z = p^\nu u$ where $u$ is a $p$-adic unit, and the rule $z \mapsto v(z) := \nu \geq 0$ defines the valuation on $\mathrm{Z}_p$, $v : \mathrm{Z}_p^* \to \mathrm{Z}^{\geq 0}$, rendering $\mathrm{Z}_p$ a DVR; the natural extension of this valuation to the field of fractions, $v : \mathrm{Q}_p^* \to \mathrm{Z}$, gives $\mathrm{Q}_p$ the structure of complete valued field.

  **Exercise 2** *Let $\bar{\mathrm{Q}}_p$ be an algebraic closure of $\mathrm{Q}_p$ and let $\bar{\mathrm{Z}}_p$ be the integral closure of $\mathrm{Z}_p$ in $\bar{\mathrm{Q}}_p$.*

  1. *Show that $\bar{\mathrm{Z}}_p$ is in fact integrally closed, and has exactly one nonzero prime ideal, which is therefore maximal.*
  2. *Show that $\bar{\mathrm{Z}}_p$ is non-noetherian by proving that the maximal ideal is not finitely generated.*

## 2.3 Non-examples

- **A plane cusp.** Consider $k$ a field and put $A = k[[x, y]]/(y^2 - x^3)$ where $k[[x, y]]$ is the ring of power series in the two independent variables $x$ and $y$ and $(y^2 - x^3)$ is the ideal you think it is. Here $A$ is a domain; it is a local, noetherian ring as well, and has precisely one nonzero prime ideal; the problem is that it isn't a PID for (for example) its maximal ideal $(x, y) \subset A$ is not generable by a single element. How to remedy this? The ring $A$ is *not* integrally closed

in its fraction field, but we can view its fraction field $K$ as the field of ("finite-tailed") Laurent series over $k$ a variable $t$ where we think of $t$ itself as $t = \frac{y}{x}$ identifying

$$x = x\frac{y^2}{x^3} = \frac{y^2}{x^2} = t^2,$$

and

$$y = y\frac{y^2}{x^3} = \frac{y^3}{x^3} = t^3.$$

Explicitly, then, we have that our $A$ can be identified with the subring of $B := k[[t]]$ generated by power series in two variables $x = t^2$ and $y = t^3$, and both $A$ and $B$ share the same field of fractions $K = k((t))$. Since the element $t \in B \subset K$ satisfies the integral polynomial equation over $A$,

$$t^2 - x,$$

(also $t^3 - y$) we have that $B$ is an integral extension of $A$ and clearly is also *the* integral closure of $A$ (in its fraction field). The ring $B$ itself is a DVR, and this will set the pattern, as we will shortly see.

- **Euler's "mistake."** Consider the ring $A := \mathrm{Z}_2[\sqrt{-3}] \subset K := \mathrm{Q}_2[\sqrt{-3}]$ where, again, $A$ is a domain; it is a local, noetherian ring as well, and has precisely one nonzero prime ideal. The maximal ideal is generated by two elements (e.g., $(2, 1-\sqrt{-3})$) but not by any single element, and its residue field is $\mathbf{F}_2$. The integral closure, though, of $A$ in $K$ is given by $B := \mathrm{Z}_2[\frac{1-\sqrt{-3}}{2}]$ (noting that $\frac{1-\sqrt{-3}}{2}$ satisfies the integral relation $X^3 - 1 = 0$) which is a DVR (it has a unique nonzero prime ideal (2) and is a PID). Its residue field is $\mathbf{F}_4$.

- **A 2-adic version of a plane cusp.** Consider the ring $A := \mathrm{Z}_2[2\sqrt{2}] \subset K := \mathrm{Q}_2[\sqrt{2}]$ where, again, $A$ is a domain; it is a local, noetherian, and has precisely one nonzero prime ideal $(2, 2\sqrt{2})$. Call $x = 2; y = 2\sqrt{2}$ and note that $y^2 - x^3 = 0$ and you see why I want to call this a 2-*adic version of a plane cusp.* Analogously, the integral closure of $A$ (in its field of fractions $K$) is $B := \mathrm{Z}_2[y/x] = \mathrm{Z}_2[\sqrt{2}]$ which is a PID, its maximal ideal being generated by $\sqrt{2}$.

## 2.4 Discrete Valuation Rings and Integral Closure.

After the above, it should be less of a surprise that we have the following ([A-M] Proposition 9.2)

**Theorem 1** *If $A$ is a noetherian local integral domain of Krull dimension one ((i.e. having no prime ideals except $(0) \neq m$), with $K$ its field of fractions, $m \subset A$ its maximal ideal, and $k = A/m$ its residue field, the following properties are equivalent.*

1. *There is a valuation $v : K \to \mathrm{Z} \cup \{\infty\}$ such that $A_v$, the set of elements in $K$ of valuation $\geq 0$, is equal to $A \subset K$.*
2. *The ring $A$ integrally closed (meaning: in its field of fractions).*

3. *The ideal $m$ is principal.*
4. *The $k$-vector space $m/m^2$ is of dimension one.*
5. *Every nonzero ideal of $A$ is a power of $m$.*
6. *There is a nonzero element $x \in A$ such that every nonzero ideal of $A$ is generated by some power of $x$.*
7. *The ring $A$ is a DVR.*

**Proof:** We will be using a bit of commutative algebra for this. But first (1) implies (2) because if $x \in K$ but not in $A$ is integral over $A$, then since it has a negative valuation, the ultrametric inequality will rule out that it can satisfy an integral relation over $A$; i.e., if we have

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

the leading term, $x^n$ has strictly lower valuation than any of the others on the RHS of this equation, making it impossible for the LHS to be 0.

To see that (2) implies (3) we will go fishing for a generator of the ideal $m$. Start modestly by choosing *any* $a \in m$ such that $a \neq 0$. Then the principal ideal generated by $a$ must be sandwiched between $m$ and some (finite) power of $m$:

$$m^\nu \subset (a) \subset m$$

for, $m$ is the only nonzero prime ideal of $A$ so the radical of $(a)$ is $m$ and since $A$ is noetherian $(a)$ contains a power of its radical. Let $m^\nu$ be the minimal power of $m$ for which this is true, and find some element $b \in m^{\nu-1}$ (convention: $m^0 = A$) not in $(a)$. We want to show that $x = a/b$ is a generator of $m$, by noting, first, that $x^{-1} \notin A$ by construction, and therefore $x^{-1}$ is *not* integral over $A$ by our hypothesis (2). We also have, by construction, that $x^{-1}m \in A$, giving two possibilities: either

- $x^{-1}m = A$, or
- $x^{-1}m \subset m \subset A$

The first of these possibilities will give us that, indeed, $x$ is a generator of $m$ and we would be done; the second of these possibilities would give us an integral relation that $x^{-1}$ satisfies over $A$.

To see that (3) implies (4): (3) already implies that $\dim_k m/m^2 \leq 1$ but if $\dim_k m/m^2 = 0$, i.e., $m = m^2$, then an application of Nakayama's Lemma would give us that $m = 0$, which it is not. Another application of Nakayama's Lemma shows that (4) implies (3).

**Exercise 3**

$$(4) \Rightarrow (5) \Rightarrow (6) \Rightarrow (7) \Rightarrow (1).$$

### 2.5 Examples from algebraic geometry

Let $A$ be a noetherian integrally closed integral domain. Let $P \subset A$ be a minimal prime ideal, meaning that the only prime ideals contained in $P$ are the ones that have to be there, namely $P$ and (0). Then $A_P$, the localization of $A$ at $P$ is of Krull dimension one, and is an integrally closed noetherian local integral domain, hence a DVR by the above theorem. If $A = k[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)$ is the coordinate ring of a (normal) algebraic variety $V$ (so, $V$ is "the locus of zeroes of $f_1, f_2, \ldots, f_m$") then any irreducible subvariety $W \subset V$ of codimension one is cut out by a minimal prime ideal $P = P_W$, and the valuation on the field of fractions of the DVR $A_{P_W}$ just records the order of zero or pole of a rational function along $W$.

