1. From Last Time

We briefly recall the following fact, which we had left unproved:

**Proposition 1.1.** Let $G$ be a finite multiplicative subgroup of a field. Then $G$ is cyclic.

**Proof.** Let $m$ be the maximal order of the elements of $G$. We will show that $m = |G|$. Of course, it is clear that $m \leq |G|$. We next claim that the order of every element of $G$ divides $m$: it suffices to show that given elements $x_1, x_2$ of orders $m_1, m_2$, there exists an element of order lcm$(m_1, m_2)$. Indeed, finding $m_1', m_2'$ which are relatively prime, divide $m_1$ and $m_2$ respectively, and have $m_1' = \text{lcm}(m_1, m_2)$, it is easy to check that $x_1^{m_1'/m_1} x_2^{m_2'/m_2}$ has the desired order. But elements of order dividing $m$ are roots of $x^m - 1$, so there can be at most $m$ of them, and we have $|G| \leq m$, so $|G| = m$, as desired. \qed

Recall that we had just shown that any additive subgroup of $\mathbb{R}^n$ which meets every bounded region in a finite set must be a lattice. Also recall the rings we are considering:

**Definition 1.2.** We say that a subring $R \subset \mathcal{O}_K$ is an **order** if $R$ contains a basis for $K$ over $\mathbb{Q}$.

We now finish the proof of the proposition from last time:

**Proposition 1.3.** The image $\psi(R^*) \subset \mathbb{R}^{r_1+r_2}$ is a lattice, and contained in the hyperplane defined by $x_1 + \cdots + x_{r_1+r_2} = 0$.

**Proof.** We first claim that $\psi(R^*)$ is contained in the hyperplane defined by $x_1 + \cdots + x_{r_1+r_2} = 0$. But since $R \subset \mathcal{O}_K$, we have $R^* \subset \mathcal{O}_K^*$, so if $x \in R^*$, we have $|N_{K/\mathbb{Q}}(x)| = 1$. But $|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r_1+r_2} |\sigma_i(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|^2$, since $|y| = |\bar{y}|$, and taking log of both sides gives the desired statement.

Next, we need to show that $\psi(R^*)$ is a lattice, or equivalently, that it contains only finitely many points in any bounded region. But note that if we restrict each coordinate log $|\sigma_i(x)|$ or $2 \log |\sigma_i(x)|$, depending on whether or not $i \leq r_1$, to be bounded by some $t$, this is equivalent to requiring that $|\sigma_i(x)| < e^t$ or $|\sigma_i(x)|^2 < e^t$, so it follows that the images $\varphi(x)$ are bounded in $\mathbb{R}^n$. Since $R^* \subset \mathcal{O}_K$, there are only finitely many $x \in R^*$ with $\varphi(x)$ in the given region in $\mathbb{R}^n$, and hence only finitely many with $\psi(x)$ in the given region in $\mathbb{R}^{r_1+r_2}$, proving that $\psi(R^*)$ is a lattice, as desired. \qed
2. Properties of orders

We begin with some properties of orders:

**Lemma 2.1.** We have:

(i) \( \varphi(R) \) is a lattice of full rank in \( \mathbb{R}^n \); in particular, the additive group of \( R \) is a free abelian group of rank \( n \).

(ii) \( R/I \) is finite for any non-zero ideal \( I \).

(iii) \( R \) is Noetherian, and has the property that every non-zero prime ideal is maximal.

(iv) For any non-zero \( x \in R \), there exist only finitely many ideals of \( R \) containing \( x \).

**Proof.** For (i), we have that \( \varphi(R) \subset \varphi(O_K) \) and is still an additive subgroup, so it is certainly a lattice. But since \( R \) contains a \( \mathbb{Q} \)-basis of \( K \), it follows by the same discriminant argument used in the case of \( O_K \) that it must span all of \( \mathbb{R}^n \), and must therefore be of full rank.

For (ii), by (i) and as in the case of \( O_K \), it suffices to see that \( I \) contains a non-zero integer. But Lemma 1.5 of lecture 3 worked for arbitrary integral domains, so the proof goes through for \( R \) as well.

For (iii), the proof follows from (ii) just as in the case of the full ring of integers.

For (iv), it suffices to show that \( R/(x) \) has only finitely many ideals. and this follows from the fact that \( R/(x) \) is finite. \( \square \)

**Remark 2.2.** \( R \) is not in general a Dedekind domain, as it will not satisfy the condition of being integrally closed. In fact, \( O_K \) is the integral closure of \( R \) in \( K \).

3. Fullness

Our aim now is to prove the harder half of the theorem:

**Proposition 3.1.** The image \( \psi(R^*) \) spans the hyperplane defined by \( x_1 + \cdots + x_{r_1 + r_2} \).

To do so, we use the following criterion:

**Lemma 3.2.** Let \( L \subset \mathbb{R}^m \) be a lattice. Then \( L \) is of full rank if and only if there exists a bounded region \( S \subset \mathbb{R}^n \) such that the translates \( S + L \) cover \( \mathbb{R}^m \).

**Proof.** Certainly, if \( L \) is full, then the translates of a fundamental parallelepiped of \( L \) cover \( \mathbb{R}^n \). Conversely, let \( S \) be a bounded region of \( \mathbb{R}^n \); say that the maximal distance of a point in \( S \) from \((0,\ldots,0)\) is \( t \). If \( L \) is not full, then its span is a proper subspace of \( \mathbb{R}^m \), and there exist vectors of distance \( > t \) from any point in this subspace. It follows that such vectors cannot be in any translate of \( S \) by \( L \). \( \square \)

To set up the argument for next time, we introduce the following ideas:

**Definition 3.3.** We have the multiplication map \( \cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n \) given by considering \( \mathbb{R}^n \) as \( \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \), and multiplying coordinates.

**Definition 3.4.** We define the norm map \( N : \mathbb{R}^n \to \mathbb{R}_{\geq 0} \) by the formula

\[
N(x_1, \ldots, x_n) = \prod_{i=1}^{r_1} |x_i| \prod_{i=1}^{r_2} (x_{r_1+2i-1}^2 + x_{r_1+2i}^2).
\]
Let \( \chi : \mathbb{R}^n \to \mathbb{R}^{r_1+r_2} \) be the map such that \( \psi = \chi \circ \varphi \). Explicitly,

\[
\chi(x_1, \ldots, x_n) = (\log |x_1|, \ldots, \log |x_{r_1}|, \log(x_{r_1+1}^2 + x_{r_1+2}^2), \ldots, \log(x_{n-1}^2 + x_n^2)).
\]

We then have the following compatibilities with existing ideas:

(i) \( \varphi(xy) = \varphi(x) \cdot \varphi(y) \) for \( x, y \in K \).

(ii) \( \chi(\bar{x} \cdot \bar{y}) = \chi(\bar{x}) + \chi(\bar{y}) \) for \( \bar{x}, \bar{y} \in \mathbb{R}^n \).

(iii) \( N(\bar{x} \cdot \cdots \cdot \bar{y}) = N(\bar{x})N(\bar{y}) \) for \( \bar{x}, \bar{y} \in \mathbb{R}^n \).

(iv) \( \log N(\bar{x}) \) is given by the sum of the coordinates of \( \chi(\bar{x}) \), for \( \bar{x} \in \mathbb{R}^n \).