Math 129 Problem Set 7

Lev Kruglyak

March 27, 2022

Problem 5.2. Let Λ be an n-dimensional lattice in $\mathbb{R}^n$ and let $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_n\}$ be any two $\mathbb{Z}$-bases for Λ. Prove that the absolute value of the determinant formed by taking the v_i as the rows is equal to the one formed from the w_i. This shows that $\mathrm{vol}(\mathbb{R}^n/\Lambda)$ can be defined unambiguously.

Let $T_v : \mathbb{R}^n \to \mathbb{R}^n$ be the invertible linear transformation which takes the unit vector e_i to v_i. Similarly construct $T_w : \mathbb{R}^n \to \mathbb{R}^n$. Then the determinants in question are equal to $|\det T_v|$ and $|\det T_w|$. Since w, v are $\mathbb{Z}$-bases for Λ, we know that $T_v(\mathbb{Z}^n) = T_w(\mathbb{Z}^n) = \Lambda$. Then $T_w \circ T_v^{-1} : \Lambda \to \Lambda$ is an invertible $\mathbb{Z}$-linear map, so $|\det T_w \circ T_v^{-1}| = 1$. However by elementary properties of the determinant, $|\det T_w \circ T_v^{-1}| = |\det T_w|/|\det T_v|$ so $|\det T_v| = |\det T_w|$ as desired.

Problem 5.3. Let Λ be as in the previous exercise and let M be any n-dimensional sublattice of Λ. Prove that

$$\mathrm{vol}(\mathbb{R}^n/M) = |\Lambda/M| \cdot \mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Let T be an invertible linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ with $T(\mathbb{Z}^n) = \Lambda$. Similarly let $H : \mathbb{R}^n \to \mathbb{R}^n$ be an invertible linear transformation with $H(\Lambda) = M$. Then $|\det H \circ T| = |\det H||\det T|$, however $(H \circ T)(\mathbb{Z}^n) = M$ so $|\det(H \circ T)| = \mathrm{vol}(\mathbb{R}^n/M)$. Similarly $|\det T| = \mathrm{vol}(R^n/\Lambda)$, so it suffices to show that $|\det H| = |\Lambda/M|$. Note that by Problem 2.27b, there is a basis $\beta_1, \ldots, \beta_n$ of Λ such that $d_1\beta_1, \ldots, d_n\beta_n$ is a basis for M. Then clearly the determinant of H is equal to $d_1 \cdots d_n$. Similarly, $\Lambda/M = (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots (\mathbb{Z}/d_n\mathbb{Z})$ so $|\Lambda/M| = d_1 \cdots d_n$. This concludes the proof.

Problem 5.4. Prove that the subset of $S \subset \mathbb{R}^n$ defined by the inequalities

$$|x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n$$

is convex.

First we'll show that S is midpoint convex. Suppose $x, y \in S$. We claim that $\frac{x+y}{2} \in S$. First, note that by the triangle inequality on $\mathbb{R}$ we have $\left|\frac{x_i+y_i}{2}\right| \leq \frac{|x_i|+|y_i|}{2}$. Similarly, using the triangle inequality on $\mathbb{R}^2$, we have

$$\sqrt{\left(\frac{x_i + y_i}{2}\right)^2 + \left(\frac{x_{i+1} + y_{i+1}}{2}\right)^2} \leq \frac{1}{2}\sqrt{x_i^2 + x_{i+1}^2} + \frac{1}{2}\sqrt{y_i^2 + y_{i+1}^2}.$$

Adding the inequalities for x and y together, and using the triangle inequalities, we thus get,

$$\sum_{i=1}^{r}\left|\frac{x_i+y_i}{2}\right|+2\sum_{\substack{i=r+1\\j=r+2}}^{n}\sqrt{\left(\frac{x_i+y_i}{2}\right)^2+\left(\frac{x_j+y_j}{2}\right)^2}\le$$

$$\frac{1}{2}\left(\sum_{i=1}^{r}|x_i|+|y_i|+2\sum_{\substack{i=r+1\\j=r+2}}^{n}\sqrt{x_i^2+x_j^2}+\sqrt{y_i^2+y_j^2}\right)\le n$$

So S is midpoint convex. Now suppose $\theta = tx+(1-t)y$ is some convex combination for $t\in[0,1]$. By taking successive midpoints of x, y, we can construct a sequence of elements of S which converges to θ. Since S is a closed set, θ must thus be in S as well. So S is convex.

