Bob Kuo
Adrian Neff
Ezzedine El Sai

Problem 7.

(a) Suppose that R is a UFD. Show that a prime ideal in R is generated as an ideal by irreducible elements it contains.

(b) Now suppose that $R = S[x]$ where S is a PID. Show that any prime ideal of R is generated by at most 2 irreducible elements. Show that if a prime requires two irreducible generators, then it has the form $I = (p, f(x))$ where p is prime in S and $f(x)$ is monic and irreducible mod p.

(c) Sketch the ordered set of primes of $S[x]$ under inclusion to the best of your ability. How long can a chain be?

Theorem 1. *If R is a UFD, then prime ideals of R are generated by the irreducible elements it contains.*

Proof. Let $\mathfrak{p} \subseteq R$ be a prime ideal and define $P = \{p \in \mathfrak{p} : p \text{ is irreducible}\}$. Clearly, $(P) \subseteq \mathfrak{p}$ since $P \subseteq \mathfrak{p}$ by definition. Now, let $a \in \mathfrak{p}$ then we want to show $a \in (P)$. By unique factorization $a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$. Where $u \in R^\times$ and each p_i is irreducible.

If $k = 2$, then by primality either $up_1^{\alpha_1}$ or $p_2^{\alpha_2}$ are in $\mathfrak{p}$. Since a prime cannot contain units, then $up_1^{\alpha_1} \in \mathfrak{p}$ implies $p_1^{\alpha_1} \in \mathfrak{p}$. Primes are radical, so it follows that either p_1 or p_2 is in $\mathfrak{p}$ and thus they are also in $\mathfrak{p}$. By induction, suppose that if $k = n$ then one of p_i for $i = 1, 2, \ldots, n$ is in $\mathfrak{p}$. Then if $k = n+1$, we can write $a = (up_1^{\alpha_1}\cdots p_n^{\alpha_n}) \cdot (p_{n+1}^{\alpha_{n+1}})$. Thus, either $up_1^{\alpha_1}\cdots p_n^{\alpha_n}$ or $p_{n+1}^{\alpha_{n+1}}$ is in $\mathfrak{p}$. That is, either $p_{n+1} \in \mathfrak{p}$, or by the induction hypothesis, some $p_i \in \mathfrak{p}$ for $i = 1, 2, \ldots, n$. It follows that for any k, at least one $p_i \in \mathfrak{p}$ and so by definition $p_i \in P$. Since a is a multiple of p_i, then $a \in (P)$. $\square$

If in addition, R is a polynomial ring over a PID then we can describe the prime ideals of R much more explicitly. First we will need a few lemmas.

Lemma 2. *Let $\mathfrak{p}$ be a nonzero prime ideal of $S[x]$ where S is a UFD. If $\mathfrak{p}$ does not contain nonzero constants, then it contains an irreducible polynomial f of minimal degree.*

Proof. The degrees of polynomials in $\mathfrak{p}$ forms a subset of $\mathbb{N}$, so by well ordering there exists a polynomial $f' \in \mathfrak{p}$ with minimal degree. Since S is a UFD then $S[x]$ is also a UFD. By unique factorization $f' = sf$ where $s \in S \setminus \{0\}$ and no primes of S divides f. If s is a unit, then $f' \in \mathfrak{p}$ implies $f \in \mathfrak{p}$. If not, then either $s \in \mathfrak{p}$ or $f \in \mathfrak{p}$. However, $s \in \mathfrak{p}$ contradicts that $\mathfrak{p}$ has no nonzero constants, so it follows that $f \in \mathfrak{p}$. Observe that f is irreducible. Suppose not, then since no primes of S divides f, then there must be non-constant polynomials $g, h \in R$ such that $f = gh$. The degrees of g and h must be less than the degree of f. However, by primality either $g \in \mathfrak{p}$ or $h \in \mathfrak{p}$ which contradicts the minimality of the degree of f. $\square$

Lemma 3. *Let $\mathfrak{p}$ be a prime ideal in a ring R and $\phi : R \to S$ be a surjective ring homomorphism such that $\ker\phi \subseteq \mathfrak{p}$. Then $\phi(\mathfrak{p})$ is prime in S.*

