MAT415 Assignment 4 Solutions

December 4, 2020

Problem 1 (Exercise 3.8 on Pg. 62). *Let $\Lambda \subset \mathbb{R}^n$ be a rank n lattice, and let $S \subset \mathbb{R}^n$ be a compact, convex, and symmetric set. If*

$$\mathrm{vol}(S) \geq 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda),$$

prove that S contains a nonzero element of Λ.

Solution. If $\mathrm{vol}(S) > 2^n\mathrm{vol}(\mathbb{R}^n/\Lambda)$, Minkowski's convex body theorem applies directly. Suppose that $\mathrm{vol}(S) = 2^n\mathrm{vol}(\mathbb{R}^n/\Lambda)$. The key step in the proof of the Minkowski body theorem now fails. Indeed, it is a priori possible for the map T to be injective! To circumvent this, we will approximate S by a sequence of convex bodies to which Minkowski's theorem applies. Let $\epsilon_1, \epsilon_2, \ldots$ be a sequence of positive real numbers tending to 0 and consider the sets $S_r = (1+\epsilon_r)S$. We have:

$$\mathrm{vol}(S_r) = (1+\epsilon_r)^n\mathrm{vol}(S) > \mathrm{vol}(S) = 2^n\mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Now, we can apply the non-compact case of Minkowski's convex body theorem to S_r to obtain a non-zero element $\lambda_r \in S_r \cap \Lambda$. For each r, let s_r be the closest point to λ_r in S (it exists because S is compact and the distance between s_r and λ_r tends to 0 because S_r is obtained from S by scaling factors which tend to 1). Then, since S is compact, we can restrict r to a subsequence and assume that s_r converges to $s^* \in S$. Then we also have that λ_r converges to s^* on that subsequence. But $\lambda_r \in \Lambda$ is a convergent subsequence in a discrete set and therefore it is eventually constant. This means that $0 \neq s^* \in S \cap \Lambda$ as required. □

Problem 2 (Exercise 3.10 on Pg. 64). *Let $S \in \mathbb{R}^n$ be the subset consisting of points*

$$e = (a_1, \ldots, a_{r_1}, x_1, y_1, \ldots, x_{r_2}, y_{r_2}),$$

which satisfy

$$f(e) = |a_1| + \cdots + |a_{r_1}| + 2\left(\sqrt{x_1^2+y_1^2} + \cdots + \sqrt{x_{r_2}^2+y_{r_2}^2}\right) \leq n.$$

Show that S is convex.

Solution. Let $0 \leq t \leq 1$ and

$$s = (a_1, \ldots, a_{r_1}, x_1, y_1, \ldots, x_{r_2}, y_{r_2}),$$

$$s' = (a'_1, \ldots, a'_{r_1}, x'_1, y'_1, \ldots, x'_{r_2}, y'_{r_2})$$

be two elements in S. Then $ts+(1-t)s' = (ta_1+(1-t)a'_1, \ldots, ta_{r_1}+(1-t)a'_{r_1}, tx_1+(1-t)x'_1, ty_1+(1-t)y'_1, \ldots, ty_{r_2}+(1-t)y'_{r_2})$. Note that for all i, we have:

$$\left|ta_i + (1-t)a'_i\right| \leq t|a_i| + (1-t)|a'_i|,$$

by the triangle inequality. Furthermore, we have:

$$\begin{aligned}\sqrt{(tx_i + (1-t)x_i')^2 + (ty_i + (1-t)y_i')^2} &= ||(tx_i + (1-t)x_i', ty_i + (1-t)y_i')||_2 \\ &\leq t||(x_i, y_i)||_2 + (1-t)||(x_i', y_i')||_2 \\ &\leq t\sqrt{x_i^2 + y_i^2} + (1-t)\sqrt{x_i' + y_i'},\end{aligned}$$

again we use the triangle inequality on the 2-norm on $\mathbb{R}^2$. Therefore, we find that $f(ts+(1-t)s') \leq tf(s) + (1-t)f(s') \leq tn + (1-t)n = n$ and so $ts + (1-t)s'$. We conclude that S is convex. $\square$

Problem 3 (Exercise 3.18 on Pg. 68)**.** *Let p be a prime number.*

(a) Let u be an integer relatively prime to p, and define $\Lambda \subset \mathbb{Z}^2$ to be the lattice in $\mathbb{R}^2$ consisting of all pairs $(a, b) \in \mathbb{Z}^2$ such that $b \equiv au \pmod p$. Show that $\operatorname{covol}(\Lambda) = p$.