Problem 5.5. Prove by induction that

$$\frac{n^n}{n!}\ge 2^{n-1}.$$

Use this to show that $|\Delta_K|\ge 4^{r-1}\pi^{2s}$, and that $|\Delta_K|>1$ whenever $K\ne\mathbb{Q}$.

The base case of $n=1$ is clear, since $1\ge 1$. Now suppose the inequality works for $n-1$ for some $n\ge 2$. Then

$$2^{n-1}\le n\cdot 2^{n-2}\le\frac{n(n-1)^{(n-1)}}{(n-1)!}\le\frac{n\cdot n^{(n-1)}}{(n-1)!}\le\frac{n^n}{n!}.$$

Then by Corollary 5.2 we have

$$\sqrt{|\Delta_K|}\ge\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s\ge 2^{r+2s-1}\frac{\pi^s}{2^{2s}}=2^{r-1}\pi^s.$$

Thus $|\Delta_K|\ge 4^{r-1}\pi^{2s}$. Note that for integers $r,s\ge 0$, $4^{r-1}\pi^{2s}\ge 1$, with equality occurring only if $(r,s)=(1,0)$. This means that $n=1$, so the only number field satsfying this is $K=\mathbb{Q}$. Thus if $K\ne\mathbb{Q}$, we have $|\Delta_K|>1$.

Problem 5.6. Show that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$ is a principal ideal domain when $m=2,3,5,6,7,173,293$, or 437.

Recall that the discriminant of a quadratic number field $\mathbb{Q}[\sqrt{m}]$ is given by

$$\Delta_{\mathbb{Q}[\sqrt{m}]}=\begin{cases}4m & m\equiv 2,3 \mod 4\\ m & m\equiv 1 \mod 4\end{cases}$$

Also for every ideal class of $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, there is some ideal J with

$$\|J\|\le\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|\Delta_{\mathbb{Q}[\sqrt{m}]}|}=\frac{1}{2}\sqrt{|\Delta_{\mathbb{Q}[\sqrt{m}]}|}=\lambda(m).$$

Calculating this Minkowski bound for $m=2,3,5$, we get $\lambda(2)\approx 1.41$, $\lambda(3)\approx 1.73$, $\lambda(5)\approx 1.12$. In all these cases, every ideal class in $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$ contains an ideal of norm 1, so every ideal class is principal. For $m = 7$, we have $\lambda(7) \approx 2.29$. All ideal classes containing $\|J\| = 1$ are principal so we only need to consider ideal classes containing $\|J\| = 2$. It suffices to only look at prime ideals with norm less than or equal to 2.

Note that $2\mathcal{O}_{\mathbb{Q}[\sqrt{7}]} = (2, 1+\sqrt{7})$ since $x^2 - 7 \equiv x^2 + 1 \equiv (x+1)^2 \mod 2$. Then $\|(2, 1+\sqrt{7})\| = 2$ and the ideal is prime. However we also have the factorization $2 = (3+\sqrt{7})(3-\sqrt{7})$. Note that

$$\frac{3+\sqrt{7}}{3-\sqrt{7}} = \frac{(3+\sqrt{7})^2}{2} = 8 + 3\sqrt{7} \in \mathcal{O}^{\times}_{\mathbb{Q}[\sqrt{7}]}$$

So $(3+\sqrt{7}) = (3-\sqrt{7}) = \mathfrak{p}$ and hence every ideal is principal.