Proof. Suppose $ab \in \phi(\mathfrak{p})$. Let $x, y, z \in R$ such that $\phi(x) = a$, $\phi(y) = b$, and $\phi(z) = ab$. Since $ab \in \phi(\mathfrak{p})$, we can choose z such that $z \in \mathfrak{p}$. Next, observe that $\phi(xy - z) = \phi(x)\phi(y) - \phi(z) = ab - ab = 0$. It follows that $xy - z \in \mathfrak{p}$ because it is in $\ker\phi$. Thus, $z \in \mathfrak{p}$ implies that $xy \in \mathfrak{p}$. By primality, then either x or y is in $\mathfrak{p}$. It follows that either a or b is in $\phi(\mathfrak{p})$. $\square$

Bob Kuo
Adrian Neff
Ezzedine El Sai

Theorem 4. *Let $R = S[x]$ where S is a PID, then if $\mathfrak{p}$ is a prime ideal in R, one of the following is true:*

(i) $\mathfrak{p} = (0)$.

(ii) $\mathfrak{p}$ *is generated by a single irreducible element.*

(iii) $\mathfrak{p} = (p, f(x))$ *where p is prime in S and $f(x)$ is monic in S and irreducible mod p.*

Proof. Since S is an integral domain because it is a PID, then $S[x]$ is also an integral domain. A ring is a domain if and only if (0) is prime, so it follows that (0) is prime in R. We now consider when $\mathfrak{p} \neq (0)$.

First, let $\iota : S \hookrightarrow S[x]$ be the inclusion map, then ι is a ring homomorphism. Thus, $\iota^{-1}(\mathfrak{p}) = \mathfrak{p} \cap S[x]$ is a prime ideal in S. Since S is a PID, then $\iota^{-1}(\mathfrak{p}) = (0)$ or (p) where p is a prime in S.

In the case that $\iota^{-1}(\mathfrak{p}) = (0)$, $\mathfrak{p}$ consists entirely of non-constant polynomials. By Lemma 2 there exists an irreducible polynomial f with minimal degree in $\mathfrak{p}$. Now let g be any non-zero polynomial in $\mathfrak{p}$. Let $K(S)$ be the fraction field of S. Viewing f and g as elements of $K(S)[x]$, define I to be the ideal generated by f and g in $K(S)[x]$. Notice that $K(S)[x]$ is a PID because $K(S)$ is a field, so $I = (h(x))$. It follows that $h(x) \mid f(x)$, but f must also be irreducible in $K(S)[x]$ by Gauss's Lemma. Furthermore, $I \neq (1)$ because otherwise, there exists $a(x), b(x) \in K(S)[x] \setminus \{0\}$ such that $a(x)f(x) + b(x)g(x) = 1$. Then there exists $q_1, q_2 \in S \setminus \{0\}$ such that $q_1 a(x) \in S[x]$ and $q_2 g(x) \in S[x]$. Denote $a'(x) = q_1 a(x)$ and $b'(x) = q_2 b(x)$ then

$$q_2 a'(x) f(x) + q_1 b'(x) g(x) = q_1 q_2.$$

That is $q_1 q_2 \in \mathfrak{p}$, so $q_1 \in \mathfrak{p}$ or $q_2 \in \mathfrak{p}$. This contradicts the assumption that $\mathfrak{p}$ contains no contants. It follows that $h(x)$ is non-constant and divides $f(x)$, so it must be associate to $f(x)$. Thus, $I = (f(x))$ in $K(S)[x]$ so $f(x) \mid g(x)$ in $K(S)[x]$. That is, $g(x) = r(x)f(x)$ for some $r(x) \in K(S)[x]$. Gauss's lemma asserts that if $f(x)$ divides $g(x)$ in $K(S)[x]$ then $f(x)$ divides $g(x)$ in $S[x]$. This shows that $\mathfrak{p}$ is generated by a single irreducible element.

On the other hand, suppose that $\iota^{-1}(\mathfrak{p}) = (p)$ for some prime $p \in S$. Observe that (p) is maximal because nonzero prime ideals are maximal in a PID. It follows that $S/(p)$ is a field. Denote $F = S/(p)$ and let $\pi : S \to S/(p)$ be the natural projection. This induces the ring homomorphism $\tilde{\pi} : S[x] \to F[x]$ defined by

$$\tilde{\pi}(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = \pi(a_n) x^n + \pi(a_{n-1}) x^{n-1} + \cdots + \pi(a_1) x + \pi(a_0).$$

The kernel of $\tilde{\pi}$ is (p), which is contained in $\mathfrak{p}$. Thus by Lemma 3, $\tilde{\pi}(\mathfrak{p})$ is prime. Since F is a field, then $F[x]$ is a PID, so $\tilde{\pi}(\mathfrak{p})$ is either (0) or $(\overline{f}(x))$ where $\overline{f}(x)$ is monic and irreducible in $F[x]$. If $\tilde{\pi}(\mathfrak{p}) = 0$, then $\mathfrak{p}$ consists of polynomials whose coefficients are multiples of (p), but that is just (p).