*Remark (John Tate):* In a local noetherian domain $A$ of Krull dimension 1, the function

$$f \mapsto \text{length}(A/fA)$$

on $A - \{0\}$ is the valuation if $A$ is a DVR and otherwise is the sum of the valuations of $f$ at the localizations of the integral closure of $A$ at its maximal ideals, if that integral closure is finite over $A$ as it is in the case of an affine variety $V$ as above.

## 3 Dedekind Domains.

Let $A$ be a noetherian integral domain of dimension one. The basic facts of life are as follows.

- Every nonzero ideal of $A$ can be expressed uniquely as a product of primary ideals with distinct radicals.
- $A$ is integrally closed if and only if the localization $A_P$ of $A$ at every nonzero prime ideal $P$ is integrally closed.

**Theorem/Definition 1** *A noetherian integral domain of dimension one $A$ is called a* **Dedekind Domain** *if, equivalently*

- *$A$ is integrally closed,*
- *the localization $A_P$ of $A$ at every nonzero prime ideal $P$ is integrally closed,*
- *the localization $A_P$ of $A$ at every nonzero prime ideal $P$ is a DVR,*
- *every prime ideal in $A$ is "locally principal."*

  *(" Locally principal" means that there is an element $\alpha \in P$ that is, in fact, a generator of the ideal $P \cdot A_P \subset A_P$.)*

**Theorem 2** *Every nonzero ideal of a Dedekind domain $A$ can be written uniquely as a product of powers of nonzero prime ideals.*

**Note:** So, another way of thinking about the condition of "local principal-ness" of a prime ideal $P$ in a Dedekind Domain $A$ is that there is an element $\alpha \in P$ such that there is an ideal $J \subset A$ with

- $(\alpha) = P \cdot J$, and
- $P$ doesn't divide $T$.

**Definition 2** *Let $A$ be a Dedekind domain, and $K$ its field of fractions. A* **fractional ideal** *of $A$ is a nontrivial, finitely generated, $A$-submodule of $K$, $J \subset K$.*

The Homework Set due September 25 is devoted to proving the basic facts of life about products and invertibility of fractional ideals. Any fractional ideal may be written uniquely as a product:

$$J = \prod_{i=1}^{s} P_i^{e_i}$$

where the $P_i$ are prime ideals in $A$ and the $e_i \in \mathrm{Z}$. We sometimes refer to the exponent $e_i$ as the *valuation* of $J$ at the prime ideal $P_i$, and denote it $v(P_i)$ so that we can also write

$$J = \prod_{P} P^{v(P)}.$$

### 3.1 Rings of integers in number fields, and function field analogues.

Let $K/\mathrm{Q}$ be a number field, which for us will mean an extension field of Q of finite degree. We have, by the *primitive element theorem* the fact that there exists an element $\Theta$ that generates $K$ over Q, so that we may write $K = \mathrm{Q}[X]/f(X)$ where $f$ is a monic irreducible polynomial having $\Theta$ as a root. There are, of course, many such $\Theta$'s, in fact, and we can (by multiplying $\Theta$ by a suitable non-zero rational integer) guarantee that the primitive element $\Theta$ is an algebraic integer, i.e., is integral over Z, or equivalently, that the monic polynomial $f$ alluded to above has rational integer coefficients.

Other than the fact that $K$ is a *field* rather than merely a finite dimensional vector space over Q, the essential structure that the vector space $K$ carries is a nondegenerate bilinear symmetric (quadratic) form

$$\langle x, y \rangle := \mathrm{Trace}_{K/\mathrm{Q}}(xy)$$

(nondegenerate because $K/\mathrm{Q}$ is a separable extension). Call this the *trace pairing.* If $\Lambda \subset K$ is a Z-submodule let $\Lambda^\sharp \subset K$ denote the submodule of elements $y \in K$ such that $\langle x, y \rangle \in \mathrm{Z}$ for all $x \in \Lambda$. Note that if $\Lambda \subset K$ is actually a lattice in the Q-vector space $K$ generated by basis elements $\lambda_1, \lambda_2, \ldots, \lambda_d \in K$ then $\Lambda^\sharp \subset K$ is also a lattice in the Q-vector space $K$ generated by the dual basis $\lambda_1^\sharp, \lambda_2^\sharp, \ldots, \lambda_d^\sharp \in K$, where *dual* of course means with respect to the trace pairing.

Let $A \subset K$ denote the ring of elements that are integral over $\mathrm{Z} \subset \mathrm{Q}$, Note that since $\langle\ ,\ \rangle : A \times A \to \mathrm{Z} \subset \mathrm{Q}$ we have that—viewing $A$ as *lattice* in $K$, $A \subset A^\sharp$.

**Theorem 3** *The ring $A$ is a Dedekind domain.*

**Proof:** Choosing a primitive element $\Theta \in K$ that is integral over Z, we have that $\mathrm{Z}[\Theta] \subset A$. Comparing with the dual lattices relative to the trace pairing, we have the following string of inclusions

$$\mathrm{Z}[\Theta] \subset A \subset A^\sharp \subset \mathrm{Z}[\Theta]^\sharp$$

and since $\mathrm{Z}[\Theta]$ is a lattice, its dual, $\mathrm{Z}[\Theta]^\sharp$ is again a lattice, and therefore $A$ itself is a lattice, is finitely generated as a Z-module, hence noetherian. $A$ is of dimension one because if there were a string of prime ideals $(0) \subset P' \subset P$ in $A$ with $P'$ nonzero, a simple argument shows that $P' \cap \mathrm{Z} = P \cap Z = (p) \subset \mathrm{Z}$ for some prime $p$, and therefore $A' = A/P'$ is an integral domain of finite cardinality, hence a field; from this we see that $P' = P$. The integral domain $A$, then, is noetherian, dimension one, and integrally closed; hence: a Dedekind domain.

**Exercise 4** *How would you modify the above discussion to obtain examples of Dedekind domains whose fields of fractions are of transcendence degree one over finite fields, and finitely generated (as fields)?*

**Exercise 5 The ring of integers is quadratic number fields** *If $K/\mathrm{Q}$ is of degree two, $K$ can be written as $\mathrm{Q}(\sqrt{d})$ where $d \in \mathrm{Z}$ is a square-free integer, Here we can take $\Theta$ to be $(\sqrt{d} \in K$. What is $\mathrm{Z}[\Theta]^\sharp \subset K$? Show that if $T_{K/\mathrm{Q}} : K \to \mathrm{Q}$ is the trace and $N_{K/\mathrm{Q}} : K^* \to \mathrm{Q}^*$ the norm, then an element $\alpha \in K$ is integral over Z if and only if $T_{K/\mathrm{Q}}(\alpha)$ and $N_{K/\mathrm{Q}}(\alpha)$ are in Z. Show that the ring of integers in $K$ is generated by $\sqrt{d}$ over Z when $d$ is not congruent to 1 modulo 4 and by $\frac{1+\sqrt{d}}{2}$ if $d$ is congruent to 1 modulo 4.*

**Note:** Let $c$ be an integer, and let $K(c)$ be the degree three field over Q possessing a root $\Theta = \Theta(c) \in K(c)$ of the polynomial $x^3 + x + c$; i.e. $K(c) = \mathrm{Q}[x]/(x^3 + x + c) = \mathrm{Q}(\Theta(c))$. Let $A(c) \subset K(c)$ denote the ring of integers in $K(c)$. So

$$\mathrm{Z}[\Theta(c)] \subset A(c) \subset K(c).$$

A session with gp/PARI computes that, for the values of $a$ between 1 and 22, ignoring the few values of $a$ where the polynomial is not irreducible, we have that $\mathrm{Z}[\Theta(c)] = A(c)$ except for the five values $c = 6, 14, 18, 19, 22$ where the indices of $\mathrm{Z}[\Theta(c)]$ in $A(c)$ are, respectively, $2, 4, 4, 7, 2$, and the Z basis of $A(c)$ is given in the table below.

