# 5 Misc. Ring Tools

2/10: **5.1.** Let $M$ and $m$ denote the lcm and gcd of natural numbers $a, b$.

(i) Prove that there is an isomorphism of rings

$$\phi : \mathbb{Z}/(a) \times \mathbb{Z}/(b) \to \mathbb{Z}/(M) \times \mathbb{Z}/(m)$$

*Hint*: Chinese Remainder Theorem.

*Proof.* Let $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$, where $e_i, f_i \geq 0$ ($i = 1, \dots, n$) and we pick all primes to be greater than zero to obviate the need for multiplication by a unit (1 or $-1$ in this case). It follows that $ab = p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}$. We know from Proposition 8.13 that we can pick $m = p_1^{\min(e_1,f_1)} \cdots p_n^{\min(e_n,f_n)}$. Additionally, since $ab = mM$, we know that we can pick

$$M = p_1^{e_1+f_1-\min(e_1,f_1)} \cdots p_n^{e_n+f_n-\min(e_n,f_n)} = p_1^{\max(e_1,f_1)} \cdots p_n^{\max(e_n,f_n)}$$

By the Chinese Remainder Theorem (CRT), or more directly Corollary 7.18, we know that

$$\mathbb{Z}/(a) = \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \qquad \mathbb{Z}/(b) = \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n})$$

Thus,

$$\mathbb{Z}/(a) \times \mathbb{Z}/(b) \cong \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \times \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n})$$

Similarly,

$$\mathbb{Z}/(M) \times \mathbb{Z}/(m) \cong \mathbb{Z}/(p_1^{\max(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\max(e_n,f_n)}) \times \mathbb{Z}/(p_1^{\min(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\min(e_n,f_n)})$$

For every $i = 1, \dots, n$, there are two relevant terms in the above direct product: $\mathbb{Z}/(p_i^{\max(e_i,f_i)})$ and $\mathbb{Z}/(p_i^{\min(e_i,f_i)})$. We divide into two cases ($\min(e_i, f_i) = e_i$ and $\min(e_i, f_i) = f_i$). If $\min(e_i, f_i) = e_i$, then $\max(e_i, f_i) = f_i$ (this holds true even when $e_i = f_i$). Thus,

$$\mathbb{Z}/(p_i^{\min(e_i,f_i)}) = \mathbb{Z}/(p_i^{e_i}) \qquad \mathbb{Z}/(p_i^{\max(e_i,f_i)}) = \mathbb{Z}/(p_i^{f_i})$$

It follows that the $i^{\text{th}}$ and $(n+i)^{\text{th}}$ slots in the direct product expansions of $\mathbb{Z}/(a) \times \mathbb{Z}/(b)$ and $\mathbb{Z}/(M) \times \mathbb{Z}/(m)$ above are identical. Now suppose $\min(e_i, f_i) = f_i$. Then for a similar reason to the previous case,

$$\mathbb{Z}/(p_i^{\min(e_i,f_i)}) = \mathbb{Z}/(p_i^{f_i}) \qquad \mathbb{Z}/(p_i^{\max(e_i,f_i)}) = \mathbb{Z}/(p_i^{e_i})$$

Thus, since the direct product operation is commutative,[1] we may flip the entries in the $i^{\text{th}}$ and $(n+i)^{\text{th}}$ slots in the direct product expansion of $\mathbb{Z}/(M) \times \mathbb{Z}/(m)$ and still have an isomorphic ring. Doing this for all $i$ proves that

$$\begin{aligned}&\mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \times \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n}) \\ &\cong \mathbb{Z}/(p_1^{\max(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\max(e_n,f_n)}) \times \mathbb{Z}/(p_1^{\min(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\min(e_n,f_n)})\end{aligned}$$

and hence by transitivity that

$$\mathbb{Z}/(a) \times \mathbb{Z}/(b) \cong \mathbb{Z}/(M) \times \mathbb{Z}/(m)$$

Stating that two sets are isomorphic as rings is equivalent to stating that there exists an isomorphism of rings

$$\phi : \mathbb{Z}/(a) \times \mathbb{Z}/(b) \to \mathbb{Z}/(M) \times \mathbb{Z}/(m)$$

so we are done. ☐

[1] Ray said that this assertion need not be justified further.