On the other hand, suppose $\tilde{\pi}(\mathfrak{p}) = (\overline{f})$. We may pick $f(x) \in S[x]$ that is monic such that $\tilde{\pi}(f(x)) = \overline{f}(x)$. That is, the coefficients of $\overline{f}(x)$ take the form $a_i + \mathfrak{p}$ where $a_n = 1$. Then the polynomial with coefficients of a_i satisfies this description. If there exists a non-trivial factorization $f(x) = a(x)b(x)$ then because $f(x)$ is monic $a(x)$ and $b(x)$ must both be non-constant polynomials. This induced the nontrivial factorization $\overline{f(x)} = \tilde{\pi}(a(x))\tilde{\pi}(b(x))$, which contradicts the irreducibility of $\overline{f}(x)$. Thus, $f(x)$ must be irreducible.

Bob Kuo
Adrian Neff
Ezzedine El Sai

Since $\tilde{\pi}$ is surjective, then

$$\tilde{\pi}^{-1}((\overline{f})) = \tilde{\pi}^{-1}(\tilde{\pi}(\mathfrak{p})) = \mathfrak{p} + \ker \tilde{\pi} = \mathfrak{p} + (p).$$

Now, $(p) \subseteq \mathfrak{p}$ so $\mathfrak{p} = \mathfrak{p} + (p)$. Notice that $f \in \tilde{\pi}^{-1}((\overline{f}(x)))$ and $\mathfrak{p}$ contains (p). Thus, $(p, f(x)) \subseteq \mathfrak{p}$. We now show that in fact $(p, f(x)) = \mathfrak{p}$. Let $g \in \mathfrak{p}$, then $\overline{g}(x) = \overline{f}(x) \cdot \overline{q}(x)$. Let $q(x)$ be a polynomial that reduces to $\overline{q}(x)$ then $\tilde{\pi}(f(x)q(x)) = \tilde{\pi}(g(x))$. That is, $f(x)q(x) - g(x) \in (p, f(x))$. However, $f(x)q(x) \in (p, f(x))$ so $g(x)$ must also be in $(p, f(x))$. It follows that we also have $\mathfrak{p} \subseteq (p, f(x))$, so $\mathfrak{p} = (p, f(x))$. □

Corollary 5. *A complete description of the ordering of primes in $S[x]$ is given by*

(i) $(0) \preceq$ *any prime.*

(ii) $(p) \preceq (q)$ *if and only if* $(p) = (q)$ *and* $(f(x)) \preceq (g(x))$ *if and only if* $(f(x)) = (g(x))$.

(iii) $(p) \preceq (q, f(x))$ *if and only if* $(p) = (q)$.

(iv) $(f(x)) \preceq (p, g(x))$ *if and only if* $g(x) \mid f(x)$ *mod* p.

(v) $(p, f(x)) \preceq (q, g(x))$ *if and only if* $(p, f(x)) = (q, g(x))$ *(i.e.* $(p) = (q)$ *and* $f(x) \equiv g(x)$ mod p*).*

Furthermore, a chain can have length at most 2.

Proof. (i) and (ii) hold in any integral domain. (iii) follows from the fact that p and q both generate the principal ideal $\iota^{-1}((p, f(x)))$, so p and q are associates. (iv) Observe that $f(x) \in (p, g(x))$ if and only if $f(x) = h_1(x)p + h_2(x)g(x)$, but this is equivalent to the condition that $g(x) \mid f(x) \bmod p$. For (v), first observe that $(p) = (q)$ because otherwise, the $(p, q) = 1$ but $(p, q) \subseteq (q, g(x))$. Now, by the isomorphism theorems, the lattice of ideals in $S/(p)$ is isomorphic to the lattice of ideals containing (p). However, $(p, f(x))$ and $(q, g(x))$ are both inverse images of maximal ideals under $\tilde{\pi}$. Then they are both maximal among ideals containing (p). Thus, containment implies equality. □