Name: Tuan Pham
ID: 4652218

Math 8201: General Algebra
Homework #4

10

(9) Problem 1, page 114 in Lang.

Let A be a commutative ring and S a multiplicative subset of A such that $0 \notin S$. We define

$$\mathcal{E} = \{\text{ideals } \underline{a} \text{ of } A \text{ such that } \underline{a} \cap S = \phi\}$$

and let $\mathfrak{p}$ be a maximal of $\mathcal{E}$ under inclusion. We'll show that $\mathfrak{p}$ is a prime ideal.

The first question arising is whether $\mathfrak{p}$ always exists. We'll confirm this fact as the following lemma.

Lemma 1: The family $\mathcal{E}$ defined above has a maximal element.

Proof. Since $0 \notin S$, the trivial ideal $\{0\}$ is contained in $\mathcal{E}$. Thus $\mathcal{E} \neq \phi$. Then $(\mathcal{E}, \subset)$ is a poset. By Zorn's lemma, to show that $(\mathcal{E}, \subset)$ has a maximal element, we only need to show that every totally ordered subset of $\mathcal{E}$ is bounded. Let $\mathcal{E}'$ be a totally ordered subset of $\mathcal{E}$ and

$$J = \bigcup_{I' \in \mathcal{E}'} I'$$

then $I' \subset J$ for all $I' \in \mathcal{E}'$. We'll show that $J \in \mathcal{E}$.

- Check $J \cap S = \phi$:

$$J \cap S = \left(\bigcup_{I' \in \mathcal{E}'} I' \right) \cap S = \bigcup_{I' \in S'} \underbrace{(I' \cap S)}_{\phi} = \phi$$

- Check J is an additive group:

Let $x, y \in J$. Then there exist $I_1, I_2 \in \mathcal{E}'$ such that $x \in I_1$ and $y \in I_2$. Since $\mathcal{E}'$ is totally ordered, either $I_1 \subset I_2$ or $I_2 \subset I_1$. Let's assume $I_1 \subset I_2$. Then $x, y \in I_2$. Since I_2 is an additive group, $x - y \in I_2$. Thus $x - y \in J$.

- Check J absorbs multiplication with A from the left:

Let $a \in A$ and $x \in J$. Then there exists $I \in \mathcal{E}'$ such that $x \in I$. Since I is an ideal, $ax \in I$. Thus $ax \in J$.

Return to the problem. If every element of S is a unit then by definition $\mathfrak{p}$ is a maximal ideal of A, i.e. a maximal proper ideal of A. Then $\mathfrak{p}$ is also a prime ideal. The problem is that elements of S are generally not units. Thus, we'll try to make elements of S units. To do so, the idea is to view A as the ring of fractions over S, $S^{-1}A$, by the following ring-homomorphism

$$\varphi : A \longrightarrow S^{-1}A$$

$$a \longmapsto \frac{a}{1}$$

because $\varphi(s)$ is a unit of $S^{-1}A$ for all $s \in S$.

To show that $\mathfrak{p}$ is prime, we show that it is a preimage of a prime ideal in $S^{-1}A$ under φ. Such a candidate is $\varphi(\mathfrak{p})$. However, $\varphi(\mathfrak{p})$ is in general not an ideal of $S^{-1}A$. Thus, instead, we try to find a maximal ideal in $S^{-1}A$ that contains $\varphi(\mathfrak{p})$.

Assume that we have a maximal ideal $\mathfrak{q}$ in $S^{-1}A$ containing $\varphi(\mathfrak{p})$. Then $\mathfrak{p}' = \varphi^{-1}(\mathfrak{q})$ is an ideal of A and $\mathfrak{p} \subset \mathfrak{p}'$. If there exists $x \in \mathfrak{p}' \cap S$ then $\varphi(x)$ is invertible and $\varphi(x) \in \mathfrak{q}$. Then $\mathfrak{q} = S^{-1}A$, which is a contradiction. Therefore $\mathfrak{p}' \cap S = \emptyset$. By the maximality of $\mathfrak{p}$, we get $\mathfrak{p} = \mathfrak{p}' = \varphi^{-1}(\mathfrak{q})$. Thus $\mathfrak{p}$ is the preimage of a maximal ideal in $S^{-1}A$, which is also prime. Thus $\mathfrak{p}$ is a prime ideal of A.

Now what is left to show is that $\varphi(\mathfrak{p})$ is contained in a maximal ideal of $S^{-1}A$. We break this into two steps:

- Show that $I = (\varphi(\mathfrak{p}))$ - the ideal of $S^{-1}A$ generated by $\varphi(\mathfrak{p})$ - is a proper ideal, i.e. $1 \notin I$.
- Show that any proper ideal I in $S^{-1}A$ is contained in a maximal ideal.

Step 1 Every element of I is of the form $x = x_1 y_1 + \dots + x_k y_k$ where

To show that $\mathfrak{p}$ is prime, we show that it is a preimage of a prime ideal in $S^{-1}A$ under φ. Such a candidate is $\varphi(\mathfrak{p})$. However, $\varphi(\mathfrak{p})$ is in general not an ideal of $S^{-1}A$. Thus, instead, we try to find a maximal ideal in $S^{-1}A$ that contains $\varphi(\mathfrak{p})$.

Assume that we have a maximal ideal $\mathfrak{q}$ in $S^{-1}A$ containing φ
Then $\mathfrak{p}' = \varphi^{-1}(\mathfrak{q})$ is an ideal of A and $\mathfrak{p} \subset \mathfrak{p}'$. If there exists $x \in \mathfrak{p}'$
then $\varphi(x)$ is invertible and $\varphi(x) \in \mathfrak{q}$. Then $\mathfrak{q} = S^{-1}A$, which is a contradi
therefore $\mathfrak{p}' \cap S = \emptyset$. By the maximality of $\mathfrak{p}$, we get $\mathfrak{p} = \mathfrak{p}' = \varphi^{-1}(\mathfrak{q})$. T
$\mathfrak{p}$ is the preimage of a maximal ideal in $S^{-1}A$, which is also prime.
$\mathfrak{p}$ is a prime ideal of A.

Now what is left to show is that $\varphi(\mathfrak{p})$ is contained in a maximal ideal of $S^{-1}A$. We break this into two steps:

- Show that $I = (\varphi(\mathfrak{p}))$ - the ideal of $S^{-1}A$ generated by $\varphi(\mathfrak{p})$ - is a proper ideal, i.e. $1 \notin I$.
- Show that any proper ideal I in $S^{-1}A$ is contained in a maxi ideal.

Step 1 Every element of I is of the form $x = x_1 y_1 + \cdots + x_k y_k$ whe

subset of $\mathcal{E}$ has an upper bound in $\mathcal{E}$. Let $\mathcal{E}'$ be a totally ordered subset of $\mathcal{E}$. Put $J = \bigcup_{I \in \mathcal{E}'} I$. Then $I \subset J$ for all $I \in \mathcal{E}'$. We'll show that $J \in \mathcal{E}$.

- Check $I_0 \subset J$: each $I \in \mathcal{E}'$ contaires I_0, so does J.
- Check J is an additive group, and that J absorbs multiplication with A from the left: this is exactly what we did in Lemma 1. The key is that $\mathcal{E}'$ is totally ordered. We see that Lemma 1 and Lemma 2 guarantee the existence of maximal ideals with quite opposite hypotheses.

(4) Let A be a commutative ring and S a multiplicative subset of A which doesn't contain zero divisors. Put 10

$$T = \{x \in A \mid \text{there exist } s \in S \text{ and } y \in A \text{ with } s = xy\}$$

In other words, if two elements of A have product belonging to S then both of them belong to T. Consequently, $S \subset T$ because $1 \in S$.

(i) First we'll show that T is a multiplicative subset of A.

Because $S \subset T$, $1 \in T$. Let $x, x' \in T$. Then there are $y, y' \in A$ such that $xy \in S$ and $x'y' \in S$. Since S is multiplicatrve, $(xy)(x'y') \in S$. Thus $(xx')(yy') \in S$, whence we get $xx' \in T$.