$$
\begin{array}{lccc}
\mathbf{6}: & 1, & \Theta, & \frac{\Theta^2-\Theta}{2} \\
\mathbf{14}: & 1, & \frac{\Theta^2+\Theta+2}{4}, & \frac{-\Theta^2+3\Theta-2}{4} \\
\mathbf{18}: & 1, & \Theta, & \frac{\Theta^2-\Theta+2}{4} \\
\mathbf{19}: & 1, & \frac{\Theta^2+3\Theta+3}{7}, & \frac{-\Theta^2+4\Theta-3}{7} \\
\mathbf{22}: & 1, & \Theta, & \frac{-\Theta^2-\Theta}{2}
\end{array}
$$

## 3.2 The group of fractional ideals in a Dedekind domain

If $A$ is a Dedekind domain, any (nonzero) fractional ideal $I \subset K$ is uniquely expressible as a (finite) product of powers of prime ideals,

$$I = \prod_P P^{v_p(I)},$$

for $v(P) \in Z$ (and all but finitely many of these exponents $v(P)$ vanishing). Writing

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

by the first Homework set (Problems 1-6 of "Homework due September 25") we have that

$$I \cdot I^{-1} = (1) = A;$$

in other words every fractional ideal is *invertible*. it follows that

$$I^{-1} = \prod_P P^{-v_p(I)}.$$

**Definition 3** *The* **group of fractional ideals of a Dedekind domain** $A$*, denoted* $\mathcal{I}(A)$*, is defined by . The underlying set is the set of of fractional ideals of* $A$*, and the multiplication law is product of ideals. The subgroup of* **principal factional ideals**, $\mathcal{P}(A) \subset \mathcal{I}(A)$ *is also what you think; namely the fractional ideals of the form* $x \cdot A \subset K$ *for some element* $x \in K^*$*. The* **ideal class group**, $\mathcal{H}(A)$*, of* $A$ *is the quotient group, so that*

$$0 \to \mathcal{P}(A) \to \mathcal{I}(A) \to \mathcal{H}(A) \to 0$$

*is an exact sequence. We also have the exact sequence*

$$0 \to A^* \to K^* \to \mathcal{P}(A) \to 0$$

*and we can splice these together to get the exact sequence,*

$$0 \to A^* \to K^* \to \mathcal{I}(A) \to \mathcal{H}(A) \to 0,$$

*which will play a leading role in some of the cohomological issues that will eventually come up.*

The identity of this group $\mathcal{I}(A)$ is the unit ideal, i.e., $(1) = A$, and since multiplication of ideals is clearly associative, the main fact that we are using is that all fractional ideals are invertible.

Clearly $\mathcal{I}(A)$ is a free abelian group generated by the nonzero prime ideals of $A$. The Dedekind domain $A$ is a PID if and only if $\mathcal{P}(A) = \mathcal{I}(A)$ if and only if $\mathcal{H}(A)$ is trivial. So, $\mathcal{H}(A)$ is (in a sense) a way of measuring of how $A$ fails to be a PID.

**Main Examples 1**

- **(Global)** *$A = \mathrm{Z}$, and $A = k[t]$ where $k$ is a finite field. And, of course, rings obtained as finite (flat) extensions of these, or localizations of those.*
- **(Local)** *$A = \mathrm{Z}_p$ for $p$ a prime number, and $A = k[[t]]$ where $k$ is a finite field. And, of course, rings obtained as finite (flat) extensions of these.*

For $A = \mathrm{Z}$ the situation is very clear: we have (since Z is a PID with group of units $\{\pm 1\}$) the group of fractional ideals $\mathcal{I}$ is canonically isomorphic to $\oplus_p \mathrm{Z}$ where the subscript $p = 2, 3, 5, 7, 11, \ldots$ runs through all prime numbers, and $\oplus_p \mathrm{Z}$ just means the direct sum of copies of the additive group Z indexed by these $p$'s. The long sequence above boils down to:

$$0 \to \{\pm 1\} \to \mathrm{Q}^* \to \oplus_p \mathrm{Z} \to 0 \to 0.$$

If $I \subset \mathrm{Z}$ is a (nonzero) ideal, rather than a general fractional ideal, we define the *norm* of $I$ to be

$$N(I) := \#(\mathrm{Z}/I) = \prod p^{v_p(I)},$$

or—equivalently—the smallest positive integer contained in $I$. We extend this, multiplicatively, to obtain an isomorphism of groups $N : \mathcal{I}(\mathrm{Z}) \cong \mathrm{Q}_{>0}$.

We extend this description to the following situations.

- Let $K/\mathrm{Q}$ be a number field and $A \subset K$ be the ring of algebraic integers in $K$; that is, the integral closure of Z in $K$. Let $N = N_{K/\mathrm{Q}} : K \to \mathrm{Q}$ denote the "classical" norm mapping (obtained in any of the equivalent standard ways we know, e.g., N(x) is the absolute value of the determinant of the endomorphism "multiplication by $x$" on the Q-vector space $K$ and, in case $x$ lies in $A$ it is also $\#(A/xA)$). For any (non)-fractional (nonzero) ideal $I \subset A$ let $I = \prod_P P^{v_P(I)}$ be its decomposition into a product of prime ideals, and define:

  $$N(I) := \#(A/IA) = \prod_P \#(A/PA)^{v_P(I)} = \prod_P N(P)^{v_P(I)},$$

  extending it multiplicatively to obtain a homomorphism,

  $$N = N_{K/\mathrm{Q}} : \mathcal{I}(A) \to \mathrm{Q}_{>0}.$$

  This homomorphism is, of course. determined by its values on the prime ideals $P$. This is what we will generally be working with.

- Let $K/\mathrm{Q}$ be a number field and $A \subset K$ the localization of the ring of algebraic integers in $K$ relative to a multiplicative system $S$ (not containing zero, of course). We can define—exactly as above—a norm homomorphism on fractional ideals. Of course, one has to be careful when one makes the comparison between this norm homomorphism for different multiplicative systems.
- When $A = k[t]$ with $k$ a finite field, the prime ideals $P \subset k[t]$ and any such $P$ is generated by a unique irreducible (monic) polynomials $f_P(t) \in k[t]$; following the format of the items above, we can define:

  $$N(P) = \#(k[t]/P) = \#(k)^{\mathrm{degree(f_P)}} = \ell^{\nu \mathrm{degree(f_P)}},$$

where $k$ has cardinality $\ell^\nu$. Extending multiplicatively, we get a homomorphism:

$$N : \mathcal{I}(k[t]) \to \ell^{\nu \mathrm{Z}} \subset \mathrm{Q}_{>0}.$$

Given a nonzero rational function $f(t) \in K := k(t)$ its norm is determined by its valuation at its zeroes and poles, i.e., at the zeroes $z_1, z_2, \ldots, z_n$ of $f(t)$ in $\bar{k}$ and by the zeroes $y_1, y_2, \ldots, y_m$ of $1/f(t)$ in $\bar{k}$. Putting $q = \#(k) = \ell^\nu$, and writing

$$f(t) = c \cdot \frac{\prod_{i=1}^n (t - z_i)^{v(z_i)}}{\prod_{j=1}^m (t - y_j)^{v(y_j)}}$$

we have

$$N(f) = q^{\sum_i v(z_i) - \sum_j v(y_j)} = q^{\text{degree Num}(f) - \text{degree Den}(f)} = q^{v_\infty(f)}$$

where $v_\infty(f)$ is the valuation at $z = 0$ of the rational function of the variable $z$ given by $f(\frac{1}{z})$.