(b) Let $\Lambda \subset \mathbb{Z}^4$ be the lattice in $\mathbb{R}^4$ consisting of all $(a, b, c, d) \in \mathbb{Z}^4$ such that:

$$c \equiv ua + vb \quad d \equiv ub - va \pmod p.$$

Show that $\operatorname{covol}(\Lambda) = p^2$.

(c) Show that the volume of a ball of radius r in $\mathbb{R}^4$ is $\pi^2 r^4/2$.

Solution. (a) The vectors $(0, p)$ and $(1, u)$ form a basis for Λ. The volume of the fundamental domain is thus equal to $\det\begin{pmatrix}1 & u \\ 0 & p\end{pmatrix} = p$.

(b) The vectors $(1, 0, u, -v), (0, 1, v, u), (0, 0, p, 0), (0, 0, 0, p)$ form a basis for Λ. The volume of the fundamental domain is thus equal to

$$\det\begin{pmatrix}1 & 0 & u & -v \\ 0 & 1 & v & u \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p\end{pmatrix} = p^2.$$

(c) There are many proofs of this, here is a quick one (from Wikipedia) that uses cylindrical coordinates to relate the volume of the ball of radius r in $\mathbb{R}^4$, $V_4(r)$, to the radius of the ball of radius r in $\mathbb{R}^2$, $V_2(r)$. For this, we think of the coordinates $(x, y, R\cos(\theta), R\sin(\theta)$ on $\mathbb{R}^4$ and we apply Fubini:

$$\begin{aligned}V_4(r) &= \int_0^{2\pi}\int_0^r V_2\left(\sqrt{r^2 - R^2}\right) R\, dR d\theta \\ &= 2\pi V_2(1)\int_0^r (r^2 - R^2) R\, dR \\ &= 2\pi V_2(1)\left[\frac{r^2R^2}{2} - \frac{R^4}{4}\right]_{R=0}^{R=r} \\ &= \frac{2\pi V_2(1) r^4}{4} \\ &= \frac{\pi^2 r^4}{2}.\end{aligned}$$

$\square$

Problem 4 (Exercise 3.40 on Pg. 79)**.** *If K is a number field, show that the sign of Δ_K is $(-1)^{r_2}$.*

Solution. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for K. Let $\sigma_1, \sigma_2 \ldots, \sigma_{r_1}$ be real embeddings of K and let $\sigma_{r_1+1}, \sigma_{r_1+2}, \ldots, \sigma_{r_1+2r_2-1}, \sigma_{r_1+2r_2}$ be the complex embeddings of K arranged so that $\sigma_{r_1+2i-1} = \overline{\sigma_{r_1+2i}}$. Now, taking the complex conjugate we find:

$$\overline{\det(\sigma_i(\alpha_j))} = \det(\overline{\sigma_i}(\alpha_j)) = (-1)^{r_2}\det(\sigma_i(\alpha_j)),$$

since we are transposing the last r_2 pairs of rows. As a result, $\det(\sigma_i(\alpha_j))$ is real if r_2 is even and purely imaginary (that is on the imaginary line) if r_2 is odd. It follows that $\Delta_K = \det(\sigma_i(\alpha_j))^2$ is positive if r_2 is even and negative if r_2 is odd. Thus, the sign of Δ_K is $(-1)^{r_2}$. □

Problem 5 (Exercise (3) on Pg. 83)**.** *Same as Problem 1.*

Problem 6 (Exercise (10) on Pg. 84)**.** *Let $K = \mathbb{Q}(\sqrt{223})$.*

(a) Find the group of units of K.

