Math 248A. The lattice of S-integers

Let K be a number field, and let S be a finite set of places of K containing the set S_∞ of archimedean places. Recall that we define the ring $\mathscr{O}_{K,S}$ of *S-integers* in K to be the set of $a \in K$ such that a is v-integral for all (necessarily non-archimedean!) $v \notin S$; that is, $\|a\|_v \le 1$ for all $v \notin S$. For $a \in \mathscr{O}_{K,S}$, we have $a \in \mathscr{O}_{K,S}^\times$ if and only if $a \neq 0$ and $a, 1/a \in K^\times$ each lie in $\mathscr{O}_{K,S}$. That is, $a \in \mathscr{O}_{K,S}^\times$ if and only if $a \in K^\times$ and $\|a\|_v, \|1/a\|_v \le 1$ for all $v \notin S$. This final condition says $\|a\|_v = 1$ for all $v \notin S$. Hence,

$$\mathscr{O}_{K,S}^\times = \{x \in K^\times \mid \|x\|_v = 1 \text{ for all } v \notin S\}.$$

1. Preliminaries

We first wish to show that $\mathscr{O}_{K,S}$ can be concretely constructed from $\mathscr{O}_K$ and knowledge of the class number. For each non-archimedean place of K, we let $\mathfrak{p}_v$ denote the corresponding prime ideal of $\mathscr{O}_K$. Since the class group is killed by the class number, for all non-archimedean v the ideal $\mathfrak{p}_v^{h(K)}$ in $\mathscr{O}_K$ is principal. Hence, the finite product $\prod_{v \in S - S_\infty} \mathfrak{p}_v^{h(K)}$ has the form $a_S\mathscr{O}_K$, so $1/a_S \in K^\times$ is non-integral at precisely those non-archimedean v that lie in S (if $S = S_\infty$ then this product is empty and we may interpret the product over the empty set $S - S_\infty$ to be the unit ideal $\mathscr{O}_K$; a_S is an element of $\mathscr{O}_K^\times$ in this case). Having constructed one such element, we now show that any such element allows us to construct $\mathscr{O}_{K,S}$ as a localization of $\mathscr{O}_K$:

Lemma 1.1. *For $a \in \mathscr{O}_K - \{0\}$, we have $\mathscr{O}_{K,S} = \mathscr{O}_K[1/a]$ if and only if the finite set of non-archimedean v for which $\|1/a\|_v > 1$ is exactly the set $S - S_\infty$. (Equivalently, the condition is that the prime factors of $a\mathscr{O}_K$ are exactly the primes $\mathfrak{p}_v$ for $v \in S - S_\infty$).*

Proof. If $\mathscr{O}_{K,S} = \mathscr{O}_K[1/a]$ then $1/a$ is v-integral for all $v \notin S$, so $\|1/a\|_v \le 1$ for all $v \notin S$. We wish to show that $\|1/a\|_v > 1$ for the other non-archimedean places, namely those $v \in S - S_\infty$. Suppose otherwise, so $\|1/a\|_{v_0} \le 1$ for some $v_0 \in S - S_\infty$. That is, assume $1/a$ is v_0-integral for some non-archimedean $v_0 \in S$. Since all elements of $\mathscr{O}_K$ are also v_0-integral, it follows that all elements of $\mathscr{O}_{K,S} = \mathscr{O}_K[1/a]$ are v_0-integral. However, this is not true: by finiteness of the class group we have $\mathfrak{p}_{v_0}^{h(K)} = a_0\mathscr{O}_K$ for some $a_0 \in \mathscr{O}_K - \{0\}$, and clearly $1/a_0 \in \mathscr{O}_{K,S}$ (since a_0 is even a local unit at all places not in S) yet $1/a_0$ is not v_0-integral for the place $v_0 \in S$ (as $\|1/a_0\|_{v_0} > 1$ due to the prime factorization of $a_0\mathscr{O}_K$).

