Homework 1

Songyu Ye

September 7, 2025

Problem 1 Check that localization preserves products and colons. Explain how this implies that the following proposition from the textbook.

Proposition 0.1 (S, Prop 1.3.5)**.** *Let A be a Dedekind domain and I a non-zero fractional ideal. Then I is invertible.*

Solution:

(i) $(a \cdot b)_{\mathfrak{p}} = a_{\mathfrak{p}} \cdot b_{\mathfrak{p}}$.

Proof. Every element of $a_{\mathfrak{p}} \cdot b_{\mathfrak{p}}$ is a finite sum of products

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \qquad (a \in a,\ b \in b,\ s, t \in S),$$

hence lies in $S^{-1}(ab) = (ab)_{\mathfrak{p}}$.

Conversely, $(ab)_{\mathfrak{p}}$ is generated (as an ideal of $A_{\mathfrak{p}}$) by the fractions $\frac{ab}{s}$ with $a \in a$, $b \in b$, $s \in S$, and

$$\frac{ab}{s} = \frac{a}{1} \cdot \frac{b}{s} \in a_{\mathfrak{p}} \cdot b_{\mathfrak{p}}.$$

So the two ideals are equal. □

(ii) $(a : b)_{\mathfrak{p}} = (a_{\mathfrak{p}} : b_{\mathfrak{p}})$.

Proof. Recall

$$(a : b) = \{x \in A \mid xb \subset a\}, \qquad (a_{\mathfrak{p}} : b_{\mathfrak{p}}) = \{z \in A_{\mathfrak{p}} \mid zb_{\mathfrak{p}} \subset a_{\mathfrak{p}}\}.$$

($\subseteq$): If $\frac{x}{s} \in S^{-1}(a : b)$, then $xb \subset a$, so for any $\frac{b}{t} \in b_{\mathfrak{p}}$ we have

$$\frac{x}{s} \cdot \frac{b}{t} = \frac{xb}{st} \in S^{-1}a = a_{\mathfrak{p}}.$$

Hence $\frac{x}{s} \in (a_{\mathfrak{p}} : b_{\mathfrak{p}})$.

($\supseteq$): Assume $\frac{x}{s} \in (a_{\mathfrak{p}} : b_{\mathfrak{p}})$. Choose generators $b = (b_1, \ldots, b_n)$. This is where we use that b is finitely generated. For each i, $\frac{x}{s} \cdot \frac{b_i}{1} \in a_{\mathfrak{p}}$, so there exists $s_i \in S$ with $s_i x b_i \in a$. Let $t = \prod_i s_i \in S$. Then $txb_i \in a$ for all i, hence $txb \subset a$, i.e. $tx \in (a : b)$. Therefore

$$\frac{x}{s} = \frac{tx}{ts} \in S^{-1}(a : b) = (a : b)_{\mathfrak{p}}.$$

□

Now let I be a nonzero fractional ideal in the Dedekind domain A. We want to show I is invertible, i.e. there exists a fractional ideal J such that $IJ = A$. Pick a nonzero prime $\mathfrak{p} \subset A$. Localize at $\mathfrak{p}$: in the DVR $A_\mathfrak{p}$, every nonzero fractional ideal is of the form

$$I_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^n \quad (n \in \mathbb{Z}).$$

Its inverse in $A_\mathfrak{p}$ is then

$$J_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^{-n},$$

so that $I_\mathfrak{p} J_\mathfrak{p} = A_\mathfrak{p}$. Thus,locally at every prime, I has an inverse. Define globally

$$J := \prod_\mathfrak{p} \mathfrak{p}^{-n_\mathfrak{p}},$$

where $I_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^{n_\mathfrak{p}}$. Only finitely many exponents $n_\mathfrak{p}$ are nonzero, so this makes sense.

Now for each prime $\mathfrak{q}$,

$$(IJ)_\mathfrak{q} = I_\mathfrak{q} J_\mathfrak{q} = A_\mathfrak{q}.$$

Since the localizations are the unit ideal everywhere, we get globally

$$IJ = A.$$

This is because if IJ were proper, it would be contained in some maximal ideal $\mathfrak{m}$, hence $(IJ)_\mathfrak{m} \subseteq \mathfrak{m}_\mathfrak{m}$, contradicting the above. Thus I is invertible with inverse J.

Problem 2 Let A be a Dedekind domain, S a multiplicatively closed subset which is strictly smaller than the set of all nonzero elements.

1. Show that the localization $S^{-1}A$ is a Dedekind domain.

2. Show that the extension of ideals (and similarly for fractional ideals) induces a surjection from the ideal class group of A to that of $S^{-1}A$.

Solution:

1. Recall that a Noetherian domain R is Dedekind iff for every nonzero prime $\mathfrak{p} \subset R$, the localization $R_\mathfrak{p}$ is a DVR.