(ii) Find necessary and sufficient conditions for uniqueness of the $\phi$. *Hint*: Do this first when $a = p^c$ and $b = p^d$, where $p$ is prime.

*Proof.* Let $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$. Then a necessary and sufficient condition for the uniqueness of $\phi$ is that

$$\boxed{e_i \neq f_i \; \forall \; i = 1, \dots, n}$$

$\square$

(iii) Prove that the condition you provided for part (ii) is sufficient.

*Proof.* Taking the hint from part (ii), we first treat the case where $a = p^c$ and $b = p^d$. WLOG, let $c \leq d$, in agreement with part (ii). Suppose that $a \neq b$. Then $c < d$. Since $\phi$ is a ring homomorphism, we know that $\phi(1,1) = (1,1)$.

Now let's investigate the behavior of $\phi(1,0)$ and $\phi(0,1)$. Let $\phi(1,0) = (\gamma, \delta)$. Since $(1,0)$ is idempotent, i.e., $(1,0)^2 = (1,0)$, we have that

$$\begin{aligned} \phi[(1,0)^2] &= \phi(1,0) \\ (\gamma, \delta)^2 &= (\gamma, \delta) \\ (\gamma^2, \delta^2) &= (\gamma, \delta) \\ (\gamma^2 - \gamma, \delta^2 - \delta) &= (0,0) \end{aligned}$$

Consider $\gamma(\gamma - 1) = 0$. It follows that $\gamma, \gamma - 1$ are zero divisors. Hence, at *least* one of $\gamma, \gamma - 1$ is a multiple of $p$. Additionally, since $p \geq 2$ and $\gamma, \gamma - 1$ are offset by 1, we know that $p$ divides at *most* one of these. Thus, we divide into two cases ($p \mid \gamma$ and $p \mid \gamma - 1$). Suppose first that $p \mid \gamma$. Then since the units of $\mathbb{Z}/p^n\mathbb{Z}$ are the integers coprime to $p$, we know that $\gamma - 1$ is a unit. It follows that there exists an element $(\gamma - 1)^{-1}$ and thus that

$$\begin{aligned} 0 &= (\gamma - 1)^{-1} \cdot \gamma(\gamma - 1) \\ 0 &= \gamma \end{aligned}$$

In the case $p \mid \gamma - 1$, we similarly derive that $0 = \gamma - 1$, or $\gamma = 1$. Thus, $\gamma \in \{1, 0\}$. Similarly, $\delta \in \{1, 0\}$.

Now suppose $\gamma = \delta = 1$. Then $\phi(1,1) = (1,1) = \phi(1,0)$ and $\phi$ is not an isomorphism, a contradiction. Similarly, if $\gamma = \delta = 0$, then $\phi(0,0) = (0,0) = \phi(1,0)$, which is the same contradiction. Therefore, $\phi(1,0) \in \{(1,0), (0,1)\}$.

It follows by a symmetric argument that $\phi(0,1) \in \{(1,0), (0,1)\}$. For the same isomorphism reason, $\phi(1,0)$ and $\phi(0,1)$ must equal distinct elements. Thus, $\phi$ can be two possible isomorphisms, since the values of $\phi(1,0)$ and $\phi(0,1)$ determine all other values of $\phi$.

We now invoke the condition that $c < d$. We know that $(1,0)^{p^c} = (0,0)$. Suppose $\phi(1,0) = (0,1)$. It follows that $\phi[(1,0)^{p^c}] = (0, p^c) \neq (0,0)$, we have a contradiction. Therefore, we must have that $\phi$ is the identity isomorphism.

Now suppose that $a, b$ have more complex prime factorizations. In particular, let $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$. The existence of $\phi$ implies the existence of an isomorphism

$$\begin{aligned} \psi : &\mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \times \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n}) \\ &\to \mathbb{Z}/(p_1^{\max(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\max(e_n,f_n)}) \times \mathbb{Z}/(p_1^{\min(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\min(e_n,f_n)}) \end{aligned}$$

Defining a restriction isomorphism to the $n$ sets consisting of elements where only the $p_i$ slots are nonzero, $\psi$ induces $n$ isomorphisms of the kind treated above. We know that all of these are unique. Thus, reassembling $\psi$, we have a unique isomorphism. It follows that $\phi$ is a unique isomorphism. $\square$

**5.2.** The Euclidean algorithm for monic polynomials is valid for every commutative ring, but it does not provide a method of obtaining the gcd because the "remainder" may not have a unit as its leading coefficient, so we cannot proceed by induction. But we may get lucky:

(i) Prove that the ideal generated by $X^m - 1$ and $X^n - 1$ in $\mathbb{Z}[X]$ is the principal ideal $(X^d - 1)$, where $d = \gcd(m, n)$.