Next, we'll that T is saturated. Suppose ~~that~~ $xy \in T$. Then there exists $u \in A$ such that $(xy)u \in S$. Thus $x(yu) \in S$, and hence $x \in T$.

By symmetry, $y \in T$.

(ii) We'll show that $S^{-1}A \simeq T^{-1}A$.

In case $0 \in S$, we get $S^{-1}A = \{0\}$. Since $S \subset T$, $0 \in T$. Then $T^{-1}A = \{0\}$. Thus $S^{-1}A \simeq T^{-1}A$. Now we consider the case $0 \notin S$. The most natural map between $S^{-1}A$ and $T^{-1}A$ is

$$\varphi : S^{-1}A \longrightarrow T^{-1}A$$
$$[(a,s)]_S \longmapsto [(a,s)]_T,$$

which is based on the fact that $S \subset T$. We'll show that φ is a ring-isomorphism.

- Check the well-definedness

Suppose that $[(a,s)]_S = [(a',s')]_S$. There exists $u \in S$ such that $u(as' - a's) \in S$. ~~Then by the definition of T, $as' - a's \in S$~~

Because u is also in T, we have $[(a,s)]_T = [(a',s')]_T$. Thus φ is well-defined.

- Check φ is a ring-homomorphism

$$\varphi([(a,s)]_S [(a',s')]_S) = \varphi([(aa',ss')]_S) = [(aa',ss')]_T = [(a,s)]_T [(a',s')]_T$$

$$= \varphi([(a,s)]_S)\,\varphi([(a',s')]_S).$$

Thus φ respects the multiplication.

* Check φ is injective

$$\varphi([(a,s)]_S + [(a',s')]_S) = \varphi([(as'+a's, ss')]_S)$$
$$= [(as'+a's, ss')]_T$$
$$= [(a,s)]_T + [(a',s')]_T$$
$$= \varphi([(a,s)]_S) + \varphi([(a',s')]_S)$$

Thus φ respects the addition. Moreover,

$$\varphi([(0,1)]_S) = [(0,1)]_T.$$

Thus φ is a ring-homomorphism.

* Check injectivity

Because φ is a ring-homomorphism, it suffices to check if $\ker\varphi = 0$.

Suppose that $\varphi([(a,s)]_S) = [(a,s)]_T = [(0,1)]_T$. Then there exists $u \in T$ such that $u(a\cdot 1 - s\cdot 0) = 0$. Thus $ua = 0$. To show that $[(a,s)]_S = [(0,1)]_S$, we need to find $s' \in S$ such that $s'a = 0$.

Since $u \in T$, by the definition of T, there exists $v \in A$ such that $uv = s' \in S$. We have $s'a = (uv)a = v(ua) = v\cdot 0 = 0$.

* Check surjectivity

Let $[(b,t)]_T \in T^{-1}A$. We'll find $[(a,s)]_S$ such that $[(a,s)]_T = [(b,t)]_T$.

Since $t \in T$, there exists $c \in A$ such that $tc = s \in S$. From here we also have $c \in T$. Then, by the reduction law of fractions, we get

$$[(b,t)]_T = [(\underbrace{bc}_{a}, \underbrace{tc}_{s})]_T = [(a,s)]_T$$

Since $s \in S$, $[(a,s)]_T = \varphi([(a,s)]_S)$. Thus $[(b,t)]_T = \varphi([(a,s)]_S)$, and φ is surjective.

Remarks

1) We didn't use the assumption "S contains no zero divisors".

2) An example for this problem is as follow.

$$A = \mathbb{Z}, \quad S = \{4^n : n \geq 0\}.$$

Then $T = \{2^n : n \geq 0\}$. The isomorphism from

$$S^{-1}A = \left\{\frac{m}{4^n} : m \in \mathbb{Z}, n \geq 0\right\} \quad \text{to} \quad T^{-1}A = \left\{\frac{m}{2^n} : m \in \mathbb{Z}, n \geq 0\right\}$$

is $\varphi : S^{-1}A \longrightarrow T^{-1}A$ such that $\varphi\left(\frac{m}{4^n}\right) = \varphi\left(\frac{m}{2^n}\right)$.

6 Let A be an integral domain and S a multiplicative subset such that $0 \notin S$. We'll try to answer whether $S^{-1}A$ is euclidean, PID, UFD provided that A is euclidean, PID, UFD respectively, and vice versa. Since the ring structure of $S^{-1}A$ doesn't change if we replace S by its saturated system T, we can assume that S is already saturated. The advantage

One property that every euclidean domain, PID, UFD has is that every two (nonzero) elements have a greatest common divisor (g.c.d.). With these two conditions (S is saturated, and every two elements of A have a g.c.d.), we have the following lemmas:

Lemma 1 Each fraction $\frac{b}{t} \in S^{-1}A$ can be written in a reduced form $\frac{b'}{t'} \in S^{-1}A$ where g.c.d. $(b', t') = 1$.

Proof Let d be a g.c.d of b and t. Then there are $b', t' \in A$ with $(b', t') = 1$ and $b = b'd$, $t = t'd$. Since $t'd = t \in S$ and S is saturated, $t', d \in S$.

Therefore, $\frac{b}{t} = \frac{b'd}{t'd} = \frac{b'}{t'} \in S^{-1}A$. ■

Lemma 2 $S^{-1}A$ is an integral domain.

Proof Suppose $\frac{x}{s}, \frac{y}{t} \in S^{-1}A$ satisfy $\frac{x}{s} \cdot \frac{y}{t} = \frac{0}{1}$. Then $\frac{xy}{st} = \frac{0}{1}$.

By definition, there exists $u \in S$ such that $u(xy \cdot 1 - st \cdot 0) = 0$. Thus $uxy = 0$. Since $u \in S$, u is nonzero. Since A is an integral domain, we get $x = 0$ or $y = 0$. If $x = 0$ then $\frac{x}{s} = \frac{0}{s} = \frac{0}{1}$. If $y = 0$ then $\frac{y}{t} = \frac{0}{t} = \frac{0}{1}$. therefore $S^{-1}A$ is an integral domain. ■

Now we return to the problem.

(b) First, assuming that A is PID, we'll show that $S^{-1}A$ is also a PID. Let J be a nontrivial ideal of $S^{-1}A$. We'll show that J is principal. Consider the ring-homomorphism $\varphi_S : A \longrightarrow S^{-1}A$, which was defined by $\varphi_S(x) = \frac{x}{1}$ for every $x \in A$. Put $I = \varphi_S^{-1}(J)$. Then I is an ideal of A. Since A is principal, there exists $a \in A$ such that $I = (a)$. Now we'll show that if $\frac{b}{t} \in J$ then $a \mid b$. If this is obtained, then $\frac{b}{t} = \frac{a}{1}\frac{\tilde{b}}{t} \in \frac{a}{1}(S^{-1}A)$. Then $J \subset \frac{a}{1}(S^{-1}A)$. Since $\frac{a}{1} \in J$ and J is an ideal, $\frac{a}{1}(S^{-1}A) \subset J$. Thus $J = \frac{a}{1}(S^{-1}A) = \left(\frac{a}{1}\right)$, which is a principal ideal.

Let $\frac{b}{t} \in J$. We'll show $a \mid b$. Since $\frac{b}{t}$ can be written in a reduced form by cancelling the g.c.d of b and t (Lemma 1), we can assume it suffices to work for the case g.c.d. $(b,t) = 1$. Put $d =$ g.c.d. (a,b). Then there exist $a', b' \in A$ such that $a = a'd$, $b = b'd$ and $(a', b') = 1$. Then

$$\frac{b}{t} = \frac{d}{t}b', \qquad a = da' = \frac{d}{t}(ta') = \frac{d}{t}c \quad \text{where } c = ta'.$$

Since $(b', t) = 1$ and $(b', a') = 1$, we get $(b', ta') = 1$, or $(b', c) = 1$.

Lemma 3 Let A be a PID and $x, y \in A$ such that $(x, y) = 1$. Then $(x) + (y) = A$.

