ALGEBRAIC NUMBER THEORY

LECTURE 6 NOTES

Material covered: Class numbers of quadratic fields, Valuations, Completions of fields.

1. Ideal class groups of quadratic fields

These are the ideal class groups of the Dedekind domains $\mathcal{O}_K$ for quadratic fields K. We already saw that we can have examples of non-PIDs even for quadratic fields. For instance, a homework problem is to show that the class group of $\mathbb{Z}[\sqrt{-m}]$ ($= \mathcal{O}_{\mathbb{Q}(\sqrt{-m})}$ if $-m \equiv 2$ or $3 \mod 4$) is nontrivial for m squarefree and composite.

Gauss conjecture: Let $h(d)$ be the class number of $\mathbb{Q}(\sqrt{d})$. Then $h(d) \to \infty$ as $d \to -\infty$. In particular, there are only finitely many fields with a given class number.

The class number 1 problem is to find all the imaginary quadratic fields whose ring of integers are PIDs. Heilbronn (1934) proved the Gauss conjecture and showed that there were at most 10 imaginary quadratic fields with class number one. Nine of them correspond to $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$ and conjecturally there was no tenth. This was proved by Heegner in 1952 using modular forms (Stark and Birch in the 1960s clarified Heegner's proof which was not believed at first). An independent proof was given by Baker in 1966 using transcendental number theory. (Baker won the Fields medal for his work on linear forms in logarithms, which provides the basis for many explicit methods in diophantine equations). Goldfeld's work in 1985 connected the class number problem to L-functions of elliptic curves, and reduced it to a finite computation in principle, for any given n.

The discriminants above are quite special, for instance notice that $e^{\pi\sqrt{163}}$ is almost an integer ($640320^2 + 744$ + error of less than 10^{-12}), and that $x^2 + x + 41$ which has discriminant -163, is prime for $x = 0, 1, \ldots, 39$.

For real quadratic fields, much less is known: for instance, it is not known if class number one happens infinitely often. Cohen-Lenstra heuristics are some precise conjectures which predict, for instance, that more than 75% of real quadratic fields will have class number 1.

2. Local fields

2.1. **Valuations.** Let K be a field. An *absolute value* or *valuation* on K is a function $|\ |: K \to \mathbb{R}$ such that

(1) $|x| \geq 0$ for all $x \in K$, with equality iff $x = 0$.
(2) $|xy| = |x||y|$ for all $x, y \in K$.
(3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$ (the triangle inequality).

We say that $|\ |$ is a *non-archimedean valuation* iff in addition to (1) and (2), $|\ |$ satisfies the stronger inequality (than (3)) $|x + y| \leq \max(|x|, |y|)$. Else we say $|\ |$ is archimedean.

Example. If $K = \mathbb{Q}$, we have the archimedean absolute value $|\ |$ which we shall label $|\ |_\infty$. Now let's define $|\ |_p$ by $\left|p^k \frac{a}{b}\right| = p^{-k}$ if $k \in \mathbb{Z}$ and a, b are not divisible by p. So $|p|_p = 1/p$ and $|a|_p = 1$ if p doesn't divide a. It is easy to check that $|\ |_p$ is a non-archimedean valuation on $\mathbb{Q}$: the triangle inequality just says that if $p^k | a$ and $p^l | b$ then $p^{\min(k,l)} | a + b$.

Remark. For any field, there is a *trivial* valuation given by $|x| = 1$ if $x \neq 0$, and $|0| = 0$. From now on we shall exclude the trivial valuation.

Remark. For any valuation, $|1| = |-1| = 1$. For we have $|1| = |1 \cdot 1| = |1|^2$, so $|1| = 0$ or 1. The former cannot hold by property (1). Similarly it's easy to show $|-1| = 1$.

Lemma 1. *Let $|\ |$ be a valuation of a field K. Let $n \in K$ be the element $1 + \cdots + 1$ (n times). Then $||$ is nonarchimedean iff n is bounded.*

Proof. Suppose $|\ |$ is nonarchimedean. Then $|1| = 1, |1 + 1| \leq \max(|1|, |1|) = 1$ and by induction $|n| \leq 1$ for all n. Now suppose $|n| \leq N$ for some $N \in \mathbb{R}$. Then let $x, y \in K$ and suppose w.lo.g. $|x| \geq |y|$.

$$|x + y|^n = |(x + y)^n| = \left|\sum \binom{n}{i} x^i y^{n-i}\right| \leq \sum N|x|^i |y|^{n-i} \leq N(n + 1)|x|^n$$

Taking n'th roots and letting $n \to \infty$ we get $|x + y| \leq |x| = \max(|x|, |y|)$. □

We say the valuations $|\ |_1$ and $|\ |_2$ are equivalent if $|x|_1 < 1 \iff |x|_2 < 1$, for all $x \in K$.

