Unique Factorization

E. L. Lady

Division Algorithm [Lang, Theorem 4.1, p. 190]**.** Let $f \in R[X]$ and let $0 \neq g$ be a *monic* polynomial in $R[X]$. Then there exists a unique polynomial $r \in R[X]$ with degree strictly less than the degree of g such that $f \equiv r \pmod{(g)}$.

Proposition [Hungerford, pp. 158–159]. (1) If R is a commutative ring and $r \in R$, then the principal ideal $(X - r)$ in $R[X]$ is the kernel of the evaluation map $\varphi_r \colon f \mapsto f(r)$ from $R[X]$ into R.

(2) [REMAINDER THEOREM] For any $f \in R[X]$, $f \equiv f(r) \pmod{(X - r)}$.

(3) If R is an integral domain, then the ideal $(X - r)$ is prime.

PROOF: : One can see that (1) $\Rightarrow$ (3). Now by the Division Algorithm, $f \equiv c \pmod{(X - r)}$ for some constant c. Since clearly $(X - r) \subseteq \operatorname{Ker} \varphi_r$, thus $f \equiv c \pmod{\operatorname{Ker} \varphi_r}$ and so $\varphi_r(f) = \varphi_r(c) = c$. But $\varphi_r(f) = f(r)$. Thus $f \equiv f(r) \pmod{(X - r)}$ so that (2) is true.

Furthermore, if $f \in \operatorname{Ker} \varphi$ then by the above

$$f \equiv f(r) = \varphi_r(f) = 0 \pmod{(X - r)}$$

so that $f \in (X - r)$. Thus $\operatorname{Ker} \varphi \subseteq (X - r)$ and since clearly $(X - r) \subseteq \operatorname{Ker} \varphi$, it follows that (1) is true. $\boxed{\checkmark}$

DEFINITION. The **height** of a prime ideal $\mathfrak{p}$ is the supremum of the lengths of all chains of prime ideals strictly contained in $\mathfrak{p}$. In particular, $\mathfrak{p}$ has height one if $\mathfrak{p}$ is not a minimal prime ideal but any prime ideal strictly contained in $\mathfrak{p}$ is minimal. If R is an integral domain, then the height one prime ideals are those prime ideals which are minimal in the set of non-trivial primes. (This is because in this case the zero ideal is prime.)

Lemma. If R is noetherian and $\mathfrak{p}$ is a prime ideal with height 0, then $(\exists r \in R)\ \mathfrak{p} = \operatorname{ann}(r)$. In particular, $\mathfrak{p}$ is made up of zero divisors.

PROOF: Clearly $\mathfrak{p}$ is minimal in $\operatorname{Supp} R$ and therefore $\mathfrak{p} \in \operatorname{Ass} R$, i. e. $\mathfrak{p} = \operatorname{ann} r$ for some r. Note that $r \neq 0$ since $\operatorname{ann} 0 = R$. Since $\mathfrak{p} r = 0$, this shows that $\mathfrak{p}$ consists of zero divisors. $\boxed{\checkmark}$

Principal Ideal Theorem. Let R be noetherian and let $r \in R$ not be a zero divisor. Then there exist prime ideals $\mathfrak{p}$ minimal among the set of primes containing r, and any such prime ideal has height one.

PROOF: Since $\operatorname{Ass} R/(r)$ is finite there exists a prime $\mathfrak{p}$ which is minimal in $\operatorname{Ass} R/(r)$. Then $\mathfrak{p}$ is also minimal in $\operatorname{Supp} R/(r)$. But $\operatorname{Supp} R/(r)$ is the set of primes which contain r. By the preceding Lemma, since they contain the non-zero divisor r they have height at least one. Let $\mathfrak{p}$ be such a prime and let $\mathfrak{q}$ be a prime ideal properly contained in $\mathfrak{p}$. We will show that $\mathfrak{q}$ is a minimal prime ideal, thus showing that $\mathfrak{p}$ has height 1. It suffices to show that $\mathfrak{q}R_{\mathfrak{p}}$ is minimal in $R_{\mathfrak{p}}$. Therefore there is no loss of generality in assuming that R is local and $\mathfrak{p}$ is its unique maximal ideal. Now with this assumption, let $\theta\colon R \to R_{\mathfrak{q}}$ [sic] be the canonical map and for $n \geq 1$ define