**Example 1** *A famous example, playing a role in the work of Kummer, and understood in somewhat different language earlier by Gauss, is given by* $A = \mathrm{Z}[\frac{1+\sqrt{-23}}{2}]$ *with fraction field* $K = \mathrm{Q}[\sqrt{-23}]$. *One easily checks that the four numbers*

$$2, 3, \frac{1+\sqrt{-23}}{2}, \frac{1-\sqrt{-23}}{2}$$

*are all irreducible in the ring* $A$ *(proof: their norms to* Q *are, respectively* $4, 9, 6,$ and $6$ *so if they were reducible there would have to exist some element* $x + y\frac{1+\sqrt{-23}}{2}$ *of* $A$ *with norm either* $2$ *or* $3$, *But the norm of such an element is* $x^2 + xy + 6y^2$ *which never achieves* $2$ *or* $3$ *as value for* $x, y \in \mathrm{Z}$*).*

*But, of course, these four are inequivalent irreducibles in* $A$ *since the units of* $A$ *consist only of* $\pm 1$, *and:*

$$\frac{1+\sqrt{-23}}{2} \cdot \frac{1-\sqrt{-23}}{2} = 2 \cdot 3$$

*which is a blatant violation of unique factorization.*

*The ideal* $I = (2, \frac{1+\sqrt{-23}}{2})$ *has norm equal to* $2$, *so is not principal, but let's cube this ideal,* $I^3$, *to get something of norm* $8$. *It is principal, generated by one of the two elements of norm* $8$ *in our ring.*

*It is in fact the case that any fractional ideal is equivalent (modulo principal ideals) to* $1$, $I$, *and* $I^2$*; i.e.,* $\mathcal{H}(A)$ *is cyclic of order three. In language closer to Gauss's, there are only these equivalence classes of binary quadratic forms (over* Z*) of discriminant* $-23$*:* $X^2 + XY + 6Y^2$ *and* $2X^2 \pm XY + 3Y^2$.

### 3.3 The full formalism of the norm

For this read, *as homework for next lecture,* Appendix A, pp. 76-79 of Cassels-Frohlich, and/or section 5 (pp. 27,28) of Chapter I of Serre.

### 3.4 Extensions of Dedekind domains.

Let $A \subset K$ be a Dedekind Domain contained in its field of fractions, and let $L/K$ be a finite separable field extension. Define $B \subset L$ to be the integral closure of $A$ in $L$.

**Proposition 1** *The ring $B$ is a Dedekind domain.*

**Proof:** Again, fixing $\Theta \in B$ a primitive element for the separable finite extension $L/K$ and using the nondegeneracy of the trace pairing, and the fact that the $A$ is noetherian, one shows that $B$ is noetherian. That it is of dimension one follows from the following argument. Suppose one has $Q \subset Q' subset B$ a proper inclusion of prime ideals in $B$ such that they both lie over the same prime $P$ in $A$, i.e., $Q \cap A = Q' \cap A = P$. Dividing by the smaller of the two, we are facing an integral extension of two integral domains $A_1 := A/P \subset B/Q' =: B_1$ and a nonzero ideal $Q'/Q = Q_1 \subset B_1$ such that $Q_1 \cap A_1 = \{0\}$. But take a minimal integral polynomial relation, $x^n + a + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, satisfied by some nonzero element $x \in Q_1$, and note that $a_0$,, being a multiple of $x$, lies in $Q_1 \cap A = 0$, but if the equation was minimal, $a_0 \neq 0$, giving the contradiction we sought.

### 3.5 Decomposition of primes in an extension

Localization is the simplifying tool that allows us to focus on, and understand, the decomposition of a prime $P$ in the extension $L/K$. We know that $PB$, being a nonzero ideal of $B$, has a unique factorization

$$PB = \prod_i Q_i^{e_i}.$$

- *Localizing at the prime $P$: reducing to the case where $A$ is a DVR.* We can localize the rings $A$ and $B$ with respect to $S = A - P$, allowing us to work in the ring extension $B_P := S^{-1}B$ over the DVR $A_P := S^{-1}A$. Noting that there is a complete equivalence between the ideals containing $P$ in $B$ and the ideals containing $P$ in $B_P$, we have the "same" formula for the unique factorization of the ideal $PB_P$ in $B_P$ as for the original $P$ in $B$. Specifically,

  $$PB_P = \prod_i Q_i^{e_i} B_P,$$

  where—again–the $Q_i \cdot B_P$ are pairwise distinct maximal ideals in $B_P$. In a word, with respect to decomposition of $PB$ we lose no information if we pass to the localization of our extension at $P$.

- Localizing at the prime $Q_i$: reducing to the case where both $A$ and $B$ are DVR's. If we go further and localize at a factor $Q_i$ for some $i$, we will have "killed" all the other factors, and are left with the following formula in the DVR $B_{Q_i}$:

  $$P \cdot B_{Q_i} = Q_i^{e_i} \cdot B_{Q_i}$$

  useful for determining $e_i$, the ramification index of $Q_i$ over $P$.

The ring $B_P$ is a Dedekind domain with finitely many maximal ideals which we simply call $Q_1, Q_2, \ldots, Q_s$ (all of them having the property that $Q_i \cap A_P = PA_P$).

The $A_P$-module $B_P$ is free of finite rank; it is of rank equal to $[L : K]$ (since $L = B_P \otimes_{A_P} K$). It follows that the $[L : K]$-dimensional $A/P = A_P/PA_P$-vector space $B_P/P_{A_P}$ breaks into the following product of vector spaces,

$$B_P/P_{A_P} = \prod_i B/Q_i^{e_i},$$

and by counting dimensions we have the standard formula,

$$[L : K] = \sum_i e_i f_i,$$

where

$$f_i = \dim_{A/P}(B/Q_i) = [B/Q_i : A/P].$$

### 3.6 Monogenic extensions

Any easy type of extension $B/A$ to analyze is when $B$ is generated by a single element $\Theta$ that is integral over $A$, i.,e. $B = A[\Theta] = A[X]/(f)$ where $f(X) \in A[X]$ is a monic polynomial, irreducible (over $K$, or equivalently over $A$) with $\Theta$ as a root. If $B/A$ is of this form, let's call it a **monogenic extension**. If $P \subset A$ is a nonzero prime ideal, the following procedure provides a construction of the decomposition

$$PB = \prod_{i=1}^{\nu} Q_i^{e_i}.$$

Let $k_P := A/P$ denote the residue field of $P$. Let $\bar{f} \in k_P[X]$ be the reduction mod $P$ of $f$ and consider the unique factorization[1] of $\bar{f}$ in $k_P[X]$,

$$\bar{f} = \prod_{j=1}^{\nu} \bar{f}_i^{e_i},$$

where the $\bar{f}_i \in k_P[X]$ are (monic) [pairwise distinct irreducible polynomials. Defining $\phi_i \in B$ to be the image under $A[X] \to B$ of a lift, $f_i \in A[X]$, of $\bar{f}_i \in k_P[X] = A[X]/P \cdot A[X]$, we let $Q_i \subset B$ be the ideal in $B$ generated by $P$ and by $\phi_i$. Put $\ell_{Q_i} := B/Q_i = k_P[X]/(\bar{f}_i)$ which reminds us that $Q_i$ is a prime ideal of degree $\deg((\bar{f}_i)$ over $P$.

**Exercise 6** *Finish the discussion above by giving a complete proof that with $B/A$ a monogenic extension of Dedekind domains as above, and with $P, Q_i$ and $e_i$ as defined above, then*

$$PB = \prod_i Q_i^{e_i}.$$

[1]So, the essential requirement to be able to construct the unique factorization of these prime ideals of Dedekind domains, at least in this context, is to be able to find factorizations of polynomials over their residue fields.

### 3.7 Examples

- **Geometric example:** Take $A$ to be $\mathbf{C}[t]$ and take your favorite Riemann surface cover, given by a single polynomial: e.g., $X^3 + X + t$. So,

$$B = \mathbf{C}[X,t]/(X^3 + X + t) \;=\; \mathbf{C}[X].$$

There are no triple points (except at infinity) and ramification points are at the zeroes of the discriminant, which computes to be the polynomial

$$-(27t^2 + 4);$$

i.e., at $t = \pm\alpha = \pm 2/3\sqrt{-3}$. (Think of this extension as given by the mapping $X \mapsto t = -(X^3 + X)$ and take derivatives; or, you can see this just by trying to expressing $X^3 + X + a$ as a square of a polynomial in $X$ times a linear polynomial, and you'll immediately find that $a$ is a root of $27t^2 + 4$.) So, the ideals $P = (t - \beta) \subset A$, for $\beta \neq \pm\alpha$, decompose in $B$ as a product of three distinct primes, while $P = (t - \alpha), P' = (t + \alpha) \subset A$ decompose as a product $Q^2 \cdot Q' \subset B$. This all makes sense, given Riemann-Hurwitz.

