MATHEMATICS IV HONOURS 2017
ALGEBRAIC NUMBER THEORY
ASSIGNMENT 2

GUS LEHRER

Question 1. Let $B(r) = \{x \in \mathbb{R}^n \mid x.x \leq r^2\}$ be the r-ball in $\mathbb{R}^n$, endowed with the Euclidean metric.

(1) Show that $\mu(B(r)) = \mathrm{Vol}(B(r)) = \omega_n r^n$, where

$$\omega_n = \int_0^{2\pi} \int_0^1 \omega_{n-2}(\sqrt{1-r^2})^{n-2} r dr d\theta = \frac{2\pi\omega_{n-2}}{n}.$$

(2) Deduce that

$$\omega_n = \begin{cases} \frac{\pi^m}{m!} \text{ if } n = 2m \\ \frac{2^{m+1}\pi^m}{n(n-2)(n-4)...3.1} \text{ if } n = 2m+1. \end{cases}$$

Question 2. Let L be an integer lattice in $\mathbb{R}^n$; that is, L is a free abelian group of rank n such that $L \subseteq \mathbb{Z}^n \subset \mathbb{R}^n$.

Suppose we fix $d := \mu(\mathbb{R}^n/L)$. Show that there is a constant $c(n,d) = 4\sqrt[n]{\frac{d^2}{\omega_n^2}}$ such that L contains a point x with $x.x \leq c(n,d)$.

Question 3. Maintain the notation of the last question. Consider the homomorphism $\phi : L \to \frac{\mathbb{Z}}{\mathbb{Z}x.x}$ given by $\phi(y) = x.y(\mod x.x)$. Let $L_0 = \ker(\phi)$.

(1) Show that L_0 is a sublattice of L, of index at most $x.x$.
(2) Show that L_0 has a decomposition $L_0 = \mathbb{Z}x \oplus x^\perp$, where $x^\perp = \{y \in L \mid x.y = 0\}$.
(3) Deduce by induction on n that there are only finitely many possibilities for L_0, and hence for L.
(4) Interpret this result as: there are finitely many isomorphism classes of positive definite forms over $\mathbb{Z}$ with given discriminant. [This is the Eisenstein-Hermite theorem]

Question 4. Use Proposition 4 (quantitative version) from lectures to prove that $\mathbb{Q}(\sqrt{d})$ has class number 1 in the following cases: $d = 2, 3, 5, 13, -1, , 2, -3, -7$.

Question 5. Let $K = \mathbb{Q}(\sqrt{-k}$, where $k > 0$ is a square free integer, and A its ring of integers.

(1) If $\mathfrak{p}$ is a prime ideal of A, and p is the unique rational prime divisor of $\mathfrak{p}$, then $\mathfrak{p}$ is principal if and only if:

$$* \text{ Either } \mathfrak{p} = (p) \text{ or } N(a) = p \text{ for some } a \in A.$$

(2) Deduce that if the class number of K is 1, then $k = 1$ or $k =$ a prime. Deduce further that if $k \equiv 2$ or 3 (mod 4), then $k = 1$ or 2.
(3) Show that if $*$ holds for all primes $p < \frac{2}{\pi}\sqrt{d}$, then the class number of K is 1.

Date: October, 2017.

Question 6. Let $\alpha = \sqrt[3]{2}$ be the real cube root of 2, and let $K = \mathbb{Q}(\alpha)$.

(1) Show that the class number of K is 1, i.e. that A is a PID.
(2) Show that the ring of integers $A = \mathbb{Z}[\alpha]$.
(3) Show that the units in A are uniquely expressible as $\pm(1 + \alpha + \alpha^2)^k$ with $k \in \mathbb{Z}$.

School of Mathematics and Statistics, University of Sydney, N.S.W. 2006, Australia
E-mail address: gustav.lehrer@sydney.edu.au