MATH 702: HOMEWORK #4

DUE WEDNESDAY, NOVEMBER 14, 2012

1. Minkowski's Lemma.

Suppose $n > 0$ is an integer. We suppose that B is a convex symmetric subset of $\mathbb{R}^n$ in the sense that if $b_1, b_2 \in B$, then B contains the line segment between b_1 and b_2 as well as $-b_1$. Recall that an additive subgroup L of $\mathbb{R}^n$ is a lattice if L is the free $\mathbb{Z}$-module generated by a basis $\{b_i\}_{i=1}^n$ of $\mathbb{R}^n$ over $\mathbb{R}$. A fundamental domain for the action of L on $\mathbb{R}$ is then the set

$$F = \{\sum_{i=1}^{n} r_i b_i : 0 \le r_i < 1\}.$$

Minkowski's Lemma states that if B contains a set U whose n-dimensional volume is well defined and larger than $2^n \mathrm{vol}(F) = 2^n \mathrm{vol}(\mathbb{R}^n/L)$, then there is a non-zero element of L in B. The proof consists of observing that the natural map $\frac{1}{2}B \to \mathbb{R}^n/L$ cannot be injective, so that $\frac{b_1}{2} \equiv \frac{b_2}{2}$ mod L for some distinct $b_1, b_2 \in B$. Then by the convexity of B, $\frac{b_1 - b_2}{2}$ is a non-zero element of $L \cap B$.

1. Suppose that $m \ge 1$ is an integer and that B contains a set U whose n-dimensional volume is well defined and larger than $m 2^n \mathrm{vol}(F)$. Show that the map $\frac{1}{2}B \to \mathbb{R}^n/L$ must have a fiber with at least $m+1$ elements.
2. With the assumptions of problem #1, show that $L \cap B$ contains at least m distinct non-zero elements.
3. Give examples to show that there are B of arbitrarily small volume such that $\#(L \cap B)$ is arbitrarily large. This shows that while one can give a lower bound on $\#(L \cap B)$ which increases with the volume of B, one cannot expect an upper bound on $\#(L \cap B)$ which depends on this volume.
4. **Extra Credit** Find the largest constant $f(m)$ depending on m alone such that for all n, B, L and F as in problem #1, one has $\#(L \cap B) \ge f(m)$. You should show by example that your $f(m)$ cannot be improved. Note that Problem #2 shows $f(m) \ge m$. What would happen if we allowed functions $f(m, n)$ which can depend both on m and n?

2. The strong approximation theorem for number fields

Let F be a number field, and let $S = \{| \ |_0, | \ |_1, \ldots, | \ |_s\}$ be a set of $s+1$ distinct normalized absolute values on F. Suppose $\epsilon > 0$ is a real constant, and that $\{x_i\}_{i=1}^s$ is a set of s elements of F. The strong approximation theorem says that there is an $x \in F$ such that $|x - x_i|_i < \epsilon$ for $1 \le i \le s$ and $|x|_v \le 1$ if $| \ |_v$ is a normalized absolute value on F which is not in S. For $z > 0$ a real number, let $B(z)$ be the set of all such x for which $|x|_0 < z$. Define $N(z)$ to be the number of elements of $B(z)$. (Here $B(z)$ and $N(z)$ depend on S, ϵ and $\{x_i\}_{i=1}^s$.)

5. Show that if $x \in B(z)$ then x lies in a fractional ideal $\mathcal{A}(z)$ which depends on z, and all of the archimedean absolute values of x are bounded by a function $b(z)$ of z.
6. Use problem #5 to show that if $x \in B(z)$, then x is a root of one of finitely many monic polynomials in $\mathbb{Q}[x]$ of degree n. Deduce that $N(z)$ is finite for all z.
7. Suppose $F = \mathbb{Q}$. Show that $N(z)$ is asymptotically linear and positive as a function of z in the sense that $\lim_{z \to +\infty} N(z)/z = \tau$ for some positive real constant τ. (Hint: Consider separately the cases in which $| \ |_0$ is archimedean and non-archimedean.)

8. **Extra Credit** Use the results in §1 about Minkowski's Theorem to prove that for all number fields F, one has $N(z) \geq \tau z + g(z)$ for some constant $\tau > 0$ and some function $g(z)$ such that $\lim_{z \to +\infty} g(z) = 0$.
9. **Research Problem** For all number fields F, can the statement in Problem #8 be sharpened to $\lim_{z \to +\infty} N(z)/z = \tau$?