# Algebraic Number Theory Homework 1

Michael Nelson

## Problem 7

### Problem 7.a

**Proposition 0.1.** *Let $R = \mathbb{Z}[\sqrt{-3}]$ and let $I = \langle 2, 1+\sqrt{-3}\rangle$. Then $I^2 = 2I$ but $I \neq \langle 2 \rangle$. In particular, proper ideals in $R$ do not factor uniquely into products of prime ideals.*

*Proof.* We have

$$\begin{aligned} I^2 &= \langle 4, 2+2\sqrt{-3}, -2+2\sqrt{-3}\rangle \\ &= \langle 4, 2+2\sqrt{-3}\rangle \\ &= 2\langle 2, 1+\sqrt{-3}\rangle \\ &= 2I, \end{aligned}$$

where we obtained the second line from the first line from the fact that $-2+2\sqrt{-3}$ can be written as a $\mathbb{Z}$-linear combination of the other two generators:

$$-2+2\sqrt{-3} = -4 + (2+2\sqrt{-3}).$$

To see that $I \neq \langle 2 \rangle$, we assume for a contradiction that $I = \langle 2 \rangle$. Then since $1+\sqrt{-3} \in \langle 2 \rangle$, there exists $a + b\sqrt{-3} \in R$ such that

$$1+\sqrt{-3} = 2a + 2b\sqrt{-3}.$$

But then this implies $2a = 1$, which is a contradiction since $2 \nmid 1$.

To see that this implies proper ideals in $R$ do not factor uniquely into products of primes, assume for a contradiction that proper ideals in $R$ do factor uniquely into products of primes. Then $I^2 = 2I$ would imply $I = \langle 2 \rangle$ since we could cancel $I$ on both sides. However this is a contradiction since $I \neq \langle 2 \rangle$ as was just shown. □

### Problem 7.b

**Proposition 0.2.** *Let $R = \mathbb{Z}[\sqrt{-3}]$ and let $I = \langle 2, 1+\sqrt{-3}\rangle$. Then $I$ is the unique prime ideal of $R$ containing $\langle 2 \rangle$.*

*Proof.* We first note that $I$ is a prime ideal since

$$\begin{aligned} R/\langle 2, 1+\sqrt{-3}\rangle &\cong \mathbb{Z}[T]/\langle T^2+3, 2, 1+T\rangle \\ &\cong \mathbb{F}_2[T]/\langle T^2+3, T+1\rangle \\ &\cong \mathbb{F}_2 \end{aligned}$$

implies $\langle 2, 1+\sqrt{-3}\rangle$ is a maximal ideal (and hence a prime ideal).

To see that $I$ is the *unique* prime ideal of $R$ containing $\langle 2 \rangle$, suppose that $J$ is any prime ideal which contains $\langle 2 \rangle$. This since

$$\begin{aligned} J &\supseteq \langle 2 \rangle \\ &\supseteq \langle 2 \rangle I \\ &= I^2, \end{aligned}$$

we see that $J \supseteq I$ since $J$ is prime. Since $I$ is maximal, we must have $J = I$. □

### Problem 7.c

The reason problem 7.a and 7.b do not contradict the theorem which says that every Dedekind domain admits unique factorization of proper ideals into products of prime ideals is simple: $R$ is not a Dedekind domain. Indeed $R$ is *not* integrally closed in its field of fractions. In particular, $(1+\sqrt{-3})/2$ belongs to $\mathbb{Q}[\sqrt{-3}]$ but does not belong to $\mathbb{Z}[\sqrt{-3}]$, and yet it is a solution to the equation

$$T^2 - T + 1 = 0,$$

where $T^2 - T + 1$ is a monic polynomial with integer coefficients. Thus $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed in $\mathbb{Q}[\sqrt{-3}]$.

## Problem 8

### Problem 8.a

**Proposition 0.3.** *Let $R$ be a PID. Then $R$ is a Dedekind domain.*

*Proof.* We need to show that $R$ is Noetherian, has dimension 1, and is integrally closed in its field of fractions. It is clear that $R$ is Noetherian since every ideal in $R$ is generated by one element and hence is finitely generated.

Let us now show that $R$ has dimension 1. Indeed, choose any nonzero nonunit $a \in R$. Then $\langle a \rangle$ is contained in a maximal ideal, say $a \in \mathfrak{m}$. Then

$$0 \subset \mathfrak{m}$$

is a chain of prime ideals of length 1. Thus $\dim R \geq 1$. To see that $\dim R = 1$, assume for a contradiction that $\dim R > 1$. Choose nonzero prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ in $R$ such that

$$0 \subset \mathfrak{p} \subset \mathfrak{q}.$$

Since $R$ is a PID, we can write $\mathfrak{p} = \langle p \rangle$ and $\mathfrak{q} = \langle q \rangle$ for some $p, q \in R$. Since $\mathfrak{p} \subset \mathfrak{q}$, there exists an $a \in R$ such that $aq = p$. Since $\mathfrak{p}$ is a prime ideal, $aq \in \mathfrak{p}$, and $q \notin \mathfrak{p}$, we see that $a \in \mathfrak{p}$. Since $\mathfrak{p} = \langle p \rangle$, there exists $b \in R$ such that $bp = a$. Then

$$\begin{aligned} p &= aq \\ &= bpq \\ &= pbq \end{aligned}$$

implies $1 = bq$ since $R$ is an integral domain. Thus $q$ must be a unit. This contradicts our assumption that $\mathfrak{q}$ is a prime ideal in $R$ (and hence must be a proper ideal).