Draw Picture

- **Back to our arithmetic example:** Take $A = \mathrm{Z}$ and $B :=$ the integral closure of Z in $L := \mathrm{Q}[X]/(X^3 + X + c)$ for $c \in \mathrm{Z}$, and $\Theta \in B$ a root of $X^3 + X + c$. Again the discriminant of $\mathrm{Z}[\Theta]$ is $= -(27c^2 + 4)$ so we know that $\Delta$, the discriminant of $B$ (i.e., the discriminant of the algebraic number field $L$), satisfies the formula

$$\Delta = \frac{-(27c^2 + 4)}{I^2}$$

where

$$I = [B : \mathrm{Z}[\Theta]]$$

is the index of $\mathrm{Z}[\Theta]$ in $B$. Here are three "exercises," the third one I don't know how to do.

**Exercise 7** *Show that the "odd part" of $\Delta$ is square-free. I.e., up to sign and powers of 2 we have that $\Delta$ is given as the product of all primes $p$ such that $v_p(27c^2 + 4)$ is odd; or equivalently, $|\Delta|$ is the unique squarefree divisor of $27c^2 + 4$ such that $\frac{27c^2+4}{|\Delta|}$ is a square. (Hint: Factor $X^3 + X + c$ modulo $p$ for $p$ an odd prime. It can't be the cube of a linear polynomial, so we can't have that $pB = Q^3$ in $B$. So either $p$ is unramified in $B$ in which case $p$ doesn't divide $\Delta$ or else we have $pB = Q^2Q'$ where $Q \neq Q'$ in which case $p \mid \Delta$ but $p^2$ doesn't. It is clearer, in my opinion,, to treat $p = 3$ separately.)*

**Exercise 8** *Discuss $v_2(\Delta)$ (i.e., the power of 2 that divides $\Delta$).*

Recall that an **order** in the ring of integers of a number field, is for some incomprehensible reason, the word that people use to refer to any subalgebra of finite index in the ring of integers. By the **index** of an order, let us mean that finite index. By the **monogenic defect** of the ring of integers of a number field let us mean the *minimum* of the indices of all monogenic orders in that ring of integers. So, if the ring of integers is itself monogenic, then its monogenic defect is 1.

**Exercise 9** *(Question raised by Dan Kane) For a given integer $c$ can we compute the $\delta(c) :=$ the monogenic defect of $B$ where $B$ is the ring of integers in $\mathrm{Q}[X]/(x^3+X+c)$? For example, given the table of last time:*

$$\begin{array}{lccc} \mathbf{6}: & 1, & \Theta, & \frac{\Theta^2-\Theta}{2} \\ \mathbf{14}: & 1, & \frac{\Theta^2+\Theta+2}{4}, & \frac{-\Theta^2+3\Theta-2}{4} \\ \mathbf{18}: & 1, & \Theta, & \frac{\Theta^2-\Theta+2}{4} \\ \mathbf{19}: & 1, & \frac{\Theta^2+3\Theta+3}{7}, & \frac{-\Theta^2+4\Theta-3}{7} \\ \mathbf{22}: & 1, & \Theta, & \frac{-\Theta^2-\Theta}{2} \end{array}$$

*can you figure out the value of $\delta(c)$ for $c = 12, 18, 19, 22$?*

**Vague Question:** Are there ways, in SAGE, or gp/PARI, of doing numerical experiments to get a sense of the statistical behavior of $\delta(c)$ for varying $c$?

### 3.8 Monogenicity of finite extensions of discrete valuations rings with separable residual field extensions

The title of this subsection is indeed a theorem:

**Theorem 4** *Let $L/K$ be a field extension (of finite degree); let $A \subset K$ be a DVR with field of fractions equal to $K$; and let $B \subset L$, the integral closure of $A$ in $L$, also be a DVR. Suppose further that $\ell/k$, the corresponding extension of residue fields, is finite separable. Then $B$ is a monogenic $A$-algebra.*

This, for example, is Prop. 12 of Chapter III section 7 in Serre's *Local Fields* and it will be discussed in a fourth hour session soon.

## 4 Local Fields

### 4.1 Normalized Absolute Values

- **Nonarchimedean primes** Let $A$ be the ring of integers in the number field $K$ and $P \subset A$ a prime ideal. For $x \in K$ put

$$\|x\|_P := NP^{-v_P(x)} = \#(A/P)^{-v_P(x)},$$

this giving a nonarchimedean absolute value, i.e., $\|x+y\|_P \leq \max\{\|x\|_P, \|y\|_P\}$.

- **Archimedean primes** If $\Theta \in K$ is a primitive element of $K$ and if its minimal polynomial relation over Q has $r_1$ real roots and $r_2$ pairs of complex roots (with $[K : /Q] = r_1 + 2r_2$) we get (the) $r_1$ distinct real imbeddings of the field $K \hookrightarrow \mathbf{R}$ and the $r_2$ (conjugate-pair) complex imbeddings $K \hookrightarrow \mathbf{C}$ by sending $\Theta$ to each of these roots. For each of these real or conjugate-pairs of complex imbeddings one obtains an absolute value: i.e., by pullback from

$|\ |_{\mathbf{R}}$ the standard absolute value on $\mathbf{R}$; or from $|\ |_{\mathbf{C}}$ on $\mathbf{C}$; there is something awkward about the normalization here, but we put $\|\ \|_{\mathbf{R}} = |\ |_{\mathbf{R}}$ and $\|\ \|_{\mathbf{C}} = |\ |^2_{\mathbf{C}}$ (i.e., in the complex case we take the square of the standard absolute value, to account for the fact that we are dealing with a conjugate pair).

It is customary (but even after a century of this custom, it remains puzzling) to call the $r_1$ real imbeddings the *real primes*, and the $r_2$ conjugate-pairs of complex imbeddings the *complex primes* of $K$.

**Theorem 5 ( Product Formula)** *If $K$ is a number field and $x \in K^*$, then*

$$\prod_v \|x\|_v \ = \ 1,$$

*where $v$ ranges through all the primes of $K$, the finite, or synonymously, the nonarchimedean, primes corresponding to the prime ideals of $A$, and the infinite or synonymously, the archimedean, primes, meaning the real and complex ones, described above.*

**Proof:** It is true for $K = \mathrm{Q}$, for the product of $\|x\|_v$ where $v$ ranges through all ordinary primes is immediately seen to be equal to $\|1/x\|_{\mathbf{R}}$, and this cancels out with the term $\|x\|_{\mathbf{R}}$ in the product above corresponding to the unique real prime $p =$ "$\infty$" of Q. To see that it is generally true, we need the formula:

$$\prod_{v\ |\ p} \|x\|_v = \|N_K^{\mathrm{Q}}(x)\|_p$$

which, being multiplicative, need only be checked on elements $x \in A - \{0\}$. Suppose that $p$ is a finite prime so that we must show

$$\prod_{P\ |\ p} \|x\|_v = \|N_K^{\mathrm{Q}}(x)\|_p.$$

In this case $\|N_K^{\mathrm{Q}}(x)\|_p = p^{-X}$ where $p^X$ is the power of $p$ dividing the order of $A/xA$. Write the ideal $(x) = \prod_P P^{v_P(x)}$ so that

$$A/xA = \prod_{P\ |\ p} A/P^{v_P(x)} \times \text{the rest}$$

where "the rest" is of order prime to $p$. This proves the formula for finite primes and an easier, but somewhat similar argument does it for the infinite prime.

## 4.2 The category of profinite groups

There are fancy ways of discussing (projective, say) limits in a category, but the following is a minimalist's discussion of *profinite groups* which will almost be sufficient for us.

Let

$$\cdots G_\nu \to G_{\nu-1} \to \cdots G_2 \to G_1 \to G_0$$

be an infinite sequence of finite groups, and linking homomorphisms $G_\nu \to G_{\nu-1}$. Put

$$G = \text{proj. lim.}_\nu\, G_\nu \subset \prod_{\nu=0}^{\infty} G_\nu$$

i.e., an element of $G$ is a system of elements $\{g_\nu \in G_\nu\}_{nu}$ that are compatible with respect to the linking homomorphisms of the sequence above, multiplication being defined coordinate-wise.

