Math 4803/8803 Homework 10

Due at the beginning of class on Wednesday, November 4.

1. Let H be a lattice in $\mathbf{R}^n$ and let H' be a subgroup of H.

a) Prove that H' is a discrete subgroup of $\mathbf{R}^n$.

b) Prove that H' is a lattice in $\mathbf{R}^n$ if and only if $[H : H'] < \infty$.

c) If H' is a lattice, show that $v(H') = [H : H']\, v(H)$.

2. Let $K = \mathbf{Q}(\sqrt{10})$, let $\mathfrak{a}$ be the ideal $(6, \sqrt{10})$ in $\mathscr{O}_K = \mathbf{Z}[\sqrt{10}]$, and let $\sigma\colon K \to \mathbf{R}^2$ be the canonical embedding.

a) Find bases for the lattices $\sigma(\mathscr{O}_K)$ and $\sigma(\mathfrak{a})$.

b) Compute $\mathrm{N}(\mathfrak{a})$, and use this to prove that $\mathfrak{a}$ is prime but not principal.

c) Use (a) to calculate the volumes $v(\sigma(\mathscr{O}_K))$ and $v(\sigma(\mathfrak{a}))$ "by hand". Verify the formulas

$$v(\sigma(\mathscr{O}_K)) = 2^{-r_2}|D_K|^{1/2} \quad \text{and} \quad v(\sigma(\mathfrak{a})) = 2^{-r_2}|D_K|^{1/2}\,\mathrm{N}(\mathfrak{a})$$

where r_2 is the number of pairs of complex embeddings of K.

d) Find a nonzero element $x \in \mathfrak{a}$ satisfying

$$|\,\mathrm{N}_{K/\mathbf{Q}}(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\,|D_K|^{1/2}\ \mathrm{N}(\mathfrak{a})$$

where $n = [K : \mathbf{Q}]$

3. In this problem, you'll use Minkowski's theorem to prove[1] the *four square theorem* that every nonnegative integer can be written as a sum of four square integers $a^2 + b^2 + c^2 + d^2$.

a) Verify Euler's identity (e.g. using a computer, or quaternions) that

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2)& \\ = (ax - by - cz - dw)^2 + (ay + bx + cw - dz)^2& \\ + (az - bw + cx + dy)^2 + (aw + bz - cy + dx)^2.&\end{aligned}$$

Use this to show that it suffices to prove that all *prime* numbers are a sum of four squares.

b) Let $B(0, r)_+$ be the open ball of radius r in $\mathbf{R}^4$. Show that its volume is

$$\mu\big(B(0, r)_+\big) = \frac{\pi^2}{2}\, r^4.$$

c) For a prime p, prove that there exist $r, s \in \mathbf{Z}$ such that $r^2 + s^2 + 1 \equiv 0 \pmod{p}$. [Rewrite the equation as $r^2 \equiv -(s^2 + 1) \pmod{p}$. How many

[1] This proof is well known, so no looking online!

values do the right and left hand sides of this equation take for varying $r, s \in \mathbf{F}_p$?]

Fix a prime p, and choose $r, s \in \mathbf{Z}$ such that $r^2+s^2+1 \equiv 0 \pmod{p}$. Let $H \leq \mathbf{R}^4$ be the lattice spanned by the columns of the matrix

$$M = \begin{bmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

d) For $x \in H$ prove that $|x|^2$ is a sum of four square integers and $|x|^2 \equiv 0 \pmod{p}$.

e) Use Minkowski's theorem to prove that there exists a nonzero lattice vector $x \in B(0, \sqrt{2p})_+ \cap (H \setminus \{0\})$.

f) Use (e) to show that there exists $x \in H$ with $|x|^2 = p$. Conclude that the four square theorem is true.