Proof Since $(x) + (y)$ is an ideal, and A is PID, there is $z \in A$ such that

$(x)+(y)=(z)$. Then $x, y \in (z)$. Thus $z \mid x$ and $z \mid y$. Thus $z \mid 1$ and hence z is a unit. Then $(z) = A$.

Return to the problem. Since $(b', c) = 1$, there exist $x, y \in A$ such that $b'x + cy = t$. Then

$$\frac{b}{t} x + \frac{a}{1} y = \frac{d}{t} b'x + \frac{d}{t} cy = \frac{d}{t} (b'x + cy) = \frac{d}{t} t = \frac{d}{1}$$

Since $\frac{b}{t}, \frac{a}{1} \in J$, we get $\frac{d}{1} \in J$. Thus $d \in \varphi_S^{-1}(J) = I$. Thus $d \in (a)$ and $a \mid d$. Since $d \mid b$ and $a \mid d$, we get $a \mid b$.

The converse is not true. Indeed, if we take $S = A \setminus \{0\}$ then $S^{-1}A = K(A)$, the field of fractions of A. A field has only two ideals: $\{0\}$, generated by 0, and the field itself, which is generated by 1. Thus $K(A)$ is always a PID (as long as A is an integral domain). ~~We get a concrete example of A~~, we have many examples of an integral domain which is not a PID, such as $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[X]$, $\mathbb{Z}[X_1, \ldots, X_n]$, ...

(c) First, assuming that A is factorial, we'll show that $S^{-1}A$ is also factorial. To do so, we'll use the following criterion of factorial rings:

"An integral domain R is factorial if and only if every $r \in R \setminus \{0\}$ admits a factorization $r = u p_1 \cdots p_k$ with p_i's are prime and $u \in U(R)$."

12

For each fraction $\frac{b}{t} \in S^{-1}A$, we have the factorization of b and t in A as follow $b = b_0 p_1 \cdots p_k$ where $b_0 \in U(A)$ and p_i's are prime,

$t = t_0 q_1 \cdots q_l$ where $t_0 \in U(A)$ and q_j's are prime.

Then $\frac{b}{t} = \frac{b_0 p_1 \cdots p_k}{t_0 q_1 \cdots q_l} = \frac{b_0}{t_0} \frac{p_1}{1} \cdots \frac{p_k}{1} \frac{1}{q_1} \cdots \frac{1}{q_l}$.

The proof will finish if we can do 3 things:

- Show that $\frac{u}{v}$ is a unit if u and v are units,
- Show that $\frac{p}{1}$ is prime (or a unit) if p is prime,
- Show that $\frac{1}{p}$ is prime (or a unit) if p is prime.

(1) Check the first one

Let u and v be units in A. Then $\frac{u}{v} \frac{u^{-1}}{v^{-1}} = \frac{uu^{-1}}{vv^{-1}} = \frac{1}{1}$. Thus $\frac{u}{v}$ is a unit in $S^{-1}A$.

(2) Check the second one

Suppose p is a prime in A and $\frac{p}{1} = \frac{a}{s} \cdot \frac{b}{t}$. Then $\frac{p}{1} = \frac{ab}{st}$. Thus $pst - ab = 0$. Thus $pst = ab$. Thus $p \mid (ab)$. Since p is prime, we get either $p \mid a$ or $p \mid b$. We can assume $p \mid a$. Then $a = a'p$ for some $a' \in A$. Then ~~$0 = pst - ab = pst - a'pb = p(st - a'b)$. Since $p \neq 0$, $st = a'b$. Thus $\frac{a'}{s} \frac{b}{t} = 1$. We have Thus $\frac{b}{t}$ is a unit in $S^{-1}A$.~~

Then $\frac{a}{s} = \frac{pa'}{s} = \frac{p}{1}\frac{a'}{s}$. Thus $\frac{p}{1} \mid \frac{a}{s}$ in $S^{-1}A$. Thus $\frac{p}{1}$ is prime (or a unit) in $S^{-1}T$.

- Check the third one

Suppose p is a prime in A and $\frac{1}{p} = \frac{a}{s}\cdot\frac{b}{t}$. Then $\frac{1}{p} = \frac{ab}{st}$. Thus $pab = st$. Thus $p \mid (st)$. Since p is prime, we get either $p \mid s$ or $p \mid t$.

We can assume $p \mid s$. Then $s = pc$ for some $c \in A$. Then

$$\frac{a}{s} = \frac{a}{pc} = \frac{1}{p}\cdot\frac{a}{c}$$

Thus $\frac{1}{p} \mid \frac{a}{s}$ in $S^{-1}A$. Thus $\frac{1}{p}$ is a prime (or a unit) in $S^{-1}A$.

The converse in not true in general. Indeed, we can take $S = A\setminus\{0\}$ so that $S^{-1}A = K(A)$, the field of fractions of A. A field is always factorial because every nonzero element is a unit. However, we can have at least one example of an integral domain which is not factorial, namely $A = \mathbb{Z}[i\sqrt{5}]$.

(a) The direction to solution is as follow.

A euclidean domain is actually a pair (A, φ) ~~with~~ where A is a ring and φ a euclidean function on it. To reject the statement of the problem, we need to find a pair (A, φ) ~~such~~ an a suitable

multiplicative subset S of A and show that we couldn't find any euclidean function Ψ on $S^{-1}A$. We've tried a lot of examples such that $A = \mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}[X]$ and used proof by contradiction, but it seemed so hard.

↑ Professor Ciocan said in one lecture that it's very hard to find an example of a PID which is not a euclidean domain. We have the chain of deduction: (A,φ) is euclidean $\Rightarrow$ A is PID $\xRightarrow{(6)}$ $S^{-1}A$ is a PID. Thus, it's very hard to find (A,φ) such that $S^{-1}A$ is not euclidean. We should lean to show that $S^{-1}A$ is also euclidean, i.e. to seek for a proof rather than a counterexample. Thus, we should construct a euclidean function Ψ on $S^{-1}A$ from φ. The idea comes from the following property of euclidean functions.

Lemma Let (A,φ) be a euclidean domain. If a and b are associated then $\varphi(a) = \varphi(b)$.

Proof Since a and b are associated, $a|b$ and $b|a$. Thus $\varphi(a) \le \varphi(b)$ and $\varphi(b) \le \varphi(a)$. Thus $\varphi(a) = \varphi(b)$ ⊠

The idea of construction is as follow:

↑ Since s and $1/s$ are viewed as units in $S^{-1}A$, we don't need to care about the fractions. In other words, $\Psi\left(\frac{a}{s}\right) = \Psi(a)$.

Based on the fact that a euclidean domain is also factorial, we have a factorization of a into primes. Then we eliminate all prime factors that belong to S to get the "core" of a in $S^{-1}A$. Then we define $\Psi(a) := \varphi(\bar{a})$ where $\bar{a}$ is the core of a.

Specifically, our proof has three steps:

1) Show that each $a \in A \setminus \{0\}$ has a representation $a = \bar{a}\, t$ where $t \in S$ and $(\bar{a}, s) = 1$ for all $s \in S$. Moreover, $\bar{a}$ is unique up to the multiplication with units.

2) Define the function $\Psi : (S^{-1}A) \setminus \{0\} \longrightarrow \mathbb{N}$ as

$$\Psi\left(\frac{a}{s}\right) := \varphi(\bar{a})$$

3) Show that Ψ is a euclidean function on $S^{-1}A$.

Step 1 First we'll show the existence of $\bar{a}$. Since A is also factorial, a can be factorized into primes. Let $\mathcal{P}$ be the set of all primes in A. We can write

$$a = u \prod_{p \in \mathcal{P}} p^{\nu(p)},$$

where u is a unit, $\nu(p) \geq 0$, and $\nu(p) = 0$ for all but finitely many $p \in \mathcal{P}$. Then $S \cap \mathcal{P}$ is the set of all primes of A lying in S. We define

$$\bar{a} = u \prod_{p \in \mathcal{P} \setminus S} p^{\nu(p)} \qquad \text{and} \qquad t = \prod_{p \in \mathcal{P} \cap S} p^{\nu(p)}$$

with the usual convention that the product is 1 if there is no factor.