For any such infinite sequence, we can define its *essential core sequence* as follows: Let

$$\Gamma_\nu := \cap_{\mu \geq \nu} \text{image } \{G_\mu \subset G_\nu\}$$

and note that when we restrict the linking homomorphisms to the subgroups $\Gamma_\nu$, to get an infinite sequence

$$\cdots \Gamma_\nu \to \Gamma_{\nu-1} \to \cdots \Gamma_2 \to \Gamma_1 \to \Gamma_0$$

the linking homomorphisms are all now surjections, and the projective limit proj. $\lim._\nu\, \Gamma_\nu$ is equal to the initial projective limit $G$, and for any $\nu$ we have an exact sequence

$$0 \to N_\nu \to G \xrightarrow{\pi_\nu} \Gamma_\nu \to 0,$$

where $N_\nu = \ker\{\pi_\nu\}$.

The group $G$ is naturally endowed with a compact Hausdorf topology and this can be viewed as given in either of the these various ways:

- A base for the topology of $G$ is the collection of [cosets of] the $N_\nu \subset G$ for all $\nu$; these subgroups $N_\nu$ are all compact open subgroups of $G$ of finite index.
- The topology on $G$ is the topology with the fewest open subsets that has the property that the projection mappings $\pi_\nu : G \longrightarrow \Gamma_\nu$ are all continuous, where the finite groups $\Gamma_\nu$ are, of course, given the discrete topology.
- The topology on $G$ is the topology it inherits as a (closed) subgroup of the product group $\prod_{\nu=0}^{\infty} \Gamma_\nu$, where—again—where the finite groups $\Gamma_\nu$ are given the discrete topology.

**Examples:**

1. **(Completions of groups)** In practice we may not be given such a neat infinite sequence of finite groups. A typical example is when we are given a discrete group $G$ and we form

   $$\hat{G} :=:= \text{ proj. lim.}_{N \subset G}\, G/N$$

   where $N \subset G$ suns through all normal subgroups of finite index in $G$.

2. **(Galois groups of field extensions of infinite degree)** In practice we may not be given such a neat infinite sequence of finite groups. A typical example is when $L/K$ is an infinite degree field extension that can be expressed as the union of all of its finite Galois subextensions of $K$. Here it is natural to consider the directed system $\mathcal{J}$ of all finite Galois subextensions

of $L/K$ where the "arrows" of the directed system are given by inclusion of subextensions, and then define the Galois group of $L/K$ to be the projective limit

$$\mathrm{Gal}(L/K) := \text{ proj. lim.}_{K'/K \in \mathcal{J}} \mathrm{Gal}(K'/K).$$

The (pro-finite) topology on this group is called the *Krull topology* and the closed subgroups of $\mathrm{Gal}(L/K)$ are naturally in one-one correspondence (following the format of classical Galois Theory) with all subfields $M \subset L$ containing $K$. So, if $K$ is a field, we may choose $\bar{K}/K$ an algebraic closure, and form

$$G_K := \mathrm{Gal}\bar{K}/K)$$

noting that $G_K$ should really be a groupoid in Grothendieck's language. That is, it is a category all of whose morphisms are isomorphisms; the objects of the category are *algebraic closures* of $K$ and the morphisms are isomorphisms over $K$. The algebraic topologists know this type of structure well, with their fundamental groups that don't depend upon a base point. Of course, once you do chose a base point, you get an honest group, but you should probably remember that your $G_K$ is really well defined only—up to inner automorphism. If $G_K$ is abelian, though, it is indeed well-defined and in those cases you might expect to actually give "proper names" to particular elements in $G_K$. A famous example of this is when $K$ is a finite field, where $G_K$ is canonically isomorphic to $\hat{\mathrm{Z}}$, the profinite completion of Z, and the "proper name" given to the element of $G_K$ corresponding to $1 \in \hat{\mathrm{Z}}$ is *Frobenius*.

3. **(Completions of rings and modules)** Typical here is to begin with a ring $A$—with "no" topology; i.e., the discrete topology) and an ideal $I \subset A$ and to form

$$\hat{A} := \text{proj.lim.}_{\nu}\ A/I^{\nu}.$$

Then $\hat{A}$ is a topological ring with a topology on it; this is called the **$I$-adic completion of $A$**. If $A/I$ is finite, then $\hat{A}$ has a *profinite topology*. A topological ring $R$ with a closed ideal $I \subset R$ such that $R/I^{\nu}$ is discrete, and such that the natural homomorphism $R \to \text{proj.lim.}_{\nu}\ R/I^{\nu}$ is an isomorphism of topological rings, is said to be **$I$-adically complete**.

The natural homomorphism

$$A \longrightarrow \hat{A}$$

may have a nontrivial kernel, but has dense image. If $M$ is an $A$-module we can perform this same $I$-adic completion process to $M$, giving the $\hat{A}$ -module

$$\hat{M} \ = \ \text{proj.lim.}_{\nu}\ M/I^{\nu}M \ = \ M \otimes_A \hat{A}.$$

**Theorem 6** *If $A$ is a noetherian local ring with $m \subset A$ its maximal ideal then the $m$-adic completion $\hat{A}$ is again a noetherian local ring with maximal ideal $\hat{m}$.*

(This is Proposition 10.16 in **[A-M]**.)

**Theorem 7** *If $A$ is a complete noetherian local ring and $B$ a ring extension of $A$ of finite type as an $A$-module, then $B$ is a (finite) product of complete local ring extensions of $A$.*

**Proof.** The ring $B$ is again noetherian, and if $m \subset A$ is the maximal ideal of $A$ with $k = A/m$ the residue field, form the finite dimensional $k$-algebra $B/mB$ and write this as a product of artinian local $k$-algebras ,

$$B/mB = \prod_j \bar{B}_j,$$

with maximal ideals $\bar{M}_j \subset \bar{B}_j$. Let $M_j \subset B$ be the inverse image of $\bar{M}_j$ under the natural homomorphism $B \to \bar{B}_j$, noting that $M_j$ runs through all the maximal ideals of $B$. These maximal ideals are pairwise relatively prime, so, letting $B_j$ denote the completion of $B$ with respect to $M_j$ an application of the Chinese Remainder Theorem gives us that the natural homomorphism

$$B \longrightarrow \prod_j B_j$$

is an isomorphism of (finitely generated) $A$-algebras.

**Remarks and Examples.**

- *The Monogenic Case.* In the special case where $f(X) \in A[X]$ is a monic irreducible polynomial generating the monogenic extension $B$, so that $B = A[X]/(f(X)) = A[\Theta]$ where $\Theta \in B$ is a root of $f$, one gets the $M_j$'s, as mentioned before, by factoring the reduction of $f$ to the residue field $k = A/m$,

  $$\bar{f}(X) = \prod_j \bar{g}_j(X)^{e_j} \in k[X]$$

  into powers, $\bar{g}_j(X)^{e_j}$ of pairwise distinct irreducibles, of $\bar{f}$. An application of Hensel's Lemma allows us to lift this factorization to

  $$f(X) = \prod_j H_j(X) \in A[X]$$

  where $\bar{H}_j = \bar{g}_j^{e_j}$ for each $j$. Put $I_j := m \cdot B + H_j(\Theta) \cdot B$ so that $B/I_j = k[X]/(\bar{g}_j^{e_j})$ is an artinian local ringlet $M_j \subset B$ is the inverse image of its maximal ideal, which is then a maximal ideal of $B$ with residue field $\ell_j := k[X]/(\bar{g}_j(X)^{e_j})$.
- *Extensions of a complete DVR.* Now suppose that $A$ is a complete DVR with fraction field $K$ and $L/K$ is a finite separable field extension, with $B \subset L$ the integral closure of $A$ in $L$. The $B$ is again a complete DVR . This is because if $B = \prod_{j=i}^{k} B_j$ as above, note that $B$ is—by hypothesis—an (integrally closed) integral domain, we obtain that $j = 1$, that $B = B_1$ is a (complete) local integral domain finite over a noetherian ring of Krull dimension one, and integrally closed. Hence, by Theorem 1 $B$ is a DVR. Also, by Theorem 4 $B$ is a monogenic extension of $A$.

