# Math 129 Problem Set 10

Lev Kruglyak

May 12, 2022

**Problem 6.11.** Show that if $\mathcal{O}_K = \mathbb{Z}$ and $m$ is any nonzero integer, then $G^+_{(m)}$ is isomorphic to $\mathbb{Z}^\times_m$.

First let's describe the equivalence relation $\sim^+_{(m)}$. Two ideals $I, J \subset \mathcal{O}_K$ are equivalent under this relationship if there exist $\alpha I = \beta J$ where $\alpha \equiv \beta \equiv 1 \mod m$. Since $\mathcal{O}_K = \mathbb{Z}$ is a PID, ideals are of the form $I = (a), J = (b)$ for some $a, b \in \mathbb{Z}$. Since $(\alpha a) = (\beta b)$ is equivalent to $\alpha a = \pm\beta b$, and this implies that $a \equiv b \mod m$, there is a one to one correspondence between elements of $\mathbb{Z}^\times_m$ and equivalence classes under $\sim^+_{(m)}$. This correspondence behaves well with respect to multiplication so $G^+_{(m)} \cong \mathbb{Z}^\times_m$.

**Problem 6.12.** Let $U^+_M$ denote the group of totally positive units in $\mathcal{O}_K$ satisfying $u \equiv 1 \mod M$. Show that $U^+_M$ is a free abelian group of rank $r + s - 1$.

In Problem 6.5, it is proved that if the field $K$ has at least one real embedding, then $U^+$, the group of all totally positive units is a free abelian group of rank $r + s - 1$. Let $u_1, \ldots, u_{r+s-1}$ be some basis for $U^+$. For every $u_i$, there is some $k_i \in \mathbb{Z}$ such that $u_i^{k_i} \equiv 1 \mod M$. Then the free module generated by $u_i^{k_i}$ has rank $r + s - 1$, and since $U^+_M \subset U_+$ which has rank $r + s - 1$, it follows that $U^+_M$ also has rank $r + s - 1$.

**Problem 6.13.** Modify the proof of Theorem 39 to yield the following improvement: If $C$ is any ray class (equivalence under $\sim^+_M$), then (with the obvious notation) we have

$$i_C(t) = \kappa^+_M t + \varepsilon_C(t)$$

where $\kappa^+_M$ is independent of $C$ and $\varepsilon_C(t)$ is $O(t^{1-1/n})$.

The proof is essentially unchanged, we know that $U^+_M$ is a free abelian group of rank $r + s - 1$, and we get the same lattice behavior and properties as for the non ray class group. The only crucial difference is that $\kappa^+_M$ would be smaller since ray classes are smaller than ordinary ideal classes.

**Problem 6.14.** Let $u_1, \ldots, u_{r+s-1}$ be any $r+s-1$ units in a number ring $\mathcal{O}_K$ and let $G$ be the subgroup of $U = \mathcal{O}_K^\times$ generated by all $u_i$ and all roots of unity in $\mathcal{O}_K$. Let $\Lambda_G$ be the sublattice of $\Lambda_U$ consisting of the log vectors of units in $G$.

(a) Prove that the factor groups $U/G$ and $\Lambda_U/\Lambda_G$ are isomorphic.

(b) Prove that the log vectors of the $u_i$ are linearly independent over $\mathbb{R}$ iff $U/G$ is finite.

(c) Define the regulator $\operatorname{reg}(u_1, \ldots, u_{r+s-1})$ to be the absolute value of the determinant formed from the log vectors of the $u_i$ along with any vector having coordinate sum 1. Show that $U/G$ is finite iff $\operatorname{reg}(u_1, \ldots, u_{r+s-1}) \neq 0$.

(d) Assuming that $\operatorname{reg}(u_1, \ldots, u_{r+s-1}) \neq 0$, prove that

$$\operatorname{reg}(u_1, \ldots, u_{r+s-1}) = |U/G| \cdot \operatorname{reg}(R).$$

**(a)** Recall that we have an (injective) embedding of $K \to \mathbb{R}^{r+2s}$ which restricts to an embedding $\lambda : \mathcal{O}_K \to \Lambda_K$, where $\Lambda_K$ is the fundamental lattice of the number field. This embedding is also an additive homomorphism, so we have a surjective map $U \to \Lambda_U/\Lambda_G$ which takes an $\alpha$ and maps it to $\lambda(\alpha) + \Lambda_G$. The kernel of this map is the set of $\alpha$ such that $\lambda(\alpha) \in \Lambda_G$, which is exactly $G$. So the first isomorphism theorem gives us a canonical isomorphism $U/G \to \Lambda_U/\Lambda_G$.