$$\mathfrak{q}_n = \theta^{-1}(\mathfrak{q}^n R_{\mathfrak{q}}).$$

Then the map $R/\mathfrak{q}_n \to R_{\mathfrak{q}}/\mathfrak{q}^n R_{\mathfrak{q}}$ induced by θ is monic, so $\operatorname{Ass} R/\mathfrak{q}_n \subseteq \operatorname{Ass} R_{\mathfrak{q}}/\mathfrak{q}^n R_{\mathfrak{q}} \subseteq \operatorname{Supp} R_{\mathfrak{q}}/\mathfrak{q}^n R_{\mathfrak{q}} = \{\mathfrak{q}\}$. Thus in particular, since $r \notin \mathfrak{q}$ (because $\mathfrak{q} \subsetneq \mathfrak{p}$ and $\mathfrak{p}$ is minimal among the primes containing r), it follows that r is not a zero divisor on $R/\mathfrak{q}_n$. Let $\bar{\mathfrak{q}}_n$ be the image of $\mathfrak{q}_n$ in $R/(r)$, i.e.

$$\bar{\mathfrak{q}}_n = (\mathfrak{q}_n + (r))/(r).$$

Since $\mathfrak{p}$ is the only prime ideal containing (r) and by assumption $\mathfrak{p}$ is maximal, we see that $\operatorname{Supp} R/(r) = \operatorname{Ass} R/(r) = \{\mathfrak{p}\}$. Therefore $R/(r)$ is artinian. Since the ideals $\bar{\mathfrak{q}}_n$ form a descending chain, $(\exists n)\, \bar{\mathfrak{q}}_{n+1} = \bar{\mathfrak{q}}_n$. I.e. $\mathfrak{q}_{n+1} + (r) = \mathfrak{q}_n + (r)$, and in particular $\mathfrak{q}_n \subseteq \mathfrak{q}_{n+1} + (r)$. Thus

$$x \in \mathfrak{q}_n \Rightarrow (\exists z \in R)(\exists y \in \mathfrak{q}_{n+1})\ x = y + zr.$$

Then $zr = x - y \in \mathfrak{q}_n$. But as noted above, r is not a zero divisor on $R/\mathfrak{q}_n$, so therefore $z \in \mathfrak{q}_n$. Hence

$$\mathfrak{q}_n \subseteq \mathfrak{q}_{n+1} + r\mathfrak{q}_n \subseteq \mathfrak{q}_{n+1} + \mathfrak{p}\mathfrak{q}_n = \mathfrak{q}_{n+1} + J(R)\mathfrak{q}_n.$$

Therefore by Nakayama's Lemma, $\mathfrak{q}_n = \mathfrak{q}_{n+1}$. But $\mathfrak{q}_n R_{\mathfrak{q}} = \mathfrak{q}^n R_{\mathfrak{q}}$, and so we get $\mathfrak{q}^n R_{\mathfrak{q}} = \mathfrak{q}^{n+1} R_{\mathfrak{q}}$, and from Nakayama's Lemma it then follows that $\mathfrak{q}^n R_{\mathfrak{q}} = 0$. This implies that $\mathfrak{q}R_{\mathfrak{q}}$ is a minimal prime ideal in $R_{\mathfrak{q}}$ (WHY?). Since there is a one-to-one correspondence between the prime ideals of $R_{\mathfrak{q}}$ and the primes of R contained in $\mathfrak{q}$, it then follows that $\mathfrak{q}$ is a minimal prime ideal in R and so $\mathfrak{p}$ has height one. $\boxed{\checkmark}$

DEFINITIONS: 1) Let r, $s \in R$. We say that r and s are **equivalent** or **associates** if $s = ur$ for some invertible element u. Note that this is equivalent to saying that $(r) = (s)$.