Conversely, suppose $a \in \mathscr{O}_K$ is nonzero and $\|1/a\|_v > 1$ for $v \in S - S_\infty$ and $\|1/a\|_v \le 1$ for $v \notin S$, so $\mathscr{O}_K[1/a] \subseteq \mathscr{O}_{K,S}$ and we want this to be an equality. For $x \in \mathscr{O}_{K,S}$, we seek to find a large N such that $a^N x \in \mathscr{O}_K$. Since $a^N x \in \mathscr{O}_{K,S}$ for any $N > 0$, the only issue is to arrange that $a^N x$ is v-integral for each $v \in S - S_\infty$. Since $\mathrm{ord}_v(a^N x) = N\mathrm{ord}_v(a) + \mathrm{ord}_v(x)$ with $\mathrm{ord}_v(a) > 0$, we can certainly find such a large N. ∎

We can now make explicit how $\mathscr{O}_{K,S}$ behaves with respect to extension on K.

Theorem 1.2. *Let K'/K be a finite extension of number fields and let S be a finite set of places of K containing S_∞. Let S' be the set of places of K' lying over S, so S' is a finite set of places of K' containing the set S'_∞ of archimedean places of K'.*

The integral closure of $\mathscr{O}_{K,S}$ in K' is $\mathscr{O}_{K',S'}$. In particular, $\mathscr{O}_{K',S'}$ is a finite $\mathscr{O}_{K,S}$-module.

Proof. Choose $a \in \mathscr{O}_K - \{0\}$ such that for non-archimedean v on K we have $\|1/a\|_v > 1$ if and only if $v \in S - S_\infty$. By Lemma 1.1, $\mathscr{O}_{K,S} = \mathscr{O}_K[1/a]$. Choose $x \in K$. For a non-archimedean place v' on K' over a place (necessarily non-archimedean) v on K, clearly $x \in K'$ is non-integral at v' if and only if $x \in K$ is non-integral at v. Taking $x = 1/a$, we see that for any non-archimedean v' on K', $\|1/a\|_{v'} > 1$ if and only if $v' \in S' - S'_\infty$. Hence, by Lemma 1.1, $\mathscr{O}_{K',S'} = \mathscr{O}_{K'}[1/a]$. Our problem is to show that the integral closure of $\mathscr{O}_K[1/a]$ in K' is $\mathscr{O}_{K'}[1/a]$, and this follows from the compatibility of integral closure with respect to localization at a multiplicative set of nonzero elements of the base ring (in this case, localization at the set of powers of a with non-negative exponent). ∎

2. The lattice condition

Our aim is to study the geometry of the diagonal embedding

$$\mathscr{O}_{K,S} \to \prod_{v \in S} K_v$$

into the finite product of the locally compact completions K_v of K at the places $v \in S$. In the classical case $S = S_\infty$ this is the embedding

$$\mathscr{O}_K \hookrightarrow \prod_{v|\infty} K_v \simeq \mathbf{R} \otimes_{\mathbf{Q}} K \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}.$$

We have seen via a $\mathbf{Z}$-basis of $\mathscr{O}_K$ (and hence ultimately by the fact that $\mathbf{Z}$ is discrete in $\mathbf{R}$ and that $\mathbf{R}/\mathbf{Z}$ is compact) that $\mathscr{O}_K$ is discrete (hence closed) and co-compact in $\mathbf{R} \otimes_{\mathbf{Q}} K$ (that is, the quotient by $\mathscr{O}_K$ is compact). We claim a similar conclusion holds for general S:

Theorem 2.1. *The image of $\mathscr{O}_{K,S}$ in $\prod_{v \in S} K_v$ is a discrete (hence closed) and co-compact subgroup.*

In general, a *lattice* Γ in a locally compact Hausdorff topological group G is a discrete subgroup such that the locally compact Hausdorff coset space G/Γ is compact. In the special case that G is a finite-dimensional $\mathbf{R}$-vector space this recovers the traditional notion of a lattice in such a vector space, and the theorem says that $\mathscr{O}_{K,S}$ is a lattice in $\prod_{v \in S} K_v$ in general.

