Mathematics W4043 Algebraic Number Theory
Assignment # 2

Benjamin Church
Worked With Matthew Lerner-Brecher

October 27, 2018

1. Let $\mathcal{O}_K$ be the ring of integers of a number field K. Then $M \subset K$ is a fractional ideal of $\mathcal{O}_K$ if M is a $\mathcal{O}_K$-module of finite type.

   (a) Let M be a fractional ideal of K then since M has finite type, $M = m_1\mathcal{O}_K + \cdots + m_n\mathcal{O}_K$. Futhermore, by Lemma 0.1 for any $\alpha \in K$ there exists $z \in \mathbb{Z}$ s.t. $\alpha z \in \mathcal{O}_K$. Therefore, for each $1 \leq i \leq n$ take $z_i \in \mathbb{Z}$ s.t. $z_i m_i \in \mathcal{O}_K$. Define $r = \text{lcm}(z_1, \ldots, z_n)$.

   For any $m \in M$, by the finite type condition, $m = o_1 m_1 + \cdots o_n m_n$ with $o_i \in \mathcal{O}_K$. But $z_i \mid r$ so $r = k_i z_i$ for $k_i \in \mathbb{Z}$ so $rm_i = k_i(m_i z_i) \in \mathcal{O}_K$. Thus, $rm = o_1 r m_1 + \cdots + o_n r m_1 = o_1 k_1(m_1 z_1) + \ldots o_n k_n(m_n z_n) \in \mathcal{O}_K$. Therefore, $\forall m \in M : rm \in \mathcal{O}_K$.

   (b) Let M and M' be fractional ideals of $\mathcal{O}_K$ then define

   $$M \cdot M' = \{o_1 m_1 m_1' + \cdots + o_n m_n m_n' \mid m_i \in M \text{ and } m_i' \in M' \text{ and } o_i \in \mathcal{O}_K\}$$

   Now M and M' are $\mathcal{O}_K$-modules of finite type so for any $m_i \in M$ write: $m_i = d_{i1} w_1 + \cdots + d_{ik} w_k$ and $m_i' = d_{i1}' w_1' + \cdots + d_{ik'}' w_{k'}'$ for $d_{ij}, d_{ij}' \in \mathcal{O}_K$ Therefore,

   $$o_1 m_1 m_1' + \cdots + o_n m_n m_n' = \sum_{l=1,i=1,j=1}^{n,k,k'} o_l d_{ij} d_{ij}' w_i w_j'$$

   Thus, $\{w_i w_j'\}$ generates $M \cdot M'$ so $M \cdot M'$ has finite type.

   (c) Let M be a fractional ideal of $\mathcal{O}_K$ then define:

   $$M^{-1} = \{\alpha \in K \mid \forall m \in M : \alpha m \in \mathcal{O}_K\}$$

   If $\alpha, \beta \in M^{-1}$ then $\forall m \in M : \alpha m, \beta m \in \mathcal{O}_K$ thus, $(\alpha + \beta)m = \alpha m + \beta m \in \mathcal{O}_K$. Also, if $o \in \mathcal{O}_K$ then $o\alpha m = (\alpha m)o \in \mathcal{O}_K$ because $\alpha m, o \in \mathcal{O}_K$. Thus, M^{-1} is an $\mathcal{O}_K$-module.

   Now M has finite type so $M = m_1\mathcal{O}_K + \cdots + m_n\mathcal{O}_K$. If $\alpha \in M^{-1}$ then $\alpha m_i \in \mathcal{O}_K$ so $\alpha \in \frac{1}{m_i}\mathcal{O}_K$ therefore, $\alpha \in \bigcap_{i=1}^{n} \frac{1}{m_i}\mathcal{O}_K$.

   Conversely, if $\alpha \in \bigcap_{i=1}^{n} \frac{1}{m_i}\mathcal{O}_K$ then for each i, $\alpha \in \frac{1}{m_i}\mathcal{O}_K$ so $\alpha m_i \in \mathcal{O}_K$ therefore, $\alpha(m_1 o_1 + \cdots + m_n o_n) = (\alpha m_1)o_1 + \cdots + (\alpha m_n)o_n \in \mathcal{O}_K$ so $\alpha \in M^{-1}$ and thus,

   $$M^{-1} = \bigcap_{i=1}^{n} \frac{1}{m_i}\mathcal{O}_K \subset \frac{1}{m_1}\mathcal{O}_K$$

However, $\frac{1}{m_1}\mathcal{O}_K$ is an $\mathcal{O}_k$-module of manifestly finite type therefore, $M^{-1} \subset \frac{1}{m_1}\mathcal{O}_K$ is an $\mathcal{O}_k$-submodule which has finite type because $\mathcal{O}_K$ is Noetherian.

