UC Berkeley Math 254A
Problem Set 2

September 25, 2014

Last Updated: September 25, 2014. Please let me know if you find any typos.

We will discuss these questions in class on **Monday, Oct. 6th.**
Written solutions are due on **Wednesday, Oct. 8th.**

1 The Minkowski bound

In this section, you will prove the "classical" Minkowski bound:

Theorem. *Let K be a number field. Then any ideal class $[\mathfrak{a}] \in Cl_K$ contains an integral ideal $\mathfrak{b}$ of norm*

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

Prove the theorem above using the following three steps:

1. Consider the following subset of $K_{\mathbb{R}}$:

$$X := \{(z_\tau)_\tau \in K_{\mathbb{R}} \ : \ \sum_\tau |z_\tau| < t\}.$$

   Show that X is convex and centrally symmetric, and that the volume of X is $2^r \pi^s \frac{t^n}{n!}$. (**You can take the formula for the volume as given! See Neukirch Ch. III, §2, (2.15) for a proof.**)

2. Show that every non-trivial (integral) ideal $\mathfrak{a}$ of $\mathcal{O}_K$ contains a non-zero element a such that

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

   Hint: recall that

$$\frac{1}{n} \cdot \sum_\tau |z_\tau| \geq \left(\prod_\tau |z_\tau|\right)^{1/n}.$$

   Now proceed similarly to the proof of the "Key Lemma" we did in class.

3. Prove the theorem above. **Hint:** the proof should be essentially the same as the proof of the "weak" Minkowski bound which we proved in class, using (2) above.

4. Suppose that K is a number field and that $K \neq \mathbb{Q}$. Prove that $|d_K| > 1$.

5. Prove that $|d_K|$ tends to ∞ as $[K : \mathbb{Q}]$ tends to ∞.

2 Computing some class groups

Compute the class group of $\mathbb{Q}(\sqrt{D})$ for the following D:

$$5, -7, 6, -11, -23, 82, -30, 79.$$

3 The fundamental unit of real quadratic fields

Let K be a real quadratic field – that is, $K = \mathbb{Q}(\sqrt{D})$ where D is a positive square-free integer.

1. What is $\mu(K)$? What is the (rational) rank of $\mathcal{O}_K^\times$?

2. Suppose that $D \neq 1 \mod 4$, and let b be the smallest positive integer such that $a^2 - Db^2 = \pm 1$ for some $a \in \mathbb{Z}$. Prove that $a + b\sqrt{D}$ is the unique positive fundamental unit of K.

3. Find the fundamental unit explicitly for $D = 2, 3, 7$.

4. Can you find/prove an analogous statement when $D = 1 \mod 4$?

5. What happens to $\mu(K)$ resp. $\mathcal{O}_K^\times$ when $D < 0$? (try $D = -3$).

4 An approximation theorem for real embeddings

Let K be a number field. We say that K is **totally real** if every embedding $K \to \mathbb{C}$ has image contained in $\mathbb{R}$. Assume that K is totally real, and let $X = \mathrm{Hom}(K, \mathbb{C}) = \mathrm{Hom}(K, \mathbb{R})$ be the set of complex (hence real) embeddings of K. Let T be a non-empty, proper subset of X. Prove that there exists a unit $\epsilon \in \mathcal{O}_K^\times$ such that $0 < \tau\epsilon < 1$ for all $\tau \in T$ and $1 < \tau\epsilon$ for all $\tau \notin T$.

Hint: apply the Minkowski Lattice Point Theorem to an appropriately chosen convex and centrally symmetric domain in the trace-zero hyperplane of $\mathbb{R}^n$, to prove that this domain contains a non-trivial element of $\lambda(\mathcal{O}_K^\times)$

5 Basics of valuation theory

You don't need to turn in answers to the questions in this section. However, you should still solve all these problems independently. These questions will be included in our discussion on Oct. 6th.

Let K be a field. Let $\mathcal{O}$ be a subring of K which satisfied the following condition: for every $x \in K$, one has $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. Such a subring $\mathcal{O}$ is called a **valuation ring** of K.

1. Prove that $\mathcal{O}$ is normal.

2. Suppose that $\mathfrak{a}, \mathfrak{b}$ are ideals of $\mathcal{O}$. Prove that $\mathfrak{a} \subset \mathfrak{b}$ or $\mathfrak{b} \subset \mathfrak{a}$ (**hint:** do the case where $\mathfrak{a}$ and $\mathfrak{b}$ are principal first). Deduce that $\mathcal{O}$ is a local ring.

3. Let $v : K^\times \to K^\times/\mathcal{O}^\times$ be the canonical quotient map. Prove that $K^\times/\mathcal{O}^\times$ can be endowed with a total ordering $\leq$ such that $\mathcal{O} = \{0\} \cup \{x \in K^\times \ : \ v(x) \geq 0\}$, and that $\{0\} \cup \{x \in K^\times \ : \ v(x) > 0\}$ is the unique maximal ideal of $\mathcal{O}$.

4. Let $v : K^\times \to \Gamma$ be a surjective homomorphism onto a totally ordered abelian group Γ, such that $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in K^\times$ $(x \neq -y)$. Prove that $\mathcal{O}_v := \{0\} \cup \{x \in K^\times \ : \ v(x) \geq 0\}$ is a valuation ring of K.

Now let $\mathcal{O}_K$ be a Dedekind domain with fraction field K.

1. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Prove that the localization $\mathcal{O}_\mathfrak{p} := (\mathcal{O}_K)_\mathfrak{p}$ is a valuation ring of K, and that $K^\times/\mathcal{O}_\mathfrak{p}^\times$ is isomorphic to $\mathbb{Z}$ (as an ordered group).

2. Consider the map $v_\mathfrak{p} : K^\times \to K^\times/\mathcal{O}_\mathfrak{p}^\times \cong \mathbb{Z}$ induced by the order-preserving isomorphism from (1) above. Prove that for a given $a \in K^\times$, all but finitely many of the $v_\mathfrak{p}(a)$ are 0.

3. Given $a \in K^\times$, prove that one has the following decomposition of the fractional ideal $a \cdot \mathcal{O}_K$ into a product of primes

$$a \cdot \mathcal{O}_K = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a)}.$$