Proof. Let S' be a finite set of places of K containing S. We first show that if $\mathscr{O}_{K,S'}$ is a lattice in $\prod_{v \in S'} K_v$ then $\mathscr{O}_{K,S}$ is a lattice in $\prod_{v \in S} K_v$. Each valuation ring $\mathscr{O}_v = \mathscr{O}_{K_v}$ for $v \nmid \infty$ is both compact and open in K_v, so $\prod_{v \in S} K_v \times \prod_{v \in S'-S} \mathscr{O}_v$ (with its product topology) is open and closed in $\prod_{v \in S'} K_v$. This open and closed subgroup meets the diagonally embedded subgroup $\mathscr{O}_{K,S'}$ in the set of elements of $\mathscr{O}_{K,S'}$ whose image in K_v lies in $\mathscr{O}_v$ for all $v \in S' - S$, and these are the elements of $\mathscr{O}_{K,S'}$ that are v-integral for all $v \in S' - S$. In other words, these are the elements of K that are integral at all non-archimedean places outside of S' and at all places in $S' - S$, which is to say at all places outside of S: these are the elements of $\mathscr{O}_{K,S}$. Hence,the subgroup $\mathscr{O}_{K,S'}$ in $\prod_{v \in S'} K_v$ meets the open and closed subgroup $\prod_{v \in S} K_v \times \prod_{v \in S'-S} \mathscr{O}_v$ in exactly $\mathscr{O}_{K,S}$, and so the discreteness hypothesis for $\mathscr{O}_{K,S'}$ implies that $\mathscr{O}_{K,S}$ has discrete image in $\prod_{v \in S} K_v \times \prod_{v \in S'-S} \mathscr{O}_v$. We may thereby infer discreteness of $\mathscr{O}_{K,S}$ diagonally embedded in $\prod_{v \in S} K_v$ via:

Lemma 2.2. *Let G and G' be Hausdorff topological groups with G' compact. Let Γ be a discrete subgroup of $G \times G'$ such that the map $\Gamma \to G$ is injective. The image of Γ in G is discrete.*

Proof. We will argue with the language of nets, but the reader who prefers to use sequences to probe the topology of a space may safely impose the condition that G and G' have a countable base of opens around each point (which certainly holds for metrizable spaces, the intended application). Let $\pi : G \times G' \to G$ be the projection. Suppose that Γ does not have discrete image in G, so there exists $\gamma \in \Gamma$ such that $\pi(\gamma)$ is a limit of a net $\{\pi(\gamma_i)\}$ where the γ_i's lie in $\Gamma - \{\gamma\}$. Consider the net $\{\gamma_i\}$ in $\Gamma \subseteq G \times G'$. Since G' is compact Hausdorff, by passing to a subnet we may arrange that the image of $\{\gamma_i\}$ in G' has a limit. By hypothesis the image of $\{\gamma_i\}$ in G has a limit, namely γ. Hence, the net $\{\gamma_i\}$ has a limit under projection to each factor and so has a limit in $G \times G'$. By discreteness of Γ in $G \times G'$, the net must be eventually constant, and so the net $\{\pi(\gamma_i)\}$ in G is eventually constant. Its limit is $\pi(\gamma)$, so $\pi(\gamma_i) = \pi(\gamma)$ for large i. By the hypothesis of injectivity for π we conclude $\gamma_i = \gamma$ for large i, a contradiction. ■

We conclude that discreteness for $\mathscr{O}_{K,S}$ in $\prod_{v \in S} K_v$ is a consequence of the assumed discreteness for $\mathscr{O}_{K,S'}$ in $\prod_{v \in S'} K_v$. By closedness of discrete subgroups, the quotients $(\prod_{v \in S} K_v)/\mathscr{O}_{K,S}$ and $(\prod_{v \in S'} K_v)/\mathscr{O}_{K,S'}$ are locally compact Hausdorff topological groups and we wish to show that compactness of the latter implies compactness of the former. Consider the natural continuous map (using quotient topologies)

$$j : (\prod_{v \in S} K_v \times \prod_{v \in S'-S} \mathscr{O}_v)/\mathscr{O}_{K,S} \to (\prod_{v \in S'} K_v)/\mathscr{O}_{K,S'}.$$

This is clearly injective, and if we can prove it is a closed embedding then the source is compact and so its image $(\prod_{v \in S} K_v)/\mathscr{O}_{K,S}$ under projection to the S-factors is certainly compact as desired. Since the source and target of j are quotients by *discrete* subgroups, the map j is locally (on source and target) an open embedding because the map $\prod_{v\in S} K_v \times \prod_{v\in S'-S} \mathscr{O}_v \to \prod_{v\in S'} K_v$ is certainly an open embedding. It is elementary definition-chasing to check that continuous map that is locally an open embedding is an open embedding if and only if it is injective, so by injectivity of j we can indeed deduce the lattice property for S if we have it for some S' containing S.