  If $A$ is a complete DVR with $K$ as field of fractions,and $z \in A$ a choice of uniformizer, we can endow

  $$K = A[1/z] = \bigcup_\nu z^{-\nu} \cdot A$$

  with the weak topology induced (in the evident way) from the topology on $A$, and view its valuation, $v_K : K^* \to \mathrm{Z}$, as a continuous mapping (where $v_K(z) = 1 \in \mathrm{Z}$ and, of course, Z is given the discrete topology). If the residue field of $A$ is finite, then $A$ is

compact, and $K$ is locally compact. If $B/A$ is a DVR extension as described in the paragraph above, with field(s) of fractions $L/K$, we have the formula

$$v_L \;=\; \frac{1}{f_{L/K}} v_K \cdot N_{L/K}.$$

4. **(Arithmetic groups over complete rings)** Take, for example, a complete noetherian local ring $A$ with maximal ideal $m$ and form

$$\mathrm{GL}_N(A) := \mathrm{proj.lim.}_\nu \mathrm{GL}_N(A/m_\nu).$$

If the residue field is finite, then $\mathrm{GL}_N(A)$ is a profinite group.

## 4.3 Completion and topologies of fields

Let $K$ be a number field and $v$ a finite or infinite prime, so that

$$\| \|_v : K \to \mathbf{R}$$

is a nonarchimedean or archimedean absolute value, which puts a topology on $K$ by defining a base of open sets to be the open discs $D_r(x) := \{y \mid \|x - y\|_v < r\}$ $(r > 0; x \in K)$. (Let $K_v$ be the *completion* of $K$ with respect to the metric determined by $\| \|_v$ or, if $v$ is complex, by $\| \|_v^{1/2}$. The completion $K_v$ is a (complete) topological field containing $K$ as a dense subfield and $\| \|_v$, extends to a continuous mapping

$$\| \|_v : K_v \to \mathbf{R}$$

satisfying the analogous properties

1. $\|x\|_v = 0 \leftrightarrow x = 0$,
2. $\|x \cdot y\|_v = \|x\|_v \cdot \|y\|_v$
3. $\|x + y\|_v \leq \max\{\|x\|_v, \|x\|_v, \}$ (in the nonarchimedean case, and the evident inequalities in the archimedean cases)

for $x, y \in K_v$.

Restricting attention to the nonarchimedean case, the valuation $v : K \to \mathrm{Z} \cap \{\infty\}$ extends to a nonarchimedean valuation $v : K_v \to \mathrm{Z} \cap \{\infty\}$ for which we have the formula

$$\|x\|_v = NP^{-v(x)}$$

for $x \in K_v$ analogous to the formula in $K$. In particular, $K_v$ is a *nonarchimedean valued field* with residue field $k_v := A/P$; let $q$ denote the cardinality of this finite field.. If $A_v \subset K_v$ is the ring of integers relative to this extended valuation (i.e., the set of elements of $K_v$ of valuation $\geq 0$) then we have:

$$A_v = \lim_n A/P^n = \lim_n A/z^n A$$

where $z$ is a uniformizer of $A$. The ring $A_v$ has a profinite topology, hence is compact, and it has a base of open and closed neighborhoods of 0 is given by $\{z^n A_v\}_n$,; here $K_v$ is the union of $z^{-n} A_v$ ($n$ tending to $\infty$).

**Theorem 8** *The additive group of $K_v$ is locally compact. (A complete nonarchimedean valued field is locally compact if and only if its residue field is finite.) The multiplicative group $K_v^*$ is locally compact.*

DRAW PICTURE: increasing annuli of different valuations, mapping of $K_v^*$ to $K_v$

Note that $A_v \subset K_v$ is a compact open.

Let $\mu$ be a Haar measure on the additive locally compact group $K_v$.

**Theorem 9** *If $E$ is a measurable subset of $K_v$, then*

$$\mu(x \cdot E) = \|x\|_v \cdot \mu(E).$$

**Proof:** May suppose that $x \neq 0$. Since $y \mapsto xy$ is an automorphism of the additive group, $E \mapsto \mu(x \cdot E)$ is a multiple of Haar measure, i.e., we have that $\mu(x \cdot E) = \phi(x)\mu(E)$ for some nonzero (well-defined) element $\phi(x) \in K_v^*$, and since both $\phi$ and $\| \ \|_v$ are multiplicative, we may suppose that $x \in A_v$, and check things for $E = A_v$ with Haar measure $\mu$ such that $\mu(A_v) = 1$. Then $\phi(x) = \mu(x \cdot A_v) = 1/(A_v/xA_v) = q^{v(x)} = \|x\|_v$.

## 4.4 Unramified extensions of Local Fields

**Theorem 10** *Let $p$ be a prime number and consider the following two categories:*

- $\mathcal{F} :=$ *The category of finite fields of characteristic $p$.*
- $\mathcal{D} :=$ *the category of unramified field extensions of $\mathrm{Q}_p$ of finite degree.*

*These categories are equivalent, via the following functors:*

- *The functor $\mathcal{D} \rightsquigarrow \mathcal{F}$ that passes from a discrete valued field to the residue field of its ring of integers.*
- *The functor $\mathcal{F} \rightsquigarrow \mathcal{D}$ that associates to any finite field $k$ of characteristic $p$ the field of fractions of its ring $W(k)$ of Witt vectors. See Chapter II section 5 of Serre's Local Fields.*

Fix a prime number $p$, and let $K/\mathrm{Q}_p$ be a finite extension, and in particular, $K$ is a *local field*. Let

$$K \ \subset \ K^{\mathrm{unr}} \ \subset \ K^{\mathrm{ab}} \ \subset \ \bar{K}$$

be the sequence of fields that you can guess. In particular, $K^{\mathrm{unr}} \subset \bar{K}$ is the maximal unramified subextension $K^{\mathrm{unr}}/K$ in $\bar{K}/K$; since $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \hat{\mathrm{Z}}$ we have that $K^{\mathrm{unr}} \subset K^{\mathrm{ab}}$. Put $G_K := \mathrm{Gal}(\bar{K}/K)$ and so the abelianization, $G_K^{\mathrm{ab}}$ is naturally isomorphic to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$

We have the exact sequence of groups

$$1 \to I_K \to G_K \to \mathrm{Gal}(K^{\mathrm{unr}}/K) \to 1$$

which splits since $\hat{\mathrm{Z}}$ is a free object in the category of profinite groups. The subgroup $I_K \subset G_K$ is called the *inertia subgroup* and denote by $AI_K \subset G^{\mathrm{ab}}$ the image of $I_K$ under projection $G_K \to G^{\mathrm{ab}}$ (call this the *abelian inertia subgroup* as distinguished, by the way, from the abelianization of the inertia subgroup, which is much bigger).

We have an exact sequence:

$$1 \to AI_K \to G_K^{\mathrm{ab}} \to \mathrm{Gal}(K^{\mathrm{unr}}/K) \to 1,$$

which—of course—also splits (noncanonically, as we shall be examining soon). If $\iota : Gal(K^{\mathrm{unr}}/K) \to G_K^{\mathrm{ab}}$ is a lifting, put

$$K^{\iota} := \{G_K^{\mathrm{ab}}\}^{\ker(\iota)};$$

i.e., $K^{\iota}$ is the fixed subfield in $G_K^{\mathrm{ab}}$ of the subgroup $\ker(\iota) \subset Gal(K^{\mathrm{unr}}/K)$.

We can think of $K^{\iota}$ as *a* maximal totally ramified subextension in $K^{\mathrm{ab}}/K$, for it is indeed totally ramified (Definition: An algebraic field extension $L/K$ is **totally ramified** if every sub-extesion $L_o/K$ of finite degree is); $K^{\iota}$ is a maximal with this property in $K^{\mathrm{ab}}$ and the italicized indefinite article reminds us that there are many such (maximal totally ramified subextensions of $K^{\mathrm{ab}}/K$).