2. Let $\{\mathfrak{p}_i \mid i \in \mathbb{N}\}$ a sequence of distinct prime ideals of $\mathcal{O}_K$. Then take $I = \bigcap_{i=1}^{\infty} \mathfrak{p}_i$. Now since $\mathcal{O}_K$ is Dedekind, its ideals have prime factorizaion. In particular, $I = \prod_{i=1}^{k} \mathfrak{q}_i$ so take $\mathfrak{p}_{r+1}$ distinct from every $\mathfrak{q}_i$. I claim that $I + \mathfrak{p}_{r+1} = \mathcal{O}_K$. In that case, $I\mathfrak{p}_{r+1} = I \cap \mathfrak{p}_{r+1} = I$. Therefore, if $I \neq \{0\}$ then $\mathfrak{p}_{r+1} = \mathcal{O}_K$ which is a contradiction. Therefore, $I = \{0\}$.

   To prove the claim, we show that for prime ideal $\mathfrak{p}$ distinct from all $\mathfrak{q}_i$ that $\prod_{i=1}^{n} \mathfrak{q}_i + \mathfrak{p} = \mathcal{O}_K$. Proceed by induction, for $k = 1$, $\mathfrak{q}_1 \subset \mathfrak{q}_1 + \mathfrak{p}$ but $\mathfrak{q}_1$ is maximal and since the ideals are distinct, $\mathfrak{q}_1 \subsetneq \mathfrak{q}_1 + \mathfrak{p}$ therefore, $\mathfrak{q}_1 + \mathfrak{p} = \mathcal{O}_K$.

   Now suppose that $\prod_{i=1}^{k} \mathfrak{q}_i + \mathfrak{p} = \mathcal{O}_K$ then $\left(\prod_{i=1}^{k} \mathfrak{q}_i\right)\mathfrak{q}_{k+1} + \mathfrak{p}\mathfrak{q}_{k+1} = \mathfrak{q}_{k+1}$. Thus, $\prod_{i=1}^{k+1} \mathfrak{q}_i + (\mathfrak{p}\mathfrak{q}_{k+1} + \mathfrak{p}) = \mathfrak{q}_{k+1} + \mathfrak{p}$ but $\mathfrak{q}_{k+1} + \mathfrak{p} = \mathcal{O}_K$ because both are maximal and also $\mathfrak{p}\mathfrak{q}_{k+1} + \mathfrak{p} = \mathfrak{p}$ because $\mathfrak{p}\mathfrak{q}_{k+1} \subset \mathfrak{p}$. Therefore, $\prod_{i=1}^{k+1} \mathfrak{q}_i + \mathfrak{p} = \mathcal{O}_K$ so the claim holds by induction.

3. Let R be an integral domain with fraction field K. And for a multiplicative subset S let

$$S^{-1}R = \left\{ \frac{r}{s} \,\middle|\, r \in R \text{ and } s \in S \right\}$$

   For any ideal $I \subset R$,

$$S^{-1}I = \left\{ \frac{r}{s} \,\middle|\, r \in I \text{ and } s \in S \right\}$$

   is an ideal of $S^{-1}R$. This holds because if $\frac{r_1}{s_1}, \frac{r_2}{s_2} \in S^{-1}I$ then $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \in s^{-1}I$ and $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2} \in S^{-1}I$ and for $\frac{r}{s} \in S^{-1}R$ and $\frac{a}{s'} \in S^{-1}I$, then $\frac{r}{s}\frac{a}{s'} = \frac{ra}{ss'} \in S^{-1}I$ all by absorption of I and multiplictive property of S.

   (a) Let $S = R\backslash\{0\}$ then

$$S^{-1}R = \left\{ \frac{p}{q} \,\middle|\, p \in R \text{ and } q \in R\backslash\{0\} \right\} = K$$

   by definition.

   (b) Let R be a Dedekind domain. Then by part (c), the map $I \mapsto S^{-1}I$ is a surjection. If $J_1 \subset J_2 \subset \cdots$ is an increasing chain of ideals of $S^{-1}R$ then $J_i = S^{-1}I_i$. Suppose that $I_i \supset I_{i+1}$, then $S^{-1}I_i \supset S^{-1}I_{i+1}$ also if $J_i \subsetneq J_{i+1}$ then $I_i \subsetneq I_{i+1}$. Therefore, $I_1 \subset I_2 \subset \cdots$ is an increasing chain of ideals of R. Since R is Noetherian, the chain of I_i terminates i.e. after some n, $I_n = I_{n+1} = \cdots$ so $I_n \supset I_{n+1} \supset \cdots$ and therefore, $J_n \supset J_{n+1} \supset \cdots$. Thus, the chain of J_i also terminates at n so $S^{-1}R$ is Noetherian.