It remains to show that $R$ is integrally closed. Let $K$ be the field of fractions of $R$. Suppose for some $x \in K$ we have

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \qquad (1)$$

for some $a_0, \dots, a_{n-1} \in R$. Express $x$ as ratio of two elements in $R$, say $x = b/c$ where $c \neq 0$. Since $R$ is a PID, we may assume that $\langle b, c \rangle = \langle 1 \rangle$. Indeed, if $\langle b, c \rangle \neq \langle 1 \rangle$, then since $R$ is a PID, there exists a nonzero $d \in R$ such that $\langle b, c \rangle = \langle d \rangle$. Thus we have

$$\begin{aligned} bx + cy &= d \\ b'd &= b \\ c'd &= c \end{aligned}$$

for some $x, y, b', c' \in R$. Combine these equations together to obtain

$$\begin{aligned} d &= bx + cy \\ &= b'dx + c'dy \\ &= d(b'x + c'y). \end{aligned}$$

Then we use the fact that $R$ is an integral domain to obtain

$$1 = b'x + c'y.$$

Thus $\langle b', c' \rangle = \langle 1 \rangle$ and

$$\begin{aligned} x &= \frac{b}{c} \\ &= \frac{b'd}{c'd} \\ &= \frac{b'}{c'}. \end{aligned}$$

So replacing $b$ with $b'$ and $c$ with $c'$ if necessary, we may assume that $\langle b, c \rangle = \langle 1 \rangle$.

Plugging in $x = b/c$ in (1), clearing the denominators, and rearranging terms, we obtain

$$b^n = -c(a_{n-1}b^{n-1} + \cdots + a_0 c^{n-1}).$$

In particular, this implies $c \mid b^n$. We claim that in fact $c \mid b$. Indeed, since $\langle b, c \rangle = \langle 1 \rangle$, there exists $x, y \in R$ such that $bx + cy = 1$ and since $c \mid b^n$, there exists $z \in R$ such that $cz = b^n$. Then

$$\begin{aligned} b^{n-1} &= b^n x + b^{n-1} cy \\ &= czx + b^{n-1} cy \\ &= c(zx + b^{n-1} y) \end{aligned}$$

implies $c \mid b^{n-1}$. Iterating this arugment, we see that $c \mid b$. Thus

$$\begin{aligned} \langle 1 \rangle &= \langle b, c \rangle \\ &= \langle c \rangle \end{aligned}$$

implies $c$ is a unit. Therefore $x \in R$, and hence $R$ is integrally closed in $K$. □

### Problem 8.b

**Proposition 0.4.** *Let $R$ be a Dedekind domain. Then $R$ is a UFD if and only if $R$ is a PID.*

*Proof.* Every PID is a UFD, so we just need to show the converse. Suppose that $R$ is a UFD. To show that every nonzero ideal in $R$ is principal, it suffices to show that every prime ideal in $R$ is principal. Indeed, let $I$ be a nonzero ideal in $R$. Since $R$ is a Dedekind domain, there exists a unique factorization of $I$ into prime ideals, say

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

If each $\mathfrak{p}_i$ is principal, then we'd have $\langle p_i \rangle = \mathfrak{p}_i$ for for some $p_i \in R$ each $1 \leq i \leq n$. Then this would imply $I = \langle p_1 \cdots p_n \rangle$. Thus we only need to show that every prime ideal in $R$ is principal, so let $\mathfrak{p}$ be a prime ideal in $R$. Let $a$ be a nonzero element in $\mathfrak{p}$ and let

$$a = p_1 \cdots p_n$$

be the unique factorization of $a$ into irreducible elements. Now

$$\begin{aligned} \mathfrak{p} &\supset \langle a \rangle \\ &= \langle p_1 \cdots p_n \rangle \\ &= \langle p_1 \rangle \cdots \langle p_n \rangle \end{aligned}$$

implies $\mathfrak{p} \supset \langle p_i \rangle$ for some $i$, where $\langle p_i \rangle$ is a prime ideal since $p_i$ is an irreducible element in a UFD. Since $R$ had dimension 1, we must have $\mathfrak{p} = \langle p_i \rangle$. □

## Problem 9

**Proposition 0.5.** *Let $R$ be a Noetherian integral domain with fraction field $K$ and let $J$ be an $R$-submodule of $K$. Then $J$ is finitely generated if and only if there exists a nonzero element $a \in R$ such that $aJ \subseteq R$.*

*Proof.* Suppose first that $J$ is finitely generated, say

$$J = \left\langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \right\rangle .$$

Then $b = b_1 \cdots b_n$ is a nonzero element in $R$ since each $b_i$ is nonzero and since $R$ is an integral domain. Also we have

$$\begin{aligned} bJ &= b_1 \cdots b_n \left\langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \right\rangle \\ &= \langle b_2 \cdots b_n a_1, \ldots, b_1 \cdots b_{n-1} a_n \rangle \\ &\subseteq R. \end{aligned}$$

Conversely, suppose $a$ is a nonzero element in $R$ such that $aJ \subseteq R$. Since $R$ is Noetherian and $aJ$ is an ideal in $R$, there exists $a_1, \ldots a_n \in R$ such that

$$aJ = \langle a_1, \ldots, a_n \rangle . \tag{2}$$

Since $a$ is nonzero and $R$ is an integral domain, this implies

$$J = \left\langle \frac{a_1}{a}, \ldots, \frac{a_n}{a} \right\rangle .$$

Indeed,

$$\begin{aligned} x \in J &\iff ax = b_1 a_1 + \cdots + b_n a_n \text{ for some } b_1, \ldots, b_n \in R \\ &\iff x = b_1 (a_1/a) + \cdots + b_n (a_n/a) \text{ for some } b_1, \ldots, b_n \in R \\ &\iff x \in \langle (a_1/a), \ldots, (a_n/a) \rangle . \end{aligned}$$

□