MATH 620 EXERCISE SET 7, FALL 2016

1. A classical theorem of Siegel asserts that

$$\lim_{F} \frac{\log(h_F\, R_F)}{\log(|\mathrm{disc}_F|^{1/2})} = 1$$

as F ranges through all quadratic fields (so that $|\mathrm{disc}_F| \to \infty$). A well-known theorem of Estermann asserts that there are infinitely many integers $m \in \mathbb{Z}$ such that m^2+1 is square free. Use these two facts to show that there for every $\varepsilon > 0$, there are infinitely many real quadratic fields F satisfying

$$h_F > |\mathrm{disc}_F|^{1/2-\varepsilon}.$$

2. This problem provides a family of totally real fields of F of a given degree $n = [F:\mathbb{Q}]$ and $n-1$ units in $\mathscr{O}_F^\times$ which generate a subgroup of finite index in $\mathscr{O}_F^\times$.

Choose and fix $n-1$ mutually distinct integers $a_1,\dots,a_{n-1}$. For any integer m, let $g_m(x) \in \mathbb{Z}[x]$ be the polynomial

$$f_m(x) = (x-m)\prod_{i=1}^{n-1}(x-a_i) + 1.$$

Clearly $f_m(a_i) = 1$ for all $i = 1,\dots,n-1$. Show that there exists a positive integer M_0 such that for all m with $|m| \geq M_0$ the following statements hold

(1) The polynomial $f_m(x)$ has n mutually distinct *real* roots $\alpha_m^{(1)},\dots,\alpha_m^{(n)}$. Moreover after suitably reordering these roots, we have $|\alpha_m^{(i)} - a_i| \leq 1/4$ for all $i = 1,\dots,n-1$, and $|\alpha_m^{(n)} - m| \leq 1/4$.

(2) There exists constants $b_1,\dots,b_{n-1} \in \mathbb{Q}$ such that

$$\lim_{|m|\to\infty} m\cdot(\alpha_m^{(i)} - a_i) = b_i \qquad \forall i = 1,\dots,n-1$$

and there exists a constant C such that

$$|m\cdot(\alpha_m^{(n)} - m)| \leq C$$

(3) $f_m(x)$ is an irreducible monic polynomial of degree n in $\mathbb{Z}[x]$. So $F_m := \mathbb{Q}(\alpha_m^{(1)}) \cong \mathbb{Q}[x]/(f_m(x))$ is a totally real number field of degree n.

(4) For each $i = 1,\dots,n-1$, $a_i - \alpha_m^{(1)} \in \mathscr{O}_{F_m}^\times$.

(5) The $n-1$ units $a_1 - \alpha_m^{(1)}, a_2 - \alpha_m^{(1)},\dots,a_{n-1} - \alpha_m^{(1)}$ generate a subgroup of finite index of $\mathscr{O}_{F_m}^\times$.

3. Let $a > 0$ be a positive real number. Let K be a number field. $f : \sigma_{K,f} \to \mathbb{Z}$ be an integer-valued function on the set $\sigma_{K,f}$ of all finite places of K such that f vanishes outside a finite subset of $\sigma_{K,f}$. Let $B(a,f)$ be the subset of $\mathbb{A}_K$ consisting of all K-adeles $(x_v)_{v\in\Sigma_K}$ such that $\mathrm{ord}_v(x_v) \geq f(v)$ for all $v \in \Sigma_{K,f}$, and $\sum_{v\in\Sigma_{K,\infty}} |x_v|_v \leq a$.

(a) Compute the volume of $B(a,f)$ with respect to the Haar measure on $\mathbb{A}_K$ such that $\mathbb{A}_K/K$ has volume 1.

(b) Let $n := [K : \mathbb{Q}]$ and let $C_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}$ be the Minkowski constant attached to K, which depends only on the degree and the number of complex places of K. Use (a) to prove the following theorem of Minkowski: in any ideal class of $\mathscr{O}_K$, there exists an ideal I such that

$$\mathbf{N}(I) \le C_K \, |\mathrm{disc}_K|^{1/2}.$$

(c) Use Minkowski's theorem to show that

$$|\mathrm{disc}_K| \ge \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)!} \ge 3$$

for all $n = [K : \mathbb{Q}] \ge 2$.

(d) Use Minkowski's theorem to show that there exists positive constant c such that

$$\log(|\mathrm{disc}_K|) \ge c \cdot [K : \mathbb{Q}].$$

for every number field K.

4. (Artin) Let $f(x) = x^5 - x + 1$.

(a) Show that $f(x)$ is irreducible over $\mathbb{Q}$.

(b) Let α be a root of $f(x)$, and let $F = \mathbb{Q}(\alpha)$. Determine the number of real and complex places of F.

(c) It is a fact that the discriminant of the polynomial $f(x)$ is $2869 = 19 \cdot 151$. (The discriminant of a polynomial can be expressed as a polynomial of the coefficients of the polynomial.) Use this fact to show that $\mathscr{O}_F = \mathbb{Z}[\alpha]$

(d) Use Minkowski's theorem to show that $\mathscr{O}_F$ is a principal ideal domain.

(e) Determine the discriminant $\mathrm{disc}_F \in \mathbb{Z}$.

Remark. The classical definition of the discriminant d_K of a number field K is the following. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis of $\mathscr{O}_F$. Let $\sigma_1, \ldots, \sigma_n$ be the set of all embeddings of K into $\overline{\mathbb{Q}}$. Then

$$\mathrm{disc}_K := \det(\sigma_i(x_j))^2 = \det(\mathrm{Tr}_{K/\mathbb{Q}}(x_i \cdot x_j)) \in \mathbb{Z}.$$

This definition is independent of the chose of $\mathbb{Z}$-basis $(x_1, \ldots, x_n)$ of $\mathscr{O}_K$. So the discriminant disc_K is a well-defined integer, not an ideal of $\mathbb{Z}$. In comparison, the ideal $\mathrm{disc}_{K/\mathbb{Q}}$ in $\mathbb{Z}$ we defined in class is $\mathrm{disc}_K \cdot \mathbb{Z}$.