   Suppose that α is integral over $S^{-1}R$. Then, for some monic polynomial $Q \in S^{-1}R[x]$, $Q(\alpha) = \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$. But each $c_i \in S^{-1}R$ so $c_i = \frac{r_i}{s_i}$ for $r_i \in R$ and $s_i \in S$. Multiply through by $s^n = (s_{n-1}s_{n-2}\ldots s_0)^n$,

$$Q(\alpha)s^n = (s\alpha)^n + r_{n-1}(s_{n-2}\ldots s_0)(s\alpha)^{n-1} + \cdots + s^{n-1}(s_{n-1}s_{n-2}\cdots s_1)r_0 = 0$$

Thus, $s\alpha$ is integral over R. However, R is Dedekind and thus integrally closed so $s\alpha \in R$. Since $s\alpha \in R$ and $s \in S$ then $\frac{s\alpha}{s} = \alpha \in S^{-1}R$ so $S^{-1}R$ is integrally closed.

Let $J \subset S^{-1}R$ be a non-zero prime ideal of $S^{-1}R$. By the bijection derived in part (c), $J = S^{-1}I$ where I is a non-zero prime ideal which is disjoint with S. Since I is a non-zero prime ideal of R and R is Dedekind, then I is maximal. Suppose that $J \subsetneq L \subset S^{-1}R$. Then $L = S^{-1}F$ for an ideal F. Then $I \subsetneq F$ so $F = R$ and thus $L = S^{-1}F = S^{-1}R$ so J is maximal. Thus, $S^{-1}R$ is Dedekind.

(c) Let D be the map from ideals of R to ideals of $S^{-1}R$ given by $D : I \mapsto S^{-1}I$. Now if $J \subset S^{-1}R$ is an ideal then consider $R \cap J \subset R$. This is an ideal of R because if $x, y \in R \cap J$ then $xy \in R$ and $xy \in J$ so $xy \in R \cap J$ and for $r \in R$, $r = \frac{r}{1} \in S^{-1}R$ so $rx \in J$ so $rx \in R \cap J$.

Take $x \in D(R \cap J)$ then $x = \frac{r}{s}$ with $r \in J$ and since $\frac{1}{s} \in S^{-1}R$, by absorption, $\frac{r}{s} = x \in J$. Take $\frac{r}{s} \in J$ with $r \in R$ then $r = s\frac{r}{s} \in J$ by absorption so $r \in R \cap J$ thus $\frac{r}{s} \in D(R \cap J)$. Therefore, $D(R \cap J) = J$ so D is surjective.

Restrict D to the set of prime ideals of R which do not intersect S. Let P be a prime ideal of R and $P \cap S = \emptyset$. Take $\frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r}{s} \in S^{-1}P$ for $r_1, r_2 \in P$. Then $r_1 r_2 s = s_1 s_2 r \in P$. P is prime so either $r_1 \in P$ or $r_2 s \in P$. If $r_2 s \in P$ then $r_2 \in P$ because $s \notin P$. Therefore, $r_1 \in P$ or $r_2 \in P$ so $\frac{r_1}{s_1} \in S^{-1}P$ or $\frac{r_2}{s_2} \in S^{-1}P$ and therefore $S^{-1}P$ is prime. Thus, $\mathrm{Im}\,(D)$ is contained within the set of prime ideals of $S^{-1}R$.

Let P and Q be prime ideals of R s.t. $P \cap S = Q \cap S = \emptyset$. Then suppose that $D(P) = D(Q)$ i.e. $S^{-1}P = S^{-1}Q$. Then $\frac{p}{s_1} = \frac{q}{s_2}$ for any $p \in P$ and $q \in Q$. Thus, $s_2 p = s_1 q$ so $s_2 p \in Q$ and $s_1 q \in P$ by absorption. The ideals are prime so $p \in Q$ and $q \in P$ since $s_2 \notin Q$ and $s_1 \notin P$. Therefore, $P \subset Q$ and $P \supset Q$ so $P = Q$. Therefore, D is injective.

Let $J \in S^{-1}R$ be prime then take $xy \in R \cap J$ with $x, y \in R$. Now $xy \in J$ so $x \in J$ or $y \in J$. Therefore, since both $x, y \in R$ then $x \in R \cap J$ or $y \in R \cap J$ so $R \cap J$ is a prime ideal in R. Suppose that $\exists s \in S \cap (R \cap J)$ then $s \in J$ so by absorption, $\frac{1}{s}s \in J$ since $\frac{1}{s} \in S^{-1}R$ thus $1 \in J$ so $J = S^{-1}R$ which contradicts J being a prime ideal. Thus, $(R \cap J) \cap S = \emptyset$ so D is surjective in the set of prime ideals of $S^{-1}R$.