   Let $\mathfrak{P}$ be a nonzero prime of $S^{-1}A$. Then $\mathfrak{P} = S^{-1}\mathfrak{p}$ for a unique prime $\mathfrak{p} \subset A$ with $\mathfrak{p} \cap S = \varnothing$. Moreover, $(S^{-1}A)_\mathfrak{P} \cong A_\mathfrak{p}$. Since A is Dedekind, every $A_\mathfrak{p}$ (for $\mathfrak{p} \neq (0)$) is a DVR; hence every $(S^{-1}A)_\mathfrak{P}$ is a DVR. Therefore $S^{-1}A$ is Dedekind.

   We also check that $S^{-1}A$ is Noetherian and an integral domain. Let I be an ideal of $S^{-1}A$. Consider its contraction in A: $I^c := \{a \in A \mid \frac{a}{1} \in I\}$. This is an ideal of A. Since A is Noetherian, I^c is finitely generated, say by $a_1, \dots, a_n$. Then $I = S^{-1}I^c = \left(\frac{a_1}{1}, \dots, \frac{a_n}{1}\right)$, so I is finitely generated in $S^{-1}A$. Thus every ideal of $S^{-1}A$ is finitely generated, i.e. $S^{-1}A$ is Noetherian.

Finally, $S^{-1}A$ is an integral domain because if $\frac{a}{s}\cdot\frac{b}{t}=0$ in $S^{-1}A$, then there exists $u\in S$ with $uab=0$ in A. Since A is an integral domain and $u\neq 0$, we must have $a=0$ or $b=0$, hence $\frac{a}{s}=0$ or $\frac{b}{t}=0$ in $S^{-1}A$.

2. Recall unique factorization of fractional ideals in Dedekind domains. In A, every nonzero fractional ideal has a unique factorization

$$I=\prod_{\mathfrak{p}}\mathfrak{p}^{n_\mathfrak{p}} \qquad (n_\mathfrak{p}\in\mathbb{Z},\ \text{all but finitely many } 0).$$

In $S^{-1}A$: the nonzero prime ideals are exactly $S^{-1}\mathfrak{p}$ with $\mathfrak{p}\cap S=\varnothing$ (because if $\mathfrak{p}\cap S\neq\varnothing$, then $S^{-1}\mathfrak{p}$ contains a unit, hence equals $S^{-1}A$). So

$$S^{-1}(\mathfrak{p}^n)=\begin{cases}(S^{-1}\mathfrak{p})^n, & \mathfrak{p}\cap S=\varnothing,\\ S^{-1}A, & \mathfrak{p}\cap S\neq\varnothing.\end{cases}$$

Hence for any fractional ideal $I=\prod_\mathfrak{p}\mathfrak{p}^{n_\mathfrak{p}}$, $S^{-1}I=\prod_{\mathfrak{p}\cap S=\varnothing}(S^{-1}\mathfrak{p})^{n_\mathfrak{p}}$.

Now take an arbitrary class $[J]\in\mathrm{Cl}(S^{-1}A)$. Factor J in $S^{-1}A$: $J=\prod_{\mathfrak{p}\cap S=\varnothing}(S^{-1}\mathfrak{p})^{m_\mathfrak{p}}$, with only finitely many nonzero $m_\mathfrak{p}\in\mathbb{Z}$. Define the fractional ideal of A by

$$I:=\prod_{\mathfrak{p}\cap S=\varnothing}\mathfrak{p}^{m_\mathfrak{p}}$$

Then by the argument above, $S^{-1}I=J$. Consequently $[J]=\Phi([I])$, proving that Φ is onto.

Problem 3 Let A be a Dedekind domain. Consider a nonzero ideal a in A. Show that every ideal in the quotient ring A/a is principal. Deduce that every ideal of A is generated by at most two elements.

Solution: Let A be Dedekind and $0\neq\mathfrak{a}\lhd A$. Factor

$$\mathfrak{a}=\prod_{i=1}^{r}\mathfrak{p}_i^{e_i} \qquad (\mathfrak{p}_i \text{ distinct}).$$

By the Chinese remainder theorem, $A/\mathfrak{a}\cong\prod_{i=1}^{r}A/\mathfrak{p}_i^{e_i}$. So it suffices to show every ideal of $A/\mathfrak{p}^e$ is principal. This is every ideal in a product of two rings is a product of ideals in each ring.

For a fixed prime $\mathfrak{p}$, the natural map $A\to A_\mathfrak{p}$ induces an isomorphism $A/\mathfrak{p}^e\xrightarrow{\sim}A_\mathfrak{p}/\mathfrak{p}^eA_\mathfrak{p}$. This is because in general we have an isomorphism $A/B\cong(A/C)/(B/C)$ for ideals $C\subset B\subset A$.