### 4.5 Tamely ramified extensions

Let $K/\mathrm{Q}_p$ be of finite degree, as usual, and let the notation $A \subset K$ and $k = A/\pi A$ have their usual meaning. Put $q = \#(k)$ and note that

$$L = K[X]/(X^{q-1} - \pi)$$

is a totally ramified, Galois, cyclic, field extension of $K$ with Galois group canonically isomorphic to $k^*$.

*not written beyond this point ...*

## 5 Adeles and Ideles

Now let $K$ be a number field, as above, and let $v$ range through the set of all "primes" of $K$ (synonym: *places* of $K$) i.e., the nonarchimedean primes corresponding to the maximal ideals of $A \subset K$, its ring of algebraic integers, and the $r_1 + r_2$ archimedean primes. let $S$ be a finite set of places of $K$ containing all archimedean ones. Define the locally compact topological ring,

$$\mathbf{A_K^S} := \prod_{\mathbf{v} \in \mathbf{S}} \mathbf{K_v} \times \prod_{\mathbf{v} \notin \mathbf{S}} \mathbf{A_v},$$

noting that it is indeed locally compact, and that for $S \subset S'$ an inclusion of finite sets of places as above, we have a natural inclusion

$$\mathbf{A_K^S} \hookrightarrow \mathbf{A_K^{S'}}$$

where the smaller topological ring is imbedded as an open subringof the larger. Define $\mathbf{A_K}$, **the ring of adeles of** $K$, to be:

$$\mathbf{A_K} := \bigcup_{\mathbf{S}} \mathbf{A_K^S} = \lim_{\mathbf{S}} \mathbf{A_K^S}$$

(... to be continued)

# 6 The Ideal Class Group and the Dirichlet Unit theorem

## 6.1 Sketch of some elements that enter into the proof of the finiteness of the ideal class group and the Dirichlet Unit Theorem.

Let $K$ be a number field and $A \subset K$ its ring of integers.

## 6.2 On the finiteness of the ideal class group

**Proposition 2** *There is a positive real number $M$ depending only on $K$ such that every nonzero ideal $I$ of $A$ contains a nonzero element $\alpha \in I$ such that*

$$|N_{K/\mathrm{Q}}(\alpha)| \ \leq \ M \cdot \#(A/I) \ = \ M \cdot N(I).$$

**Proof 1** *Let $d := [K : \mathrm{Q}]$. Fix a basis $\alpha_i$ (for $i = 1, \ldots, d$) of $A$ as* Z*-module, and let $\alpha_i \hookrightarrow \mathbf{C}$ (for $i = 1, \ldots, d$) be the $d$ distinct imbeddings.*

*Put*

$$M := \prod_{i=1}^{d} \sum_{j=1}^{d} |\sigma_j(\alpha_i)|.$$

*For the positive number $m$ such that $m^d \leq N(I) < (m+1)^d$ use the Dirichlet Box Principle on the collection*

$$\sum_{i=1}^{d} m_i \alpha_i$$

*($m_i \in \mathrm{Z}$ and $0 \leq m_i \leq m$) to see that at least two of these are congruent mod $I$ and therefore taking the difference we have an $\alpha = \sum_{i=1}^{d} m_i \alpha_i$ with $|m_i| \leq m$ contained in $I$, so compute:*

$$|N_{K/\mathrm{Q}}(\alpha)| = \prod_{i=1}^{d} |\sigma_i(\alpha)| \leq \prod_{i=1}^{d} \sum_{j=1}^{d} m_i |\sigma_j(\alpha_i)|.$$

*So,*

$$\prod_{i=1}^{d} \sum_{j=1}^{d} m_i |\sigma_j(\alpha_i)| \leq m^d \cdot \prod_{i=1}^{d} \sum_{j=1}^{d} |\sigma_j(\alpha_i)| = m^d \cdot M \leq N(I) \cdot M.$$

**Note:** One can, and should, improve the $M$. Note also that however we do improve it we will never get $M < 1$. The classical formula for a good $M$, using Minkowski's theorem about points in lattices is the *Minkowski constant*

$$M = \frac{d!}{d^d} (\frac{4}{\pi})^{r_2} \cdot \sqrt{|\mathrm{disc}(A)|}.$$

Note also that $\frac{d!}{d^d}$ tends to zero quite rapidly as $n$ goes to infinity, and since even the best $M$ is $\geq 1$ we would get from the above that

$$\sqrt{|\mathrm{disc}(A)|} \ \geq \ \frac{d^d}{d!} (\frac{\pi}{4})^{r_2}.$$

and the RHS here is always strictly $> 1$ if $d > 1$.

**Corollary 11** *Every ideal class group of $A$ contains an ideal $J$ with $N(J) \leq M$.*

**Proof 2** *For $C$ an ideal class, we work with the inverse of $C$, and find an ideal $I \in C^{-1}$, an $\alpha \in I$ with Norm $\leq M \cdot N(I)$ and factor ideals*

$$(\alpha) = I \cdot J$$

*so that*

$$N((\alpha)) = |N_{K/\mathrm{Q}}(\alpha)| = N(I) \cdot N(J)$$

*giving*

$$N(J) \leq M.$$

**Corollary 12** *The ideal class group of $K$ is finite.*

**Read:** Chapter V section 4 (i.e., pages 119-122, at least in my edition) of Lang's Algebraic number theory.

### 6.3 Comments on the Dirichlet Unit Theorem.

Recall

$$A^* \to \prod_{v \mid \text{real}} \{\pm 1\}_{\{v\}} \times \prod_{v \mid \text{complex}} S^1_{\{v\}} \times \prod_{v \text{ infinite}} \mathbf{R}^{>0}_{\{v\}}$$

and the projection

$$\Lambda \subset \{ \prod_{v \text{ infinite}} \mathbf{R}^{>0}_{\{v\}} \}^o.$$

Recall that the D.U.T. follows from the assertion that $\Lambda$ is a discrete lattice of maximal rank in

$$\{ \prod_{v \text{ infinite}} \mathbf{R}^{>0}_{\{v\}} \}^o \cong \mathbf{R}^{r_1+r_2-1}.$$

Some ingredients of the classical proof of this:

- **From the Geometry of Numbers:**

  **Proposition 3** *There is a constant $C$ such that for any archimedean place $v_0$ of $K$ and for any $\alpha \in A$ ( nonzero) there is a $\beta \in A$ (nonzero) with*

  $$|N_{K/\mathbf{Q}}(\beta)| \leq C$$

  *with*

  $$\|\beta\|_v \ < \ \|\alpha\|_v$$

  *for all archimedean $v \neq v_0$.*

- **Using finiteness of the set of ideals of bounded norm:**

  **Corollary 13** *For any archimedean place $v_0$ of $K$ is a unit $u \in A^*$ with*

  $$\|u\|_v < 1$$

  *for all archimedean $v \neq v_0$.*

- **Applying logs and reducing it to the computation of the rank of a matrix:**

  **Proposition 4** *Let $(a_{ij})$ be an $N \times N$ matrix of real numbers such that $a_{ii} > 0$ for all $i$, and $a_{ij} < 0$ for all $i \neq j$, and such that each row sums to 0. Then $(a_{ij})$ has rank $N-1$.*

  **Proof 3** *Suppose that we have $\sum_{i=1}^{N-1} t_i V_i = 0$ for some constants $t_i$ ($i = 1, \ldots, N-1$) and where $V_i$ is the $i$-th column of our matrix. After minor modification we can suppose that there is a $k \leq N-1$ such that $t_k = 1$ and all the $t_i$ are $\leq 1$. Now concentrate on the $k$-th row*

  $$0 = \sum_{i=1}^{N-1} t_i a_{ki} = t_k \sum_{i=1}^{N-1} a_{ki} - \sum_{i=1}^{N-1} (t_k - t_i) a_{ki} \geq \sum_{i=1}^{N-1} a_{ki} > \sum_{i=1}^{N} a_{ki} = 0.$$

# 7 Comments on Function fields

To be continued ...