(b) Show that the ideal class group of $\mathcal{O}_K$ is cyclic of order 3.

Solution. (a) Since K is a real quadratic field, we know by Dirichlet's unit theorem that $\mathcal{O}_K^* \cong \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$, for some fundamental unit ε of K. It thus suffices to find a fundamental unit ε of K. The continued fraction expansion of $\sqrt{223}$ is $[14, \overline{1, 13, 1, 28}]$ and the period of the fraction is 4. We compute $(p_4, q_4) = (224, 15)$ and conclude that we can take

$$\varepsilon = 224 + 15\sqrt{223}.$$

(b) Note that $223 \not\equiv 1 \pmod 4$. Therefore $\mathbb{Z}[\sqrt{223}]$ is the rings of integers in $\mathbb{Q}(\sqrt{223})$. The discriminant is 892 and the norm form is $N(a + b\sqrt{-14}) = a^2 - 223b^2$. We will use Minkowski's bound. Recall that the Minkowski bound is given by:

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

In our case, $M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^0\sqrt{892} \sim 14.93$. We thus factor $(2), (3), (5), (7), (11), (13)$.

$$\begin{aligned}
(2) &= (2, \sqrt{223}+1)^2 = \mathfrak{p}_2^2 \\
(3) &= (3, \sqrt{223}+1)(3, \sqrt{223}+2) = \mathfrak{p}_3\,\mathfrak{p}_3' \\
(5) &= \mathfrak{p}_5 \\
(7) &= \mathfrak{p}_7 \\
(11) &= (11, \sqrt{223}+5)(11, \sqrt{223}+6) = \mathfrak{p}_{11}\,\mathfrak{p}_{11}' \\
(13) &= \mathfrak{p}_{13}
\end{aligned}$$

Therefore, the class group is generated by $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_{11}$. Now, let's note that we have two interesting elements in $\mathcal{O}_K$, namely $15 + \sqrt{223}$ and $16 + \sqrt{223}$, which respectively have norm 2 and 33. Noting that $15 + \sqrt{223} = (1 + \sqrt{223}) + 7 \cdot 2$ we see that $\mathfrak{p}_2 = (15 + \sqrt{223})$. Thus, $\mathfrak{p}_2$ is trivial in the class group. It is also immediate that $(16 + \sqrt{223}) = \mathfrak{p}_3\,\mathfrak{p}_{11}$. Thus, the class group is generated by $[\mathfrak{p}_3]$.

To find the order of $\mathfrak{p}_3$, we look for another element of small norm. Notice that $-14+\sqrt{223}$ has norm -27. Furthermore, $(-14+\sqrt{223}) \subset \mathfrak{p}_3$ and since 3 does not divide $-14+\sqrt{223}$ in $\mathcal{O}_K$, we must have $(-14+\sqrt{223}) = (\mathfrak{p}_3)^3$. Thus, $[\mathfrak{p}_3]$ has order 1 or 3.

To show that $[\mathfrak{p}_3]$ has order 3, we need to show that $\mathfrak{p}_3$ is not principal. We proceed by contradiction. Suppose that $\mathfrak{p}_3$ were principal and write $\mathfrak{p}_3 = (\gamma)$. We have $\mathfrak{p}_3^3 = (\beta)$ where $\beta = -14+\sqrt{223}$ and from the description of units in part (a), we have:

$$\mathfrak{p}_3^3 = (\beta) = (\gamma^3),$$

and thus

$$\pm\varepsilon^m\beta = \gamma^3$$

for some $m \in \mathbb{Z}$ and for $\varepsilon = 224 + 15\sqrt{223}$. Without loss of generality, we may assume that $m = 0, 1, 2$ after multiplying by an appropriate power of ε^3. We conclude that there is at least one element of the list $\pm\beta, \pm\varepsilon\beta, \pm\varepsilon^2\beta$ which is a cube in $\mathcal{O}_K$. There are now a couple of ways to proceed, with the general idea being to find a homomorphism into a field where we can tell which elements are cubes or not. Here's the very clever solutions that quite a few students found! By Kummer's factorisation theorem, we have a homomorphism:

$$\pi\colon \mathcal{O}_K \to \mathcal{O}_K/5\mathcal{O}_K = \mathbb{F}_{25} = \mathbb{F}_5[\sqrt{3}].$$