2) We say that r **divides** s and write $r|s$ if $(\exists t)\, s = rt$. This is equivalent to stating that $(s) \subseteq (r)$.

3) We say that r is **irreducible** if r is not invertible and not 0 and $r = st$ implies that either s or t is invertible.

4) We say that r is **prime** if the principal ideal (r) is prime. One easily sees that prime elements are irreducible.

Easy Lemma. An element $r \in R$ is irreducible if and only if (r) is maximal among the set of proper principal ideals.

Theorem. Let R be an integral domain (not necessarily noetherian). The following conditions are equivalent:

(1) R is factorial (Hungerford, Def. 3.5, p. 137).
(2) Every element in R is a product of irreducible elements and the principal ideals generated by irreducible elements are prime.
(3) R satisfies the ascending chain condition on principal ideals and the principal ideals generated by irreducible elements are prime.

Furthermore, these conditions imply

(4) All height-one prime ideals are principal.

Conversely, if R is noetherian then (4) implies (1).

PROOF: (1) $\Rightarrow$ (2): Let $p \in R$. To say that (p) is prime means that $rs \in (p) \Rightarrow r \in (p)$ or $s \in (p)$, or, equivalently, $p|rs \Rightarrow p|r$ or $p|s$. Thus clearly if R is factorial and p is irreducible then (p) is prime.

(2) $\Rightarrow$ (1): If $p_1 \dots p_r = q_1 \dots q_s$ where all the ideals (p_i) and (q_j) are prime, then $q_1 \dots q_r \in (p_1)$ so $(\exists j)\, q_j \in (p_1)$, i.e. $(q_j) \subseteq (p_1)$. But since q_j is prime (q_j) is maximal among proper principal ideals, so $(q_j) = (p_1)$ and we may as well suppose $q_j = p_1$. It then follows by induction that the two factorizations are the same.

(1) & (2)$\Rightarrow$(3): To say that $(r) \subseteq (s)$ is to say that s is a factor of r. If R is factorial, then any non-trivial element has only finitely many factors (up to multiplication by units). Thus clearly principal ideals must satisfy the a.c.c.

(3) $\Rightarrow$ (2): Suppose BWOC that there exist elements in R which are not products of irreducible elements. Since R has a.c.c. on principal ideals, we see that there exists a principal ideal (r) which is maximal among those principal ideals whose generators are not products of irreducible elements. Then (r) is not irreducible, so $r = st$ where $(r) \subsetneq (s)$, $(r) \subsetneq (t)$. Thus by the maximality of (r), s and t are products of irreducible elements and we derive a CONTRADICTION.

(2) $\Rightarrow$ (4): Let $\mathfrak{p}$ be a non-trivial height-one prime and let $0 \neq p \in \mathfrak{p}$. By (2), p is a product of irreducible factors, $p = p_1 \cdots p_n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, at least one of

these factors, say p_1, belongs to $\mathfrak{p}$. Thus $0 \neq (p_1) \subseteq \mathfrak{p}$. By assumption, (p_1) is prime and $\mathfrak{p}$ has height one. Thus $\mathfrak{p} = (p_1)$, so $\mathfrak{p}$ is principal.

(4) $\Rightarrow$ (3): By assumption, R is noetherian and hence satisfies the a.c.c. on principal ideals. Now let $r \in R$ be irreducible. By the Principal Ideal Theorem there exists a height-one prime $\mathfrak{p}$ with $(r) \subseteq \mathfrak{p}$. By hypothesis, $\mathfrak{p}$ is principal. But since r is irreducible, (r) is maximal in the set of proper principal ideals. Thus $(r) = \mathfrak{p}$, so (r) is prime. $\boxed{\checkmark}$

Lemma. If R is a commutative ring such that all prime ideals are principal, then R is a principal ideal ring.