Then $a = \bar{a}t$. Since a doesn't contain any prime in S, it is relatively prime to all elements of S.

Now we'll show the uniqueness up to a unit factor of $\bar{a}$. Suppose that we have $a = a_1 t_1 = a_2 t_2$ where $t_i \in S$, and $(a_i, s) = 1$ for all $s \in S$. Then $(t_1, a_2) = 1$. Since $t_1 \mid (a_2 t_2)$, we get $t_1 \mid t_2$. By symmetry, $t_2 \mid t_1$. Thus t_1 and t_2 are associated, i.e. there exists a unit $u \in A$ such that $t_1 = u t_2$. Therefore, $a = a_2 t_2 = a_1 t_1 = a_1 (u t_2) = (u a_1) t_2$. Thus $a_2 = u a_1$.

Thus a_1 and a_2 are associated.

Step 2 We define the following map $\Psi : (S^{-1}A) \setminus \{0\} \longrightarrow \mathbb{N}$

$$\Psi\left(\frac{a}{s}\right) = \varphi(\bar{a}).$$

- Check the well-definedness

First we see from the above lemma that φ of two associated elements are the same. Thus $\varphi(\bar{a})$ is definite, regardless of the choice of $\bar{a}$, as soon as a is given. Secondly, suppose that $\frac{a}{s} = \frac{b}{t} \neq 0$, we'll show that $\varphi(\bar{a}) = \varphi(\bar{b})$. We have $at = bs$. We write $a = \bar{a} t_1$, $b = \bar{b} s_1$ where $t_1, s_1 \in S$. Then $(\bar{a} t_1) t = (\bar{b} s_1) s =: c$. Then $c = \bar{a}(t_1 t) = \bar{b}(s_1 s)$. Then $\bar{a}$ and $\bar{b}$ are representatives of $\bar{c}$. By the uniqueness of $\bar{c}$ as shown in step 1, $\bar{a}$ and $\bar{b}$ are associated. Thus $\varphi(\bar{a}) = \varphi(\bar{b})$.

Step 3 We'll show that Ψ is a euclidean function on $S^{-1}A$.

The idea of division is as follow. Take $\frac{a}{s}$ and $\frac{b}{t}$ in $S^{-1}A \setminus \{0\}$.

- Take the core of a and b: $\bar{a}, \bar{b}$
- Divide $\bar{a}$ by $\bar{b}$ as two elements in A: $\bar{a} = \bar{b}q + r$
- By ignoring all factors in the numerators and denominators that belong to S, we obtain a division in $S^{-1}A$.

Specifically, we write $a = \bar{a}s'$, $b = \bar{b}t'$ where $s', t' \in S$. Then

$$\frac{a}{s} = \frac{s'}{s}\bar{a} = \frac{s'}{s}(\bar{b}q + r) = \frac{s't'}{st'}\bar{b}q + \frac{s'r}{s} = \frac{s'}{st'}bq + \frac{s'r}{s} = \frac{b}{t}\left(\frac{ts'}{st'}q\right) + \frac{s'r}{s}.$$

- If $r = 0$ then $\frac{s'r}{s} = 0$.
- If $r \neq 0$ then $\varphi(r) < \varphi(\bar{b})$. We write $r = \bar{r}r'$ where $r' \in S$. Then

$$\Psi\left(\frac{s'r}{s}\right) = \Psi\left(\frac{s'r'}{s}\bar{r}\right) = \varphi(\bar{r}) \quad \text{(by the definition of } \Psi\text{)}$$

$$\Psi\left(\frac{b}{t}\right) = \Psi\left(\frac{t'}{t}\bar{b}\right) = \varphi(\bar{b}) \quad \text{(by the definition of } \Psi\text{)}$$

Since $\bar{r} \mid r$, we have $\varphi(\bar{r}) \leq \varphi(r)$. Thus,

$$\Psi\left(\frac{s'r}{s}\right) = \varphi(\bar{r}) \leq \varphi(r) < \varphi(\bar{b}) = \Psi\left(\frac{b}{t}\right)$$

Therefore we obtain a division in $S^{-1}A$. The quotient is $\frac{ts'}{st'}q$, and the remainder is $\frac{s'r}{s}$. What is left is to show that $\Psi\left(\frac{a}{s}\right) \leq \Psi\left(\frac{a}{s}\frac{b}{t}\right)$ for all $\frac{a}{s}, \frac{b}{t} \in (S^{-1}A) \setminus \{0\}$. We have

$$\Psi\left(\frac{a}{s}\right) = \Psi\left(\frac{s'}{s}\bar{a}\right) = \varphi(\bar{a})$$

$$\Psi\left(\frac{a}{s}\frac{b}{t}\right) = \Psi\left(\frac{s'\bar{a}}{s}\cdot\frac{t'\bar{b}}{t}\right) = \varphi(\bar{a}\bar{b})$$

Since $\varphi(\bar{a}) \leq \varphi(\bar{a}\bar{b})$, we get $\Psi\left(\frac{a}{s}\right) \leq \Psi\left(\frac{a}{s}\frac{b}{t}\right)$.

For example, $A = \mathbb{Z}$ and $S = \{2^n : n \geq 0\}$. Then $S^{-1}A = \{\frac{m}{2^n} : m \in \mathbb{Z}, n \geq 0\}$.

Take $x = \frac{23}{2^8}$ and $y = \frac{7}{24}$. ~~We have~~ The core of x is 23, of y is 7. We have $23 = 7.3 + 2$. Thus,

$$\frac{23}{2^8} = \frac{7.3+2}{2^8} = \frac{7}{2^4}\cdot\underbrace{\frac{3}{2^4}}_{\text{quotient}} + \underbrace{\frac{1}{2^7}}_{\text{remainder}}.$$

Like in the case (b), (c), the converse is not true in general. We take $S = A\setminus\{0\}$. Then $S^{-1}(A) = K(A)$, which is always a field and thus euclidean. For any integral domain A that is not euclidean, for instance $A = \mathbb{Z}[i\sqrt{5}]$, $A = \mathbb{Z}[X_1, X_2], \ldots$, we get a counterexample.

11 Problem 6, Lang p. 115

Let A be a factorial ring and p a prime of A. We put $S = A\setminus(p)$. Then we get the local ring of A at p, namely $A_{(p)} := S^{-1}A$. We'll show that $A_{(p)}$ is a principal ring.

First, we'll show that $\frac{p}{1}$ is the only prime element of $A_{(p)}$. ~~According to part (c), Problem 6 above, $A_{(p)}$ is factorial and for every prime $q \in A$,~~

Because $S = A \setminus (p)$, $xy \in S$ implies $xy \notin (p)$; thus $x \notin (p)$ and $y \notin (p)$ because (p) is an ideal; thus $x \in S$ and $y \in S$. Therefore S is saturated.

Consider $\frac{a}{s} \in A_{(p)}$. Since A is factorial, there exists factorizations into prime elements of a and s in A.

$$a = a_0 p_1 \cdots p_k, \quad s = s_0 q_1 \cdots q_\ell,$$

where a_0, s_0 are units in A, p_i and q_j are prime elements of A. Since S is saturated, $s_0, q_1 \cdots, q_\ell \in S$. Then we get

$$\frac{a}{s} = \frac{a_0}{s_0} \frac{p_1 \cdots p_k}{q_1 \cdots q_\ell} = \underbrace{\frac{a_0}{s_0} \frac{1}{q_1 \cdots q_\ell}}_{\text{unit of } A_{(p)}} p_1 \cdots p_k$$

Thus any element $\frac{a}{s} \in A_{(p)}$ can be written in the form $\frac{a}{s} = u \frac{p_1}{1} \cdots \frac{p_k}{1}$ where u is a unit of $A_{(p)}$ and p_i's are prime elements in A. By part (c), Problem 6 above, $A_{(p)}$ is factorial. Thus each element $\frac{q}{1}$, where q is a prime in A, must be either a unit or a prime in $A_{(p)}$. Moreover, each prime element in $A_{(p)}$ must be of the form $u \frac{q}{1}$ where u is a unit in $A_{(p)}$ and q is a prime in A. If $q \neq (p)$ then $q_1 \notin (p)$; thus $q_1 \in A \setminus (p) = S$; thus $\frac{q}{1}$ is a unit of $A_{(p)}$. Therefore, the only possible prime of $A_{(p)}$ is $u \frac{p}{1}$. We know that $A_{(p)}$ is a local ring with the maximal ideal

$$\underline{m} = S^{-1}(p) = \left\{ \frac{a}{s} : a \in (p), s \notin (p) \right\}$$

Thus $\{m\} \subset \left(\frac{p}{1}\right)$. Since p is not a unit in A, $1 \notin \left(\frac{p}{1}\right)$. Thus $\left(\frac{p}{1}\right)$ is an proper ideal of $A_{(p)}$. Thus $\left(\frac{p}{1}\right) \subset \underline{m}$. Thus $\underline{m} = \left(\frac{p}{1}\right)$ and $\frac{p}{1}$ is a prime of $A_{(p)}$ by the maximality of $\underline{m}$. Therefore, $\frac{p}{1}$ is the only prime element, up to a unit factor, of $A_{(p)}$.