Exercise. Show that two valuations $|\ |_1$ and $|\ |_2$ are equivalent iff there is a real number $s > 0$ such that $|\ |_1 = |\ |_2^s$.

Remark. If $|\ |$ is nonarchimedean and $|x| \neq |y|$ then $|x + y| = \max(|x|, |y|)$. This is because if for instance $|x| > |y|$ then $|x| = |x+y-y| \leq \max(|x+y|, |y|)$, forcing $|x| \leq |x + y|$ which alongwith $|x + y| \leq \max(|x|, |y|) = |x|$ implies $|x + y| = |x|$.

Theorem 1 (Ostrowski's theorem)**.** *Every valuation of $\mathbb{Q}$ is equivalent to $|\ |_\infty$ or to $|\ |_p$ for some p.*

Proof. Suppose first $|\ |$ is nonarchimedean. Then by the proof of the above lemma, $|n| \leq 1$ for all positive integers n. Since the valuation is nontrivial and $|-1| = 1$, we must have $|n| < 1$ for some n (else by multiplicativity, the absolute value of every nonzero rational number would be 1). The smallest such n is clearly a prime, say p. Now if $q \neq p$ is another prime, then $ap + bq = 1$ for some integers p. So $|b||q| = |1 - ap| = 1$ by the remark above. Since $|b| \leq 1$, we have $|q| \geq 1$ and so $|q| = 1$. So the valuation of every prime other than p is 1, and this shows that $|\ |$ must be equivalent to $|\ |_p$. Namely, if $c = 1/|p| > 1$ equals $p^s, s > 0$, then $|\ | = |\ |_p^s$.

Now let's assume $|\ |$ is archimedean. We'll show that for positive integers $m, n > 1$, that $|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}$. Then if this common value is c, it will follow that $|m| = c^{\log m} = e^{\log c \cdot \log m} = m^{\log c}$ for natural numbers $m > 1$, and therefore that $|x| = |x|_\infty^{\log c}$ for all rational numbers x. Note that $c > 1$ because the valuation is archimedean, and so exceeds 1 for some natural number.

The proof of the claim is as follows. Write m in base n as $m = a_0 + a_1 n + \cdots + a_r n^r$ where $a_i \in \{0, 1, \ldots, n-1\}$ and $n^r \leq m < n^{r+1}$, so that $r \leq \frac{\log m}{\log n}$. Then $|a_i| = |1 + \cdots + 1| \leq a_i |1| \leq n$, so we get

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

If we plug in m^k instead of m, we get

$$|m|^k \leq n \left(1 + \frac{k \log m}{\log n}\right) |n|^{k\frac{\log m}{\log n}}$$

Taking k'th roots and letting $k \to \infty$ we get $|m| \leq |n|^{\frac{\log m}{\log n}}$ or $|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}$. By symmetry, we get the other inequality. □

Definition 1. *An exponential valuation v of K is a function $v : K^\times = K \backslash \{0\} \to \mathbb{R}$ such that*

(1) $v(xy) = v(x) + v(y)$.
(2) $v(x + y) \geq \min(v(x), v(y))$.

We an extend to all of K by defining $v(0) = \infty$. Note that $c^{-v(x)}$ for any $c > 1$ defines a nonarchimedean valuation of K.

We say v is a *discrete valuation* if $v(K)$ is a discrete subgroup of $\mathbb{R}$ (hence $\cong \mathbb{Z}$ as a group).

We say that a discrete valuation is *normalized* if $v(K) = \mathbb{Z}$, i.e. the smallest positive value of v is 1.

Example. $v_p(x) = -\log_p |x|_p$ defines a normalized discrete valuation. $v_p(x)$ is nothing but the highest power of p dividing x.

If v is a normalized discrete valuation of K, then we let $\mathfrak{o} = \{x \in K \mid v(x) \geq 0\}$ be the *valuation ring* of v, and $\mathfrak{p} = \{x \in K \mid v(x) \geq 1\}$ be the *prime* associated to v. It is easy to check that p is maximal and then $\mathfrak{o}/\mathfrak{p}$ is a field, the *residue field* of v.