PROOF: Since all prime ideals are finitely generated, R is noetherian. Thus if there exist ideals which are not principal then there exists an ideal $\mathfrak{a}$ which is maximal with this property. By hypothesis, $\mathfrak{a}$ cannot be prime. Thus there exist r, $s \notin \mathfrak{a}$ with $rs \in \mathfrak{a}$. Then $\mathfrak{a} + (r) \supsetneq \mathfrak{a}$, so $\mathfrak{a} + (r)$ must be principal, say $\mathfrak{a} + (r) = (r')$. Now let

$$\mathfrak{b} = \{x \in R \mid xr' \in \mathfrak{a}\}.$$

Obviously $\mathfrak{a} \subseteq \mathfrak{b}$. Now $sr' \in s\mathfrak{a} + (rs) \subseteq \mathfrak{a}$, so $s \in \mathfrak{b}$. Thus $\mathfrak{b} \supsetneq \mathfrak{a}$ so $\mathfrak{b}$ must be principal, say $\mathfrak{b} = (b)$. Now by definition of $\mathfrak{b}$, $r'\mathfrak{b} \subseteq \mathfrak{a}$. On the other hand, if $a \in \mathfrak{a}$ then $a \in \mathfrak{a} + (r) = (r')$ so $a = xr'$ for some x, where clearly $x \in \mathfrak{b}$, so $a \in r'\mathfrak{b}$. Thus $\mathfrak{a} = r'\mathfrak{b} = r'(b) = (r'b)$. Thus $\mathfrak{a}$ is principal, a CONTRADICTION. This shows that there cannot exist ideals in R which are not principal, so R is a PID. $\boxed{\checkmark}$

Corollary. If R is an integral domain such that all non-trivial prime ideals are maximal, then R is factorial if and only if R is a principal ideal domain. In particular, in this case R is noetherian.

PROOF: ($\Leftarrow$): It is well know that PIDs are factorial.

($\Rightarrow$): Suppose that R is factorial. By the preceding Theorem, all height one primes are principal. But by assumption, all non-trivial primes have height one. Thus all prime ideals are principal, so by the above lemma R is a PID. $\boxed{\checkmark}$

Proposition/Definition. If R is a factorial domain and $r_1, \ldots, r_n \in R$, then there exists a unique principal ideal $\mathfrak{c}$ which is minimal with respect to the property $(\forall i)\, r_i \in \mathfrak{c}$. The ideal $\mathfrak{c}$ (or an element c which generates it) is called the **greatest common divisor** of the r_i.

Lemma/Definition. Let R be a factorial domain.

1) If $\mathfrak{c}$ is an ideal in R and $f \in R[X]$, then $f \in \mathfrak{c}R[X] \iff$ all the coefficients of f belong to $\mathfrak{c}$. Furthermore, $R[X]/\,\mathfrak{c}R[X] \approx (R/\mathfrak{c})\,[X]$.

2) For any non-trivial $f \in R[X]$, there exists a unique principal ideal $\mathfrak{c}$ of R which is minimal with respect to the property $f \in \mathfrak{c}R[X]$. The ideal $\mathfrak{c}$ (or element c generating $\mathfrak{c}$) is called the **content** of f and denoted $\operatorname{cont}(f)$.

Gauss's Lemma. (1) If R is an commutative ring and $\mathfrak{p}$ is a prime ideal in R, then $\mathfrak{p}R[X]$ is a prime ideal in $R[X]$.

(2) If R is a factorial domain and $f,\ g \in R[X]$, then $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$.

PROOF: (1) USUAL PROOF: We easily see that if $\mathfrak{p}$ is a prime ideal of R and if f and g both have leading coefficients not belonging to $\mathfrak{p}$, then $fg \notin \mathfrak{p}R[X]$. Now let $f,\ g$ be *any* polynomials with $f,\ g \notin \mathfrak{p}R[X]$. Let s and t be the largest exponents such that the coefficient of X^s in f and of X^t in g do not belong to $\mathfrak{p}$. Then we can write $f = X^{s+1}f_1 + f_2$ and $g = X^{t+1}g_1 + g_2$, where $f_2,\ g_2$ have degrees s and t and have leading coefficients not belonging to $\mathfrak{p}$ and $f_1,\ g_1 \in \mathfrak{p}R[X]$. It follows easily that $f_2g_2 \notin \mathfrak{p}$ and then $fg \equiv f_2g_2 \not\equiv 0 \pmod{\mathfrak{p}R[X]}$. Thus $\mathfrak{p}R[X]$ is prime. (NOTE: This is a stupid proof, but it's the one given in Lang (Theorem 6.1, p. 198) and Hungerford (Lemma 6.11, p. 162) and is fairly standard.)