Next, since $A_{(p)}$ is factorial, each element in it is a product of units and prime elements. Since all prime elements of $A_{(p)}$ are of the form $u\frac{p}{1}$, where u is a unit, every element of $A_{(p)}$ is of the form $u\frac{p^k}{1}$ where u is a unit in A and $k \geq 0$. Let J be an ideal of $A_{(p)}$ such that $J \neq \{0\}$, $J \neq A_{(p)}$, we'll show that J is a principal ideal. Let k be the smallest nonnegative integer such that $\frac{p^k}{1} \in J$. Then $k \geq 1$ because $J \neq A_{(p)}$. Then $\left(\frac{p^k}{1}\right) \subset J$. We want to show that $\left(\frac{p^k}{1}\right) = J$. Every element $x \in J$ is of the form $x = u\frac{p^h}{1}$ where u is a unit of $A_{(p)}$ and $k \leq h$. Then $x = \frac{p^k}{1}\left(\frac{up^{h-k}}{1}\right) \in \left(\frac{p^k}{1}\right)$.

Thus $J \subset \left(\frac{p^k}{1}\right)$, and $J = \left(\frac{p^k}{1}\right)$. Therefore J is a principal ideal.

10

(7) Let A be a factorial ring, but not a field, such that $U(A)$ is a finite group. We'll show that there are infinitely many non-associated primes in A. We will following three steps:

1) Show that A is an infinite set.

2) Show that there is at least a prime element in A.

3) Show that there are infinitely many non-associated primes in A.

Step 1 We'll show that if A is an integral domain and A is finite then A is a field. To do so, we show that each element $x \in A \setminus \{0\}$ is invertible. Since A is finite, the entries of the sequence $1, x, x^2, x^3, \dots$ couldn't be pairwise distinct. Thus there exist $n < m$ such that $x^n = x^m$. Since A is an integral domain, we can apply the cancellation law to get $x^{m-n} = 1$. Thus x is invertible.

Step 2 Suppose by contradiction that there is no prime element in A. Since A is factorial, each element $a \in A$ is a product of units and primes in A. Since A has no primes, a is a product of units. Thus a is also a unit. Thus $A = U(A)$, which is finite. This is impossible by Step 1.

Step 3 Suppose by contradiction that there are only finitely many primes in A, called $p_1, \dots, p_m$. Since A is factorial, each element $a \in A$ is of the form $a = u p_1^{n_1} \cdots p_m^{n_m}$ where $u \in U(A)$ and $n_1, \dots, n_m \geq 0$. Thus,

$$A = \left\{ u p_1^{n_1} \cdots p_m^{n_m} \mid u \in U(A),\ n_i \geq 0 \right\}$$

We have $U(A)$ is finite. If we can show that each p_i has finite order then A is a finite set, which is a contradiction. By symmetry, it suffices to show that p_1 has finite order.

For each $n \geq 0$, we put $a_n = p_1^n p_2 \cdots p_m + 1$. Then a_n has no prime divisor in A. Indeed, suppose $p_i \mid a_n$ for some $i = 1, \ldots, m$. Then $p_i \mid (p_1^n p_2 \cdots p_m + 1)$. Then $p_i \mid 1$, which means p_i is a unit. This is a contradiction. Therefore, a_n must be a unit. Since $a_n \in U(A)$ for all $n \geq 0$ and $U(A)$ is a finite set, there exist $r < s$ such that $a_r = a_s$. Then

$$p_1^r p_2 \cdots p_m + 1 = p_1^s p_2 \cdots p_m + 1$$

Thus, $p_1^r p_1 \cdots p_m (1 - p_1^{s-r}) = 0$. Then $p_1^{s-r} = 1$, which implies p_1 is a unit. This is a contradiction.

10 (8) We'll describe all prime ideals of $\mathbb{Z}[X]$.

Let I be a prime ideal of $\mathbb{Z}[X]$. Then $I \neq \{0\}$ and $I \neq \mathbb{Z}[X]$.

For each $f(X) \in \mathbb{Z}[X] \setminus \{0\}$ has an integer content because

$$\mathrm{cont}(f) = \text{g.c.d.}(a_0, a_1, \ldots, a_n)$$

where $f(X) = a_n X^n + \cdots + a_1 X + a_0$. Because $\mathbb{Z}$ has only two units, 1 and -1, we can choose $\mathrm{cont}(f)$ to be the positive one. Then we put

$$m_f = (\deg(f), \mathrm{cont}(f)) \in (\mathbb{N} \cup \{0\}) \times \mathbb{N}$$

This Cartesian product is endowed with the lexicographical order

$$(x, y) \leq (z, t) \iff x < z \text{ or } \begin{cases} x = z \\ y \leq t \end{cases}$$

Thus, we can compare m_f with m_g for any $f, g \in \mathbb{Z}[X] \setminus \{0\}$.

To describe the ideal I, we follow the following steps:

Step 1: Take $h(X) \in I \setminus \{0\}$ such that m_h is smallest possible, i.e. take the polynomials in $I \setminus \{0\}$ with smallest degree, then choose among them a polynomial h with smallest content. Then we'll show that

1) If $\deg h > 0$ then $I = (h)$ - the ideal generated by $h(X)$ - and $h(X)$ is a prime of $\mathbb{Z}[X]$. Conversely, if $h(X)$ is a prime of $\mathbb{Z}[X]$ then $I = (h)$ is a prime ideal.

2) If $\deg h = 0$ then $h(X) = \pm p$ for some prime number $p \in \mathbb{Z}$.

Step 2: We deal with the case $p \in I$ where p is some prime number in $\mathbb{Z}$. We'll show that

1) $\pm p\mathbb{Z}$ are the only ~~prime~~ elements in $\mathbb{Z} \setminus \{0\}$ belonging to I.

2) If $I \setminus (p) = \phi$ then $I = (p)$ is a prime ideal of $\mathbb{Z}[X]$.

3) If $I \setminus (p) \neq \phi$ then we can take $g \in I \setminus (p)$ with smallest m_g. Then $I = (p, g(X))$ - the ideal generated by two elements p and $g(X)$.

Up to here, we can conclude that there are only two kinds of prime ideals in $\mathbb{Z}[X]$:

- First kind: principal ideals $I = (h(X))$ where $h(X)$ is a prime element of $\mathbb{Z}[X]$. This kind includes the case $h(X) = p$ because a prime in $\mathbb{Z}$ is also a prime in $\mathbb{Z}[X]$.
- Second kind: ideals generated by two element $I = (p, g(X))$ where p is a prime in $\mathbb{Z}$ and $g(X) \in I \setminus (p)$.

There is one problem with the second kind: $g(X)$ hasn't been fully characterized because $g(X)$ was chosen based on the assumption that I was already given. Therefore, we need a detail characterization for $g(X)$.

Step 3: we suggest a way to choose $g(X)$ to guarantee that $I = (p, g(X))$, is always a prime ideal of $\mathbb{Z}[X]$. The steps are:

1) If $I = (p, g(X))$ is an ~~prime~~ ideal, we can assume that $g(X) = a_n X^n + \dots + a_1 X + a_0$ where $a_i \in \{0, 1, \dots, p-1\}$ and $a_n \neq 0$.