Now we use the preceding considerations with a suitable $S' \supseteq S$ to increase S to be the preimage of a finite set of places of $\mathbf{Q}$ (containing the archimedean place), and so (by Theorem 1.2) $\mathscr{O}_{K,S}$ is the integral closure of $\mathbf{Z}[1/N]$ in K for a suitable nonzero integer N, so $\mathscr{O}_{K,S} = \mathscr{O}_K[1/N]$. For $S_0 = \{\infty, p|N\}$ we have

$$\prod_{v\in S} K_v = \prod_{v_0\in S_0} (\prod_{v|v_0} K_v) \simeq \prod_{v_0\in S_0} K \otimes_{\mathbf{Q}} \mathbf{Q}_{v_0} \simeq K \otimes_{\mathbf{Q}} \prod_{v_0\in S_0} \mathbf{Q}_{v_0}.$$

Since $K = \mathscr{O}_K[1/N] \otimes_{\mathbf{Z}[1/N]} \mathbf{Q}$, we get a natural isomorphism

$$\phi : \mathscr{O}_K[1/N] \otimes_{\mathbf{Z}[1/N]} \prod_{v\in S_0} \mathbf{Q}_v \simeq \prod_{v\in S} K_v.$$

Since $\mathbf{Z}[1/N]$ is a PID we may find a free basis for $\mathscr{O}_K[1/N]$ as a $\mathbf{Z}[1/N]$-module, and it is a simple exercise (check!) that using any such choice of basis to identify the source of ϕ with a product of copies of $\prod_{v_0\in S_0} \mathbf{Q}_{v_0}$ makes ϕ into a topological isomorphism. Hence, upon picking such a basis we may reduce the problem of discreteness and co-compactness for $\mathscr{O}_K[1/N]$ in $\prod_{v\in S} K_v$ to the problem of discreteness and co-compactness for $\mathbf{Z}[1/N]$ in $\prod_{v_0\in S_0} \mathbf{Q}_{v_0}$. This completes the reduction of our problem to the case of the field $\mathbf{Q}$.

To check discreteness in the case $K = \mathbf{Q}$ (with $\mathscr{O}_{K,S} = \mathbf{Z}[1/N]$ for a suitable nonzero integer N) we observe that $(-1,1) \times \prod_{p|N} \mathbf{Z}_p$ is an open neighborhood of the origin in $\prod_{v\in S} \mathbf{Q}_v$ that meets $\mathscr{O}_{K,S} = \mathbf{Z}[1/N]$ in the set of elements $x \in \mathbf{Z}[1/N]$ that are p-integral for all $p|N$ and satisfy $|x| < 1$. The p-integrality for all $p|N$ says exactly $x \in \mathbf{Z}$, and clearly if $x \in \mathbf{Z}$ and $|x| < 1$ then $x = 0$. This proves discreteness. For co-compactness it suffices to prove that the natural continuous map

$$[0,1] \times \prod_{p|N} \mathbf{Z}_p \to (\prod_{v\in S} \mathbf{Q}_v)/\mathbf{Z}[1/N]$$

with compact source is surjective. Pick an element $x \in \prod_{v\in S} \mathbf{Q}_v$. Every element of $\mathbf{Q}_p/\mathbf{Z}_p$ admits a representative of the form a_p/p^{e_p} with $e_p \geq 0$ and $a_p \in \mathbf{Z}$, and so by subtracting an element of the form $\sum_{p|N} a_p/p^{e_p} \in \mathbf{Z}[1/N]$ we can find a representative for $x \bmod \mathbf{Z}[1/N]$ that lies in $\mathbf{R} \times \prod_{p|N} \mathbf{Z}_p$. Adjusting by a further element of $\mathbf{Z}$ (diagonally embedded) allows us to find a representative for $x \bmod \mathbf{Z}[1/N]$ lying in $[0,1] \times \prod_{p|N} \mathbf{Z}_p$ as desired. ■