More intelligently, we can notice that there is an obvious map $\psi\colon R[X] \to R/\mathfrak{p}\,[X]$ whose kernel is $\mathfrak{p}R[X]$. Thus to see that $\mathfrak{p}R[X]$ is prime it suffices to see that $R/\mathfrak{p}\,[X]$ is an integral domain. I. e. we need the lemma that if D is an integral domain then $D[X]$ is an integral domain. This is easy since if $f,\ g \neq 0 \in D[X]$ then it is clear that the leading coefficient of fg is non-zero.

(2) First, it is obvious that if $r \in R$, then $\operatorname{cont}(rf) = r\operatorname{cont}(f)$. Second, we note that in the case where $\operatorname{cont}(f) = \operatorname{cont}(g) = R$, then $f,\ g \notin pR[X]$ for every irreducible element $p \in R$. Since R is factorial, (p) is prime and by (1) $pR[X]$ is prime, so $fg \notin pR[X]$. Thus if $\mathfrak{c}$ is a principal ideal such that $fg \in \mathfrak{c}R[X]$ then $\mathfrak{c} = R$, so that in this case $\operatorname{cont}(fg) = R = \operatorname{cont}(f)\operatorname{cont}(g)$.

In general we can write $f = a\hat{f},\ g = b\hat{g}$, where $\operatorname{cont}(f) = (a)$, $\operatorname{cont}(g) = (b)$, and $\operatorname{cont}(\hat{f}) = \operatorname{cont}(\hat{g}) = R$. Then $\operatorname{cont}(fg) = ab\operatorname{cont}(\hat{f}\hat{g}) = (ab) = \operatorname{cont}(f)\operatorname{cont}(g)$. $\boxed{\checkmark}$

Proposition. Let R be a factorial domain and let K be the quotient field of R.

(1) Let $g,\ h \in K[X]$ be such that $gh \in R[X]$. Then there exists a non-trivial element $u \in K$ such that $ug,\ u^{-1}h \in R[X]$.

(RESTATED: If a polynomial in $R[X]$ "factors over K," then it "factors over R.")

(2) Let $f \in R[X]$ and $f = cf_1$, where $c = \operatorname{cont}(f)$. Then $(f_1) = R[X] \cap fK[X]$.

(3) If f is an irreducible polynomial in $R[X]$ then either f is an irreducible constant in R or $\operatorname{cont}(f) = R$ and f is also irreducible in $K[X]$.

PROOF: (1) We can choose a and $b \in R$ such that $ag \in R[X]$, $bh \in R[X]$. (In other words, a and b should be common denominators for the coefficients of f and g, respectively.) Now choose $u = a/\operatorname{cont}(ag)$. Then $ug = ag/\operatorname{cont}(ag) \in R[X]$ by the definition of content. And

$$u^{-1} = \frac{\operatorname{cont}(ag)}{a} = \frac{\operatorname{cont}(ag)\operatorname{cont}(bh)}{a\operatorname{cont}(bh)} = \frac{\operatorname{cont}(abgh)}{a\operatorname{cont}(bh)} = \frac{b\operatorname{cont}(gh)}{\operatorname{cont}(bh)},$$

so $u^{-1}h = \operatorname{cont}(gh)bh/\operatorname{cont}(bh) \in R[X]$.

(2) ($\subseteq$): Clear.