2) For $g(X) \in \mathbb{Z}[X]$ with coefficients in $\{0, 1, \dots, p-1\}$, if $I = (p, g(X))$ is a prime ideal then g is a prime in $(\mathbb{Z}/p\mathbb{Z})[X]$ if viewed as an element in $(\mathbb{Z}/p\mathbb{Z})[X]$. (and m_g is smallest possible in $I \setminus (p)$)

3) ~~For~~ If $g(X) \in \mathbb{Z}[X]$ with coefficients in $\{0, 1, \dots, p-1\}$ and is a prime in $(\mathbb{Z}/p\mathbb{Z})[X]$ then $I = (p, g(X))$ is a prime ideal.

Now we have the following conclusions:

There are only two kinds of prime ideals in $\mathbb{Z}[X]$.

- Generated by one element: $I = (h(X))$ where $h(X)$ is ~~a~~ any prime in $\mathbb{Z}[X]$.
- Generated by two elements: $I = (p, g(X))$ where p is ~~a~~ any prime in $\mathbb{Z}$ and $g(X)$ is any polynomial in $\mathbb{Z}[X]$ ~~if~~ with coefficients in $\{0, 1, \dots, p-1\}$ and is a prime in $(\mathbb{Z}/p\mathbb{Z})[X]$ is viewed as a polynomial on $\mathbb{Z}/p\mathbb{Z}$.

Details of proofs

Step 1 Take $h(X) \in I \setminus \{0\}$ such that m_h is smallest possible.

1) Suppose that $\deg h > 0$. ~~Let $g(X)$ be in I arb~~ Take $g(X) \in I \setminus \{0\}$ arbitrarily. We show that $h(X)$ divides $g(X)$ in $\mathbb{Z}[X]$.

Since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, $\mathbb{Q}[X]$ is a euclidean domain. We view $h(X)$ and $g(X)$ as two elements in $\mathbb{Q}[X]$. Then there exist $q(X), r(X) \in \mathbb{Q}[X]$ such that $g(X) = h(X)\, q(X) + r(X)$ where $r(X) = 0$ or $\deg r(X) < \deg h(X)$. Suppose by contradiction that $r(X) \neq 0$. Then $\deg r(X) < \deg h(X)$. Let n be an integer (non-zero) such that $nq(X), nr(X) \in \mathbb{Z}[X]$.

Then $\underbrace{nq(X)}_{\in I} = \underbrace{h(X)}_{\in I}\ \underbrace{(nq(X))}_{\in \mathbb{Z}[X]} + nr(X)$. Thus $nr(X) \in I$. Moreover,

$\deg(nr(X)) = \deg(r(X)) < \deg(h(X))$. Thus $m_{nr} < m_h$. This contradicts the assumption that m_h is the smallest possible of an $h \in I$. Therefore, $r(X) = 0$. We get $g(X) = h(X)q(X)$. We'll show that $q \in \mathbb{Z}[X]$.

Since $g, h \in \mathbb{Z}[X] \setminus \{0\}$, $\text{cont}(g) = n_1 \in \mathbb{N}$, $\text{cont}(h) = n_2 \in \mathbb{N}$. Since $q \in \mathbb{Q}[X] \setminus \{0\}$, $\text{cont}(q) = \frac{a}{b}$ with $a, b \in \mathbb{N}$ and $\gcd(a,b) = 1$. By Gauss's lemma, we have $\text{cont}(g) = \text{cont}(h)\text{cont}(q)$, or $n_1 = n_2 \frac{a}{b}$.

Thus $b \mid (n_2 a)$. Since $(a,b) = 1$, we have $b \mid n_2$. Put $n_2 = bc$, where $c \in \mathbb{N}$. We write $h = n_2 \bar{h}$ and $q = \frac{a}{b}\bar{q}$ where $\bar{h}(X)$ and $\bar{q}(X)$ are primitive polynomials in $\mathbb{Z}[X]$. Then

$$g = hq = n_2 \bar{h} \frac{a}{b} \bar{q} = ac\bar{h}\bar{q} = \bar{h}(ac\bar{q})$$

Thus $\bar{h}(ac\bar{q}) \in I$. Since I is a prime ideal, either $\bar{h} \in I$ or $ac\bar{q} \in I$.

- If $\bar{h} \in I$ then $m_{\bar{h}} \geq m_h$ by the choice of $h(X)$. Since $\deg \bar{h} = \deg h$, $\text{cont}(\bar{h}) \geq \text{cont}(h)$. Thus $1 \geq n_2$, which implies $n_2 = 1$. Thus $bc = 1$ and hence $b = c = 1$. Then $\text{cont}(q) = a \in \mathbb{N}$. Thus $q(X) \in \mathbb{Z}[X]$.
- If $ac\bar{q} \in I$ then $n_2 q = bcq = bc\frac{a}{b}\bar{q} = ac\bar{q} \in I$. Since I is prime, $n_2 \in I$ or $q \in I$. Since $\deg n_2 = 0 < \deg h$, $n_2 \notin I$. Thus $q(X) \in I \subset \mathbb{Z}[X]$.

Therefore we always have $q(X) \in \mathbb{Z}[X]$. Consequently, $g(X) \in h(X)\mathbb{Z}[X]$ for all $g \in I \setminus \{0\}$. Thus $I = (h(X))$. Since I is a prime ideal, $h(X)$ is also a prime in $\mathbb{Z}[X]$. (in fact $h(X)$ is only irreducible, but because $\mathbb{Z}[X]$ is factorial, it's also a prime).

Conversely, if $h(X)$ is a prime element of $\mathbb{Z}[X]$ then $(h(X))$ is a prime ideal of $\mathbb{Z}[X]$.

2) Suppose that $\deg h = 0$. We'll show that $h(X) = p$, a prime number in $\mathbb{Z}$. Since $\deg h = 0$, $h(X) = n$, some nonzero integer in $\mathbb{Z}$. Since I is a prime ideal, it doesn't contain ± 1. Thus $n \neq \pm 1$. If n is not a prime number, then we can write $n = ab$ where $1 < |a|, |b| < |n|$. Since I is a prime ideal and $n = ab \in I$, either $a \in I$ or $b \in I$. Suppose that $a \in I$. Then

$$m_a = (\deg a, \operatorname{cont}(a)) = (0, |a|) < (0, |n|) = m_h.$$

This contradict the choice of $h(X)$ at the beginning. Thus $h(x) = \pm p$ for some prime number $p \in \mathbb{Z}$.

Step 2 Here we only consider the case there exists a prime $p \in \mathbb{N}$ such that $p \in I$.

28

1) We'll show that $\pm p\mathbb{Z}$ are the only elements in $\mathbb{Z}\setminus\{0\}$ belong to I.

Suppose by contradiction that there exists $n \in I\setminus\{0\}$ such that $n \in \mathbb{Z}$ and $n \notin p\mathbb{Z}$. Then $(n,p)=1$. Since $\mathbb{Z}$ is a priciple ideal, $(n)+(p)=(1)$.

Thus $1 \in (n)+(p) \subset I$. This is a contradiction.

2) If $I\setminus(p) = \phi$ then $I=(p)=p\mathbb{Z}[X]$. This is a prime ideal in $\mathbb{Z}[X]$ because p is a prime in $\mathbb{Z}[X]$.

3) Suppose that $I\setminus(p) \neq \phi$. Then we can take $g(X) \in I\setminus(p)$ with smallest m_g, i.e. take the polynomials in $I\setminus(p)$ with smallest degree, then choose among the a polynomial $g(X)$ with smallest content. We'll show that $I=(p, g(X))$. We have $(p, g(X)) \subset I$. Suppose by contradiction that $(p, g(X)) \neq I$. Then we continue to choose $f(X) \in I\setminus(p, g(X))$ with smallest possible m_f. By viewing $f(X)$ and $g(X)$ as two polynomials in $\mathbb{Q}[X]$, we have the division $f(X)=g(X)q(X)+r(X)$ where $q(X), r(X) \in \mathbb{Q}[X]$ and either $r=0$ or $\deg r < \deg g$.