This homomorphism sends $\pi(a + b\sqrt{223}) = \overline{a} + \overline{b}\sqrt{3}$, where $\overline{a}, \overline{b}$ are the reductions of a and b modulo 5. In particular, it sends ε to -1, which is a cube! Therefore, if we show that the element $\pi(\beta) = 1 + \sqrt{3} \in \mathbb{F}_5[\sqrt{3}]$ is not a cube, then none of the elements $\pm\beta, \pm\varepsilon\beta, \pm\varepsilon^2\beta$ can be cubes in $\mathcal{O}_K$.

Checking that $1+\sqrt{3}$ is not a cube in $\mathbb{F}_5[\sqrt{3}]$ is a finite computation. Either compute the cubes of the 25 elements of $\mathbb{F}_{25}[\sqrt{3}]$ and verify that $1+\sqrt{3}$ is not part of the list. Or notice that any non-zero cube a^3 in $\mathbb{F}_5[\sqrt{3}]$ must satisfy $(a^3)^8 = 1$ and calculate that $(1+\sqrt{3})^8 = 2+\sqrt{3} \neq 1 \in \mathbb{F}_5[\sqrt{3}]$.

Therefore, we have our contradiction and we conclude that the ideal class group of $\mathcal{O}_K$ is cyclic of order 3.

$\square$

Problem 7 (Exercise (11) on Pg. 85). *Which of the following Diophantine equations have integer solutions?*

(a) $X^2 - 223Y^2 = \pm 11$.

(b) $X^2 - 223Y^2 = \pm 11^3$.

(c) $X^2 - 223Y^2 = \pm 11^{19}$.

Solution. We use the notation of Problem 6. Let $K = \mathbb{Q}(\sqrt{223})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{223}]$ denotes its ring of integers.

(a) A solution to the equation $X^2 - 223Y^2 = \pm 11$ would imply the existence of a principal ideal in $\mathcal{O}_K$ having norm 11. In particular, this would mean that $[\mathfrak{p}_{11}]$ and thus $[\mathfrak{p}_3]$ was trivial in the ideal class group of K. This would imply that the ideal class group of K is trivial which would contradicts Problem 6. Therefore, the Diophantine equation $X^2 - 223Y^2 = \pm 11$ has no integer solutions.

(b) By Problem 6, we know that the ideal $\mathfrak{p}_{11}^3$ is principal. Let's say $(\gamma) = \mathfrak{p}_{11}^3$. Then, $N(\gamma) = \pm 11^3$, and so there is an integer solution to the Diophantine equation $X^2 - 223Y^2 = \pm 11^3$. Note that reducing the equation $X^2 - 223Y^2 = 11^3$ modulo 4 gives $X^2 + Y^2 = 3 \pmod 4$ which does not have a solution. Thus, in fact, $N(\gamma) = -11^3$ and only $X^2 - 223Y^2 = -11^3$ has integer solutions.

(c) By Problem 6, $[\mathfrak{p}_{11}]^8[\mathfrak{p}'_{11}]^8[\mathfrak{p}_{11}]^3 = [(1)]$ in the ideal class group. In particular, the ideal $\mathfrak{p}_{11}^{11}\,\mathfrak{p}'^{8}_{11}$ is principal. Let's say $(\gamma) = \mathfrak{p}_{11}^{11}\,\mathfrak{p}'^{8}_{11}$. Then $N(\gamma) = \pm 11^{19}$. Therefore, there is an integer solution to the Diophantine equation $X^2 - 223Y^2 = \pm 11^{19}$. For the same reason as in (b), we must in fact have $N(\gamma) = -11^{19}$ and only $X^2 - 223Y^2 = -11^{19}$ has integer solutions.

$\square$