*Proof.* We will prove that $(X^m - 1, X^n - 1) = (X^d - 1)$ via a bidirectional inclusion proof. Suppose first that $p \in (X^m - 1, X^n - 1)$. Then there exist polynomials $a, b \in \mathbb{Z}[X]$ such that $p(X) = a(X) \cdot (X^m - 1) + b(X) \cdot (X^n - 1)$. Now since $d = \gcd(m, n)$, there exist $s, t$ such that $m = sd$ and $n = td$. Using $s, t$, we may write

$$X^m - 1 = (X^d - 1) \cdot \sum_{i=0}^{s-1} X^{di} \qquad\qquad X^n - 1 = (X^d - 1) \cdot \sum_{i=0}^{t-1} X^{di}$$

Therefore,

$$\begin{aligned}
p(X) &= a(X) \cdot (X^m - 1) + b(X) \cdot (X^n - 1) \\
&= a(X) \cdot (X^d - 1) \cdot \sum_{i=0}^{s-1} X^{di} + b(X) \cdot (X^d - 1) \cdot \sum_{i=0}^{t-1} X^{di} \\
&= \left[ a(X) \cdot \sum_{i=0}^{s-1} X^{di} + b(X) \cdot \sum_{i=0}^{t-1} X^{di} \right] \cdot (X^d - 1) \\
&\in (X^d - 1)
\end{aligned}$$

as desired.

On the other hand, suppose that $p \in (X^d - 1)$. Then there exists a polynomial $a \in \mathbb{Z}[X]$ such that $p(X) = a(X) \cdot (X^d - 1)$. WLOG let $n \leq m$. Then since

$$X^m - 1 = X^{m-n}(X^n - 1) + (X^{m-n} - 1)$$

we see that we can actually invoke a Euclidean algorithm for monic polynomials here. Thus, continuing, we will eventually reach $X^d - 1$ and thus can rewrite

$$X^d - 1 = b(X) \cdot (X^m - 1) + c(X) \cdot (X^n - 1)$$

Therefore,

$$\begin{aligned}
p(X) &= a(X) \cdot (X^d - 1) \\
&= a(X) \cdot [b(X) \cdot (X^m - 1) + c(X) \cdot (X^n - 1)] \\
&= a(X)b(X) \cdot (X^m - 1) + a(X)c(X) \cdot (X^n - 1) \\
&\in (X^m - 1, X^n - 1)
\end{aligned}$$

as desired. □

(ii) Deduce that $\gcd(q^m - 1, q^n - 1) = (q^d - 1)$ for every integer $q$.

*Proof.* Consider the evaluation homomorphism $\mathrm{ev}_q : \mathbb{Z}[X] \to \mathbb{Z}$. Since every integer $z \in \mathbb{Z}$ is an element of $\mathbb{Z}[X]$, $\mathrm{ev}_q$ is surjective. It follows by Exercise 7.3.24(b) of Dummit and Foote (2004) (proven in HW2) that $\mathrm{ev}_q$ sends ideals to ideals. Thus, under $\mathrm{ev}_q$,

$$(X^m - 1, X^n - 1) \mapsto (q^n - 1, q^m - 1) \qquad\qquad (X^d - 1) \mapsto (q^d - 1)$$

It follows since $(X^m - 1, X^n - 1) = (X^d - 1)$ as per part (i) that $(q^n - 1, q^m - 1) = (q^d - 1)$, and hence $\gcd(q^m - 1, q^n - 1) = (q^d - 1)$, as desired. □

**5.3.** Let $K$ be the quotient field of a UFD $R$. If $f \in R[X]$ is a monic polynomial, $c \in K$, and $f(c) = 0$, then $c \in R$.