If $r \neq 0$ then $\deg r < \deg g$. Let $n \in \mathbb{N}$ be such that $nq, nr \in \mathbb{Z}[X]$.

Then $\underbrace{nf(X)}_{\in I} = \underbrace{g(X)}_{\in I}\underbrace{(nq(X))}_{\in \mathbb{Z}[X]} + \underbrace{nr(X)}_{\in \mathbb{Z}[X]}$

Thus $nr(X) \in I \setminus \{0\}$. Since $\deg(nr(X)) \leq \deg = \deg r(X)$

$< \deg g(X)$,

and $g(X)$ was chosen (in $I \setminus (p)$) such that m_g is smallest possible, we must have $nr(X) \in (p)$. Thus $nf(X) \in (p, g(X))$. We consider two cases.

* If $p \nmid n$ then $(n, p) = 1$. Thus there exist $u, v \in \mathbb{Z}$ such that $nu + pv = 1$.

We have $f(X) = (nu+pv) f(X) = \underbrace{u(nf(X))}_{\in (p, g(X))} + \underbrace{pvf(x)}_{\in (p)} \in (p, g(X))$.

This is a contradiction.

* If $p \mid n$:

What we get until here is the following statement:

[If $n \in \mathbb{N}$ be such that $nq, nr \in \mathbb{Z}[X]$ then $p \mid n$ and $nr(X) \in (p)$] (*)

We put $cont(q) = \frac{a}{b}$, $cont(r) = \frac{c}{d}$ where $a, b, c, d \in \mathbb{N}$ and $(a, b) = (c, d) = 1$.

We write $q(X) = \frac{a}{b} \bar{q}(X)$, $r(X) = \frac{c}{d} \bar{r}(X)$ where $\bar{q}(X)$ and $\bar{r}(X)$ are primitive polynomials in $\mathbb{Z}[X]$. If we choose $n = lcm(b, d)$ then nq, $nr \in \mathbb{Z}[X]$. By the statement (*), we have $p \mid n$ and $nr(X) \in (p)$.

We ~~put~~ write $n = bb' = dd'$ with $(b', d') = 1$. We have

$$nf(X) = ng(X) q(X) + nr(X)$$

or $$nf(X) = bb' g(X) \frac{a}{b} \bar{q}(X) + dd' \frac{c}{d} \bar{r}(X)$$

$$= ab' g(X) \bar{q}(X) + cd' \bar{r}(X)$$

Since $nr(X) \in (p)$, we have $cd'\bar{r}(X) \in (p)$. Thus $p \mid cd'\bar{r}(X)$. Since $\bar{r}(X)$ is a primitive polynomial, $p \nmid \bar{r}(X)$. Thus $p \mid cd'$. Then

$$ab' g(X) \bar{q}(X) = nf(X) - cd'\bar{r}(X) \in (p)$$

Thus $p \mid (ab' g(X) \bar{q}(X))$. Since $\bar{q}(X)$ is a primitive polynomial, $p \nmid \bar{q}(X)$. Since $g(X) \in I \setminus (p)$, $p \nmid g(X)$. Thus $p \mid ab'$. What we have until now are

$$\begin{cases} (b', d') = 1 & (1) \\ p \mid (bb') & (2) \\ p \mid (dd') & (3) \\ p \mid (cd') & (4) \\ p \mid (ab') & (5) \end{cases} \qquad \begin{cases} (a, b) = 1 & (6) \\ (c, d) = 1 & (7) \end{cases}$$

By (2), $p \mid b$ or $p \mid b'$. We have the following chain of deduction

$$p \mid b' \xRightarrow{(1)} p \nmid d' \xRightarrow{(3)} p \mid d \xRightarrow{(7)} p \nmid c \xRightarrow{(4)} p \mid d'$$

Contradiction

$$p \mid d' \xRightarrow{(1)} p \nmid b' \xRightarrow{(2)} p \mid b \xRightarrow{(6)} p \nmid a \xRightarrow{(5)} p \mid b'$$

Contradiction

Therefore $p \nmid b'$ and $p \nmid d'$. We have

$$p \nmid b' \xRightarrow{(2)} p \mid b \xRightarrow{(6)} p \nmid a \xRightarrow{(5)} p \mid b'$$

This is also a contradiction. Therefore, the case $r \neq 0$ cannot happen.

- $r = 0$:

Then $f_1(X) = q(X) q_1(X)$. We continue to write $\text{cont}(q) = \frac{a}{b}$ with $a, b \in \mathbb{N}$, $(a,b) = 1$

and $q(X) = \frac{a}{b} \bar{q}(X)$ where $\bar{q}(X)$ is a primitive polynomial in $\mathbb{Z}[X]$. Then

$$f(X) = \frac{a}{b} g(X) \bar{q}(X) \quad , \text{ or } \quad b f(X) = a g(X) \bar{q}(X).$$

- If $p \nmid b$ then there exist $u, v \in \mathbb{Z}$ such that $bu + pv = 1$. We have

$$f(X) = (bu + pv) f(X) = u\underbrace{(b f(X))}_{\in (g)} + \underbrace{pv f(X)}_{\in (p)} \in (p, g(X)).$$

This is a contradiction.

- If $p \mid b$ then $p \mid \left(a g(X) \bar{q}(X)\right)$. Then $p \mid a$ or $p \mid g(X)$ or $p \mid \bar{q}(X)$. But
  - $p \nmid a$ because $(a,b) = 1$,
  - $p \nmid g(X)$ because $g \in I \setminus (p)$,
  - $p \nmid \bar{q}(X)$ because $\bar{q}(X)$ is a primitive polynomial in $\mathbb{Z}[X]$.

In conclusion, there is no such an $f(X)$. We must have $I = (p, g(X))$.

Step 3

1) Let $I = (p, g(X))$ is an ideal of $\mathbb{Z}[X]$, we then write

$$g(X) = a_n X^n + \cdots + a_1 X + a_0$$

For each $i = 0, 1, \ldots, n$, there exists $\bar{a}_i \in \{0, 1, \ldots, p-1\}$ such that $p \mid (a_i - \bar{a}_i)$.

We put $\bar{g}(X) = \bar{a}_n X^n + \cdots + \bar{a}_1 X + \bar{a}_0$. Then $g(X) - \bar{g}(X) = \sum_{i=0}^{n} (a_i - \bar{a}_i) X^i \in (p)$.

Thus $\bar{g}(X) \in I = (p, g(X))$. Therefore, we could assume from the beginning that $g(X)$ has coefficients in $\{0, 1, \ldots, p-1\}$.

2) Let $g(X) \in \mathbb{Z}[X]$ with coefficients in $\{0, 1, \ldots, p-1\}$ such that $I = (p, g(X))$ is a prime ideal of $\mathbb{Z}[X]$ and m_g is smallest possible in $I \setminus (p)$. We'll show that g, if viewed as an element in $(\mathbb{Z}/p\mathbb{Z})[X]$, is a prime. Suppose by contradiction that this is not true.

Then g is not ~~irreducible~~ prime in $(\mathbb{Z}/p\mathbb{Z})[X]$. Because $\mathbb{Z}/p\mathbb{Z}$ is a field, $(\mathbb{Z}/p\mathbb{Z})[X]$ is factorial. Then a prime in $(\mathbb{Z}/p\mathbb{Z})[X]$ is of the same meaning as an irreducible element in it. Then g is not irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$.