Therefore, D is a bijection from the set of prime ideals of R which are disjoint with S and the prime ideals of $S^{-1}R$.

(d) Let R be a Dedekind domain and $\mathfrak{p}$ be a prime ideal of R. Define $S_\mathfrak{p} = R \setminus \mathfrak{p}$ and $R_\mathfrak{p} = S_\mathfrak{p}^{-1}R$. If $s, s' \in S_p$ then if $ss' \in \mathfrak{p}$ then either $s \in \mathfrak{p}$ or $s' \in \mathfrak{p}$ because $\mathfrak{p}$ is a prime ideal. However, $s, s' \in S_p$ so neither are in $\mathfrak{p}$. Thus, $ss' \notin \mathfrak{p}$ so $ss' \in S_p$. Also, $1 \notin \mathfrak{p}$ because a prime ideal cannot be the entire ring thus $1 \in S_p$. Now there is a bijection between the prime ideals of R which do not intersect with $S_\mathfrak{p}$ and the prime ideals of $R_\mathfrak{p}$. If some ideal $I \subset R$ is a non-zero prime ideal and $I \cap S_\mathfrak{p} = I \cap (R \setminus \mathfrak{p}) = \emptyset$ then $I \subset \mathfrak{p}$ but

R is a Dedekind domain so every non-zero prime ideal is maximal so $I = \mathfrak{p}$. Thus $\mathfrak{p}$ is the unique non-zero prime ideal of R that is disjoint with $S_\mathfrak{p}$. Using the bijection, $S_p^{-1}\mathfrak{p}$ is the unique prime ideal of $R_\mathfrak{p}$. Furthermore, because R is Dedekind so is $R_\mathfrak{p} = S_\mathfrak{p}^{-1}R$. Thus, $R_\mathfrak{p}$ is a discrete valuation ring.

$R_\mathfrak{p}$ is a Noetherian ring and $R_\mathfrak{p}$ is a $R_\mathfrak{p}$-module of finite type. Therefore, since $\mathfrak{p}$ is an ideal of $R_\mathfrak{p}$ then $\mathfrak{p}$ is an $R_\mathfrak{p}$-submodule and thus has finite type. Let $\mathfrak{p} = c_1R_\mathfrak{p} + \cdots + c_nR_\mathfrak{p}$. Then (c_i) is an ideal of $R_\mathfrak{p}$ which is a Dedekind domain so it has a prime factorization. Since there is only one prime ideal, $(c_1) = \mathfrak{p}^{k_i}$. Take c to be the c_i with the least k_i then $(c_i) = \mathfrak{p}^{k_i} \subset \mathfrak{p}^{k_c} = (c)$ so $c_i \in (c)$. Therefore, $c_i = rc$ so $\mathfrak{p} = cR_\mathfrak{p} = (c)$.

For any $a \in R_\mathfrak{p}$, the ideal (a) has a prime factorization because $R_\mathfrak{p}$ is a Dedekind domain. Thus, $(a) = \mathfrak{p}^k = (c)^k = (c^k)$. Thus, $a = rc^k$ and $c^r = sa$ thus $a = (rs)a$. Since $R_\mathfrak{p}$ is a domain, $rs = 1$ so r is a unit.

Lemmas

Lemma 0.1. *If $\mathcal{O}_K$ is the ring of algebraic integers of a number field $K/\mathbb{Q}$ and $\alpha \in K$ then $\exists z \in \mathbb{Z}$ s.t. $z\alpha \in \mathcal{O}_K$.*

Proof. Since $K/\mathbb{Q}$ is a finite field extension, $[K : \mathbb{Q}] = n$ so for any $\alpha \in K$, $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is a dependent set. Therefore, $\exists c_i \in \mathbb{Q} : Q(\alpha) = \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$. For each c_i there are integers $p_i, q_i \in \mathbb{Z}$ s.t. $c_i = \frac{p_i}{q_i}$. Multiply by $z = \operatorname{lcm}(q_{n-1}, \ldots, q_0)$ and let $k_iq_i = z$ so

$$z^nQ(\alpha) = (z\alpha)^n + p_{n-1}k_{n-1}(z\alpha)^{n-1} + \cdots + p_0k_0z^{n-1} = 0$$

So $z\alpha \in \mathcal{O}_K$. □