*Proof.* Since $f(c) = 0$, it follows that

$$f(X) = q(X) \cdot (X - c)$$

for some $q \in K[X]$. Note that since $f$ is monic, $q$ must have leading coefficient 1. The main takeaway from the above equation is that $f$ is reducible in $K[X]$. Thus, since $R$ is a UFD, $\operatorname{Frac} R = K$, $f \in R[X]$, and $f$ is reducible in $K[X]$, Gauss' Lemma asserts that there exist $r, s \in K$ such that $rq, s(X - c) \in R[X]$ and

$$f(X) = rq(X) \cdot s(X - c)$$

is a factorization of $f$ in $R[X]$. But since $q, (X - c)$ have leading coefficient 1 and $f$ is monic, we must have $rs = 1$. Therefore,

$$f(X) = q(X) \cdot (X - c)$$

is a factorization in $R[X]$. In particular, $X - c \in R[X]$, meaning that $c \in R$, as desired. $\square$

**5.4.** State whether true or false. If false, give a counterexample.

(i) If $R$ is a UFD, then $D^{-1}R$ is a UFD.

*Answer.* True. $\square$

(ii) Let $K$ be the field of fractions of a PID $R$. If $R \subset A \subset K$ is a chain of rings, then $A = D^{-1}R$ for some multiplicative subset $D$ of $R$.

*Answer.* True. $\square$

(iii) Same problem as in (ii), except that now $R$ is a UFD.

*Answer.* True. $\square$

(iv) Let $K$ be the field of fractions of an integral domain $R$. If $D_1, D_2$ are multiplicative subsets of $R$, then $D_1^{-1}R$ and $D_2^{-1}R$ are subrings of $K$. If $D_1^{-1}R = D_2^{-1}R$, then $D_1 = D_2$.

*Answer.* False.
Let $R = \mathbb{Z}$. Pick $D_1 = \mathbb{N}$ and $D_2 = \mathbb{Z} - \{0\}$. Then since $D_1 \subset D_2$, any $a/b \in D_1^{-1}R$. If $a/b \in D_2^{-1}R$, then we divide into two cases. If the denominator is positive, we are done. If the denominator is negative, represent the fraction by another member of the equivalence class: $-a/-b \in D_1^{-1}R$. $\square$

**5.5.** Let $f \in \mathbb{Z}[X]$ be a polynomial with content 1. Let $p$ be prime and let $\bar{f}$ denote the image of $f$ in $\mathbb{F}_p[X]$. If $\deg(f) = \deg(\bar{f})$ and $\bar{f}$ is irreducible, show that $f$ is irreducible in $\mathbb{Z}[X]$.

*Proof.* To prove that $f$ is irreducible in $\mathbb{Z}[X]$, it will suffice to show that for any factorization $f = qh$ of $f$, $q$ or $h$ is a unit. Let $f = qh$, let $d = \deg(f)$, and let $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$. We have that

$$\bar{f} = \pi(f) = \pi(qh) = \pi(q)\pi(h) = \bar{q} \cdot \bar{h}$$

Since $\bar{f}$ is irreducible, either $\bar{q}$ or $\bar{h}$ is a unit in $\mathbb{F}_p[X]$. WLOG, let $\bar{h}$ be a unit. Then $\deg(\bar{h}) = 0$. Thus,

$$\deg(\bar{q}) = \deg(\bar{f}) - \deg(\bar{h}) = d - 0 = d$$

It follows since $\deg(q) \geq \deg(\bar{q})$ that $\deg(q) = d$, and hence $\deg(h) = 0$ as well. Consequently, $h$ is an integer. Moreover, since $c(f) = 1$, $h \mid 1$, so $h = \pm 1$, i.e., is a unit. Therefore, $f$ is irreducible in $\mathbb{Z}[X]$. $\square$

**5.6.** If $R$ is a (commutative) ring of characteristic $p$, where $p$ is prime, show that $(a+b)^p = a^p + b^p$.

*Proof.* By the binomial theorem,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} y^k = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^{p-k} y^k$$

It follows that in all cases except when $k = 0, p$, the coefficient is a multiple of $p$. In particular, if the coefficient is a multiple of $p$ in a ring of characteristic $p$, the coefficient is equal to zero. Therefore, all terms save the $k = 0$ and $k = p$ terms disappear, leaving only

$$(a+b)^p = a^p + b^p$$

as desired. $\square$