Then there exist $\bar{u}(X), \bar{v}(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ which are not units such that $\bar{g}(X) = \bar{u}(X)\bar{v}(X)$. Since every nonzero element in $\mathbb{Z}/p\mathbb{Z}$ is invertible, $\bar{u}(X), \bar{v}(X) \notin \mathbb{Z}/p\mathbb{Z}$. Thus $1 \le \deg \bar{u}$, $\deg \bar{v} \le \deg \bar{g} = \deg g$. Fix $u(X), v(X) \in \mathbb{Z}[X]$ such that $u(X) = \bar{u}(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$ and $v(X) = \bar{v}(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. We have $g(X) - u(X)v(X) \in p\mathbb{Z}[X]$, and

$$1 \le \deg u = \deg \bar{u} < \deg g$$
$$1 \le \deg v = \deg \bar{v} < \deg g$$

We have $u(X)v(X) \in g(X) + p\mathbb{Z}[X] \subset I$. Since I is a prime ideal,

either $u(X) \in I$ or $v(X) \in I$. Since $g(X)$ is such that m_g is smallest in $I \setminus (p)$, $u(X) \in (p)$ or $v(X) \in (p)$. Then $g(X) \in u(X)u(X) + p\mathbb{Z}[X] \subset (p)$. This is a contradiction.

3) Let $g(X) \in \mathbb{Z}[X]$ with coefficients in $\{0, 1, \dots, p-1\}$ and is a prime in $(\mathbb{Z}/p\mathbb{Z})[X]$. We will show that $I = (p, g(X))$ is a prime ideal in $\mathbb{Z}[X]$. To avoid confusion, we will denote $\bar{g}(X) = \sum_{i=0}^{n} \bar{a}_i X^i$ where $g(X) = \sum_{i=0}^{n} a_i X^i$ and $\bar{a}_i$ is the residue class of a_i in modulo p. We have $\bar{g}$ is a prime in $(\mathbb{Z}/p\mathbb{Z})[X]$. To show that $I = (p, g(X))$ is a prime ideal of $\mathbb{Z}[X]$, there are two steps to do:

- Show that if $f, h \in \mathbb{Z}[X]$ such that $fh \in I$ then $f \in I$ or $h \in I$.
- Show that $1 \notin I$, i.e. I is a proper ideal of $\mathbb{Z}[X]$.

The first step

Let $f, h \in \mathbb{Z}[X]$ such that $fh \in I$. Then there exist $u(X), v(X) \in \mathbb{Z}[X]$ such that $f(X)h(X) = g(X)u(X) + pv(X)$. Taking the reduction map from $\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$, we get an equation in $(\mathbb{Z}/p\mathbb{Z})[X]$.

$$\bar{f}(X)\bar{h}(X) = \bar{g}(X)\bar{u}(X).$$

Since $\bar{g}(X)$ is a prime in $(\mathbb{Z}/p\mathbb{Z})[X]$, we must have either $\bar{g}(X) \mid \bar{f}(X)$

or $\bar{g}(X) \mid \bar{h}(X)$. Assume without lost of generality that $\bar{g}(X) \mid \bar{f}(X)$.

Then we can write $\bar{f}(X) = \bar{g}(X)\,\bar{q}(X)$. Choose a representative $q(X) \in \mathbb{Z}[X]$ of $\bar{q}(X)$, we have $f(X) - g(X)\,q(X) \in p\mathbb{Z}[X]$. Thus $f(X) = g(X)q(X) + p\mathbb{Z}[X]$. therefore $f(X) \in (p, g(X)) = \underline{I}$.

The second step

Suppose by contradiction that $1 \in I$. Then there exist $u(X), v(X) \in \mathbb{Z}[X]$ such that $1 = g(X)\,u(X) + p\,v(X)$.

For each polynomial $f(X) = a_n X^n + \cdots + a_1 X + a_0$, we denote $X^n f\left(\frac{1}{X}\right)$ to be the polynomial with coefficients as in $f(X)$ but with a reverse order, i.e.

$$X^n f\left(\frac{1}{X}\right) := a_0 X^n + a_1 X^{n-1} + \cdots + a_n$$

Put $m = \deg g$ and $n = \deg v$. Then $n \geq m > 1$ and $u(X)$ is of degree $n-m$. We write $v(X) = a_n X^n + \cdots + a_1 X + a_0$. Then

$$\begin{aligned} g(X)u(X) = 1 - pv(X) &= 1 - p(a_n X^n + \cdots + a_1 X + a_0) \\ &= -p a_n X^n - \cdots - p a_1 X + (1 - p a_0). \end{aligned} \tag{1}$$

We can almost use Eisenstein's criterion, provided that the coefficients $-p a_n, \ldots, -p a_1, 1 - p a_0$ should be written in a reversed order, Replacing X by $\frac{1}{X}$ and then multiplying both sides of (1) by X^n, we get

$$X^n g\left(\frac{1}{X}\right) u\left(\frac{1}{X}\right) = (1-pa_0)X^n - pa_1 X^{n-1} - \cdots - pa_{n-1}X - pa_n. \quad (2)$$

What prevents us from using the Eisenstein's criterion is that p may divide a_n. Assume for the moment that $p \nmid a_n$. We write

$$g(X) = b_m X^m + \cdots + b_1 X + b_0 \quad \text{where } b_i \in \{0, 1, \ldots, p-1\},\ b_m \neq 0,$$

$$u(X) = c_{n-m} X^{n-m} + \cdots + c_1 X + c_0,$$

Then (2) gives us

$$(1-pa_0)X^n - pa_1 X^{n-1} - \cdots - pa_n = \left(X^m g\left(\frac{1}{X}\right)\right)\left(X^{n-m} u\left(\frac{1}{X}\right)\right)$$

$$= (b_0 X^m + b_1 X^{m-1} + \cdots + b_m)(c_0 X^{n-m} + c_1 X^{n-m-1} + \cdots + c_{n-m})$$

By Eisenstein's criterion, the left hand member is irreducible in $\mathbb{Q}[X]$. Thus either $b_0 X^m + b_1 X^{m-1} + \cdots + b_m$ or $c_0 X^{n-m} + c_1 X^{n-m-1} + \cdots + c_{n-m}$ must be a nonzero rational number. Thus, either $g(X) = b_m X^m$ or $u(X) = c_{n-m} X^{n-m}$. If $m \neq n$ then we'll always have $g(0)u(0) = 0$. Then the equation

$$1 = g(X)u(X) + pv(X) \quad (3)$$

evaluated at $X = 0$ gives $1 = pv(0)$. This is a contradiction. Therefore $m = n$ and $u(X)$ is just a number in $\mathbb{Z}$. We write $u(X) = a \in \mathbb{Z}$. Then (3) becomes

$$1 = a\,g(X) + pv(X). \quad (4)$$

Comparing the leading coefficients gives us $0 = ab_n + pa_n$. Thus $p \mid (ab_n)$

Since $b_m \in \{1, \dots, p-1\}$, $p \mid a$. Then the right-hand member of (4) divides p while the left doesn't. This is a contradiction.

Therefore, the entire proof would complete if we could have a representation $1 = g(X)u(X) + pv(X)$ in which the leading coefficient of $v(X)$ is not divisible by p. Nevertheless, we have proved above that $u(X)$ cannot be a constant polynomial.

We see that $1 = g(X)(c_{n-m}X^{n-m} + \dots + c_1 X + c_0) + p\,v(X)$.

Equating the leading coefficient gives us $0 = c_{n-m}b_m + pa_n$. Thus $p \mid (c_{n-m}b_m)$. Since $b_m \in \{1, \dots, p-1\}$, $p \mid c_{n-m}$. Equating the constant term gives us $1 = b_0 c_0 + pa_0$. Thus $p \nmid c_0$. Thus there exists $k \in \{0, 1, \dots, n-m-1\}$ such that $p \nmid c_k$ and $p \mid c_i$ for all $i > k$. Then we can write $u(X) = p\,u_1(X) + u_2(X)$ where the leading coefficient of $u_2(X)$ is not divisible by p. Then

$$\begin{aligned} 1 &= g(X)\left(p\,u_1(X) + u_2(X)\right) + p\,v(X) \\ &= g(X)\,u_2(X) + p\underbrace{\left(g(X)\,u_1(X) + v(X)\right)}_{w(X)} \end{aligned}$$

Here we encounter again a representation $1 = g(X)u_2(X) + p\,w(X)$, where $u_2(X)$ and $w(X)$ play the roles of $u(X)$ and $v(X)$ respectively. Then the leading coefficient of $u_2(X)$ must be divisible by p. This is a contradiction.