But $A_\mathfrak{p}$ is a DVR (Dedekind $\Rightarrow$ localizations at nonzero primes are DVRs). In a DVR with uniformizer π, all ideals are powers of the maximal ideal, hence in the quotient $A_\mathfrak{p}/\mathfrak{p}^eA_\mathfrak{p}$ the ideals are exactly $\frac{\mathfrak{p}^kA_\mathfrak{p}}{\mathfrak{p}^eA_\mathfrak{p}}$ $(0\leq k\leq e)$, and each is generated by the class of π^k. Thus every ideal of $A_\mathfrak{p}/\mathfrak{p}^eA_\mathfrak{p}$, hence of $A/\mathfrak{p}^e$, is principal.

Now let I be an ideal of A. Pick some nonzero a not in I, and consider the image of I in $A/(a)$. It is principal, generated by some $\overline{b} \in A/a$. Pick a lift $b \in A$ of $\overline{b}$. Then I contains the ideal (a, b), and the image of I in $A/(a, b)$ is zero. So $I = (a, b)$ is generated by two elements.

Problem 4 Let d be a square free integer (which is either positive or negative). Determine the integral closure of $\mathbb{Z}[\sqrt{d}]$ (a.k.a. the ring of integers) in $\mathbb{Q}(\sqrt{d})$. (For example, give an explicit $\mathbb{Z}$-basis for the integral closure.)

Solution: We claim that if $K = \mathbb{Q}(\sqrt{d})$ with d square-free, then the ring of integers is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod 4. \end{cases}$$

Equivalently, an explicit $\mathbb{Z}$-basis is

$$\{1, \sqrt{d}\} \quad \text{if } d \equiv 2, 3 \pmod 4, \qquad \left\{1, \tfrac{1+\sqrt{d}}{2}\right\} \quad \text{if } d \equiv 1 \pmod 4.$$

Let $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. The minimal polynomial over $\mathbb{Q}$ is

$$x^2 - 2ax + (a^2 - b^2 d),$$

so α is an algebraic integer iff the coefficients are integers:

$$2a \in \mathbb{Z}, \qquad a^2 - b^2 d \in \mathbb{Z}. \tag{$*$}$$

Write $b = n/r$ in lowest terms with $n \in \mathbb{Z}, r > 0$ and $m = 2a$. Then

$$a^2 - b^2 d = \frac{m^2}{4} - \frac{n^2 d}{r^2} \in \mathbb{Z}.$$

Multiply by $4r^2$:

$$m^2 r^2 - 4n^2 d \in 4r^2\mathbb{Z}.$$

The left hand side is a multiple of r^2, and d is squarefree, n and r are coprime, so $r^2 \mid 4$, so $r = 1$ or 2.

Suppose $r = 1$. Then $b = n \in \mathbb{Z}, a = m/2$. If m even, then $a \in \mathbb{Z}$. Condition (*) gives nothing new, so $\alpha \in \mathbb{Z}[\sqrt{d}]$. If m odd, then $a^2 = \frac{m^2}{4} \equiv \frac{1}{4} \pmod 1$. For (*) to hold, we would need $b^2 d \equiv \frac{1}{4} \pmod 1$, which only happens when $d \equiv 1 \pmod 4$ (this overlaps with Case B below). So if $d \equiv 2, 3 \pmod 4$, the only integrals are with $a, b \in \mathbb{Z}$, i.e. $\mathcal{O}_K \subset \mathbb{Z}[\sqrt{d}]$. The reverse inclusion is clear, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

Suppose $r = 2$. Now $b = n/2$. Then

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} = \frac{m-n}{2} + n \cdot \frac{1+\sqrt{d}}{2}.$$

So $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $\frac{m-n}{2} \in \mathbb{Z}$.

If n is even, then $n^2 d \equiv 0 \pmod 4$. Condition (*) then requires $m^2 \equiv 0 \pmod 4$, so m is even. Suppose both m, n even. Then $\alpha \in \mathbb{Z}[\sqrt{d}]$ (trivial case). If n is odd, then $n^2 d \equiv d \pmod 4$. So condition (*) becomes $m^2 \equiv d \pmod 4$. Now m^2 is either 0 or 1 $\pmod 4$. If $d \equiv 1 \pmod 4$, then we need $m^2 \equiv 1$, so m must be odd. Thus m and n have the same parity. If $d \equiv 2, 3 \pmod 4$, there is no solution (since $d \equiv 2, 3$ cannot be a quadratic residue mod 4).

This implies that m and n have the same parity when $d \equiv 1 \pmod 4$. If $d \equiv 1 \pmod 4$, then indeed $\frac{1+\sqrt{d}}{2}$ is integral (it satisfies $x^2 - x + \frac{1-d}{4} = 0$ with integer constant term). Hence we get a larger order:

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

If $d \equiv 2, 3 \pmod 4$, then the congruence condition forces m, n both even, so the element reduces back to one in $\mathbb{Z}[\sqrt{d}]$. No genuinely new elements appear.