**(b)** Suppose first that the log vectors of the $u_i$ are linearly independent over $\mathbb{R}$. Then letting $\log : \Lambda_K \to \mathbb{R}^{r+s}$ be the standard log map, it follows that $\log(u_1, \ldots, u_{r+s-1})$ is a $r+s-1$ dimensional sublattice of $\log \Lambda_K$. Thus the quotient is finite. If the quotient is infinite, we get a clear contradiction which shows that the log vectors aren't linearly independent.

**Problem 7.1.** Fill in details in the proof of Theorem 42:

(a) Show that

$$1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots = (1 - 2^{1-s})\zeta(s)$$

for $s > 1$.

(b) Verify that $1 - 2^{1-s}$ has a simple zero at $s = 1$.

**(a)** Observe that

$$(1 - 2^{1-s})\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s} - 2\sum_{n=1}^\infty \frac{1}{(2n)^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots.$$

**(b)** First we'll expand $1 - 2^{1-s}$ as a power series. Note that

$$2^z = e^{z \log 2} = \sum_{n=0}^\infty \frac{(z \log 2)^n}{n!}$$

so $1 - 2^{1-s}$ has the power series

$$1 - 2^{1-s} = 1 - \sum_{n=0}^\infty \frac{(1-s)^n \log^n 2}{n!} = -\sum_{n=1}^\infty \frac{(1-s)^n \log^n 2}{n!} = (s-1)\left(\sum_{n=1}^\infty \frac{(1-s)^{n-1} \log^n 2}{n!}\right).$$

The second part of the factor has simple form, and the power of $(s-1)$ is one, so the zero at 1 is simple.

**Problem 7.3.** Let $A$ and $B$ be disjoint sets of primes in a number field. Show that

$$\delta(A \cup B) = \delta(A) + \delta(B)$$

if all of these polar densities exist, and that if any two of them exist, then so does the third.

First suppose all the polar densities exist. By definition, we have $\zeta_{K,A}(s) = (s-1)^{n\delta(A)} g_A(s)$ for some analytic function $g_A(s)$ which is defined and nonzero at $s = 1$. We have the same for $\zeta_{K,B}(s)$. Then,

$$\zeta_{K,A\cup B}(s) = \prod_{\mathfrak{p} \in A \cup B} \left(1 - \frac{1}{\|\mathfrak{p}\|^s}\right)^{-1} = \prod_{\mathfrak{p} \in A} \left(1 - \frac{1}{\|\mathfrak{p}\|^s}\right)^{-1} \prod_{\mathfrak{p} \in B} \left(1 - \frac{1}{\|\mathfrak{p}\|^s}\right)^{-1}$$

which can be extended to a function $(s-1)^{n(\delta(A)+\delta(B)} g_A(s) g_B(s)$, and so $\delta(A \cup B) = \delta(A) + \delta(B)$. Now suppose that two of them exist; there are two cases to consider. If both $\delta(A)$ and $\delta(B)$ exist, then the above argument shows that $\delta(A \cup B)$ must also exist. To address the other case, suppose without loss of generality that $\delta(A)$ and $\delta(A \cup B)$ exist. Then

$$\zeta_{K,B}(s) = \frac{\zeta_{K,A\cup B}(s)}{\zeta_{K,A}(s)}$$

so any extension of the two that exist gives an extension to $\zeta_{K,B}(s)$ giving a well defined density.

**Problem 7.6.** Let $H$ be a proper subgroup of $\mathbb{Z}_m^*$. Give an elementary proof, using nothing more that the Chinese remainder theorem that there are infinitely many primes $p \in \mathbb{Z}$ such that $\overline{p} \notin H$.

Suppose for the sake of contradiction that there were a finite number of primes $p_1, \ldots, p_k$ with $\overline{p_i} \notin H$. Let $x \in \mathbb{Z}$ be an integer congruent to $1 \mod p_i$ for all $i$ (This works by Chinese remainder theorem) and $\overline{x} \notin H$. We can ensure the second part since all $x + np_1 \cdots p_k$ are solutions for some fundamental solution $x < p_1 \cdots p_k$. Then