Let $\pi \in \mathfrak{o}$ be any element of $\mathfrak{o}$ with $v(\pi) = 1$. Then for any $x \in K^\times$ we have $x = \pi^n y$ for some integer n and some y with $v(y) = 0$, i.e. $y \in \mathfrak{o}^\times$ is a unit of $\mathfrak{o}$. So $\mathfrak{o}$ is in fact a PID with unique maximal ideal $\mathfrak{p}$ which is principal, equal to (π). Such an element π is called a uniformizer of $\mathfrak{o}$ (or of v).

Such a ring $\mathfrak{o}$, which comes from a discrete valuation of a field K, is called a *discrete valuation ring*, or DVR for short.

2.2. **Completions.** We'll now construct the p-adic numbers.

Let $|\ |$ be an absolute value on a field K. We say a sequence $\{a_n\}$ of elements of K is a Cauchy sequence of for all $\epsilon > 0$, there is an N such that $m, n \geq N$ implies $|a_m - a_n| < \epsilon$. Recall that the field $\mathbb{R}$ is constructed from $\mathbb{Q}$ as the set of Cauchy sequences (for the usual archimedean valuation) modulo the null sequences, i.e. those which tend to zero. We will imitate that construction for an arbitrary absolute value.

Let

$$\mathcal{C} = \text{Cauchy sequences} = \{\{a_n\}_{n\in\mathbb{N}} \mid \forall \epsilon > 0, \exists N \text{ such that } m, n \geq N \Rightarrow |a_m - a_n| < \epsilon\}$$

and

$$\mathcal{M} = \text{Null sequences} = \{\{a_n\}_{n\in\mathbb{N}} \mid \forall \epsilon > 0, \exists N \text{ such that } m \geq N \Rightarrow |a_m| < \epsilon\}$$

Then $\mathcal{C}$ is a ring under componentwise addition and multiplication. The field K embeds inside $\mathcal{C}$ by taking $x \in K$ to the constant sequence $\{x, x, \dots\}$. The subset $\mathcal{M}$ is a maximal ideal of $\mathcal{C}$ (check!) and so $\mathcal{C}/\mathcal{M} = \widehat{K}$ is a field containing K, called the completion of K with respect to $|\ |$. We will make some observations before we describe the structure of $\widehat{K}$ a little more explicitly.

First note that the valuation extends to $\widehat{K}$ by defining $|\{a_n\}| = \lim_{n\to\infty} |a_n|$. The limit exists because we have from the triangle inequality that $|a_m| - |a_n| \leq |a_m - a_n|$ and similarly $-(|a_m| - |a_n|) \leq |a_m - a_n|$, so that $||a_m| - |a_n|| \leq |a_m - a_n|$. Therefore $\{|a_n|\}$ is a Cauchy sequence of real numbers, so it converges. Check that the extension satisfies the properties of a valuation. This extension is unique in the following sense: the valuation $|\ |$ makes K into a metric space, and for any metric space X, there is a unique metric space $\hat{X}$ which is complete and into which X embeds isometrically as a *dense* subspace. So the metric and hence the valuation on $\widehat{K}$ is forced.

From now on assume $|\ |$ is nonarchimedean, corresponding to an exponential valuation v. Let $\hat{v}$ be the extension of v to $\widehat{K}$ as above.

Lemma 2. *Let $\{a_n\}$ be a Cauchy sequence in K converging to an element different from 0. Then $\lim_{n\to\infty} |a_n| = |a_m|$ for m large enough.*

Proof. Let $0 < r = \lim_{n\to\infty} |a_n|$. Choose $\epsilon < r/2$. Let N be large enough such that $|a_m| > r - \epsilon$ for $m \geq N$ and also such that $|a_m - a_n| < \epsilon$ for $m, n \geq N$. Then $|a_m| > |a_n - a_m|$ and so $|a_n| = |a_m|$, for all $n \geq m \geq N$. So the sequence of $|a_n|$ is constant beyond $n = N$, and therefore equals the limit r. Hence $|a_m| = r = \lim_{n\to\infty} |a_n|$ for $m \geq N$. □

Corollary 1. *The value group $\hat{v}(\widehat{K})$ of $\widehat{K}$, equals that of K.*

18.786 Topics in Algebraic Number Theory
Spring 2010