Problem (Proof Explanation). Our goal is to prove the following correspondence for rational primes p:

$$\{\text{ideals } p\mathcal{O}_K \text{ which split in } \mathcal{O}_K\} \iff \{p \mid \Delta_K\}.$$

The proof starts by describing the determinant Δ_K as the determinant $|\mathrm{T}^K_{\mathbb{Q}}(\alpha_i\alpha_j)|$ where $\{\alpha_i\}$ is an integral basis for $\mathcal{O}_K$. Let's consider this determinant over the field $\mathbb{F}_p$, so it is zero since $p|\Delta_K$. So the rows must be linearly dependent over $\mathbb{F}_p$. This means that there are integers $m_1, \ldots, m_n \in \mathbb{Z}$ not all divisible by p such that

$$\sum_{i=1}^{n} m_i \mathrm{T}^K_{\mathbb{Q}}(\alpha_i\alpha_j) \equiv 0 \mod p$$

for all j. Letting $\alpha = \sum m_i\alpha_i$, the above equality is equivalent to $p \mid \mathrm{T}^K_{\mathbb{Q}}(\alpha\alpha_j)$ for each j. So $\mathrm{T}^K_{\mathbb{Q}}(\alpha\mathcal{O}_K) \subset p\mathbb{Z}$. Since not all m_i are divisible by p, it follows that $\alpha \notin p\mathcal{O}_K$. Suppose for the sake of contradiction that p is unramified in $\mathcal{O}_K$. Let $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_k$. Then $\alpha \notin \mathfrak{p}$ for some $\mathfrak{p} = \mathfrak{p}_i$.

For this next step, we'll pass up to the normal closure L of K, prove that the trace $\mathrm{T}^L(\alpha\mathcal{O}_L) \in p\mathbb{Z}$, and finally use the Galois theory of prime decompositions to prove that we get a sum of distinct automorphisms summing to zero, a contradiction.

Let L be the normal closure of K over $\mathbb{Q}$. Since p is unramified in K, it must also be unramified in the normal closure L by the corollary to Theorem 4.31. Let $\mathfrak{q}$ be some prime lying over $\mathfrak{p}$ in $\mathcal{O}_L$. We also have $\alpha \notin \mathfrak{q}$ because $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

Now use the Chinese remainder theorem to get an element $\beta \in \mathcal{O}_L$ which isn't in $\mathfrak{q}$ but is in all of the other primes of $\mathcal{O}_L$ lying over p. Then we have the following:

1. $\mathrm{T}^L(\alpha\beta\mathcal{O}_L) \subset \mathfrak{q}$
2. $\sigma(\alpha\mathcal{O}_L) \subset \mathfrak{q}$ for each $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) - D(\mathfrak{q} \mid p)$.

The first statement follows immediately since we've shown that $\mathrm{T}^L(\alpha\mathcal{O}_L) \subset p\mathbb{Z} \subset \mathfrak{q}$. For the second statement, $\beta \in \sigma^{-1}(\mathfrak{q})$ since $\sigma^{-1}\mathfrak{q}$ is distinct from $\mathfrak{q}$. (Otherwise $\sigma \in D(\mathfrak{q} \mid p)$). Thus $\sigma(\beta) \in \mathfrak{q}$, hence implying the second statement. Now combining the two results together:

$$\sum_{\sigma \in D(\mathfrak{q}|p)} \sigma(\alpha\beta\mathcal{O}_L) \subset \mathfrak{q}.$$

Here the sum is interpreted to run over all $\mathcal{O}_L$. Now recall that members of $D(\mathfrak{q} \mid p)$ induce automorphisms for $L_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q}$. Let's reduce everything mod $\mathfrak{q}$, including the automorphisms. Then

$$0 = \sum_{\sigma \in D(\mathfrak{q}|p)} \widetilde{\sigma}(\alpha\beta L_{\mathfrak{q}}) = \sum_{\sigma \in D(\mathfrak{q}|p)} \widetilde{\sigma}(L_{\mathfrak{q}}).$$

Since the intertia group $E(\mathfrak{q} \mid p)$ is trivial since p is unramified in L, the automorphism $\widetilde{\sigma}$ are all distinct. However automorphisms are linearly independent over the base field, so we have a contradiction and we are done.