($\supseteq$): Note that if $f = cf_1$ where $\operatorname{cont}(f) = (c)$ then $fK[X] = f_1K[X]$ and $\operatorname{cont}(f_1) = R$. Now if $g \in R[X] \cap fK[X]$ then $(\exists h \in K[X])\, f_1h = g \in R[X]$. By 1) there exists $u \in K$ such that $uf_1 \in R[X]$, $u^{-1}h \in R[X]$. But $u = u\operatorname{cont}(f_1) = \operatorname{cont}(uf_1) \in R$ so that $h = uu^{-1}h \in R[X]$. Thus $g = f_1h \in (f_1)$, showing that $R[X] \cap fK[X] \subseteq (f_1)$.

(3): Straightforward from (1). However we can also (perhaps perversely) argue as follows: If f is not constant then $(f) \subsetneq \operatorname{cont}(f)$. If f is irreducible then (f) is a maximal proper principal ideal and so $\operatorname{cont}(f) = R$. Now suppose BWOC that f is irreducible in $R[X]$ and not constant and that f factors in $K[X]$. Then $fK[X] \subsetneq gK[X]$ for some non-constant $g \in K[X]$, where $0 < \deg(g) < \deg(f)$. We may assume WLOG that $g \in R[X]$. By (2),

$$(f) = R[X] \cap fK[X] \subsetneq R[X] \cap gK[X] \subsetneq R[X]$$

where the first inclusion is proper because of the degrees, and for the same reason $R[X] \cap gK[X] \neq R[X]$. But by (1), $R[X] \cap gK[X]$ is a principal ideal generated by $g/\operatorname{cont}(g)$. Thus (f) is not a maximal proper principal ideal, a CONTRADICTION. ☑

Corollary. If R is factorial, and f is a *monic* polynomial in R[X], and $r \in K$ is a *root* of f (i.e. $f(r) = 0$), then $r \in R$.

Lemma. Let R be a subring of a commutative ring S and $\mathfrak{P}$ a prime ideal in S. Then $\mathfrak{P} \cap R$ is a prime ideal in R.

Theorem. If R is a factorial domain, then so is $R[X]$. In this case the irreducible elements of $R[X]$ are the constant polynomials c, where c is irreducible in R, together with those polynomials $f \in R[X]$ such that $\operatorname{cont}(f) = R$ and f is irreducible as a polynomial in $K[X]$, where K is the quotient field of R.

PROOF: We have already seen that any irreducible element in $R[X]$ is either an irreducible constant in R or is a polynomial with content (1) which is also irreducible in $K[X]$. Conversely, if p is an irreducible element of R, then pR is a prime ideal of R and by Gauss's Lemma $pR[X]$ is prime, and consequently p is irreducible in $R[X]$. Now let $f \in R[X]$ be such that f is irreducible in $K[X]$ and $\operatorname{cont}(f) = R$. We have already noted that this implies that $(f) = R[X] \cap fK[X]$. Furthermore, $K[X]$ is factorial [Lang, Corollary 4.3, p. 191] and so the principal ideal $fK[X]$ is a prime ideal in $K[X]$ and hence $(f) = R[X] \cap fK[X]$ is a prime ideal in $R[X]$, hence f is irreducible. Thus we see that the irreducible elements in $R[X]$ are as claimed and that the principal ideals they generate are prime.

Finally, if $(g) \subseteq (f)$ then $f|g$ and $\deg(f) \leq \deg(g)$ and $\operatorname{cont}(f) \supseteq \operatorname{cont}(g)$. If further $\deg g = \deg f$ then g and f differ by a constant multiple, and if in addition $\operatorname{cont}(g) = \operatorname{cont}(f)$ then f and g differ by multiplication by a unit. Thus if $(g) \subsetneq (f)$ then either $\deg f < \deg f$ or $\operatorname{cont} f \supsetneq \operatorname{cont} g$. Since the degrees cannot decrease indefinitely and since R satisfies the a.c.c. on principal ideals, we see that $R[X]$ satisfies the a.c.c. on principal ideals. Thus $R[X]$ is factorial. ☑