4 Ring Homomorphisms

Definition 4.1 A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all $a, b \in R$,

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism.*

Proposition 4.1 (Theorems 15.1, 15.2) *Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.*

(i) *$\phi(A)$ is a subring of S. In particular, $\phi(R)$ is a subring of S.*

(ii) *If A is an ideal of R, then $\phi(A)$ is an ideal of $\phi(R)$. In particular, if ϕ is onto, $\phi(A)$ is an ideal of S.*

(iii) *$\phi^{-1}(B)$ is an ideal of R. In particular,* $\mathrm{Ker}(\phi)$ *is an ideal of R.*

(iv) *ϕ is one-to-one if and only if* $\mathrm{Ker}(\phi) = \{0\}$.

(v) *If ϕ is an isomorphism from R to S, then ϕ^{-1} is an isomorphism from S onto R.*

Theorem 4.2 (Theorem 15.3) *Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/ker(\phi)$ to $\phi(R)$, given by $r + \mathrm{Ker}(\phi) \mapsto \phi(r)$, is an isomorphism. In symbols, $R/\mathrm{Ker}(\phi) \approx \phi(R)$.*

Proof. Let us consider the induced group isomorphism:

$$\bar{\phi} : R/ker(\phi) \to \phi(R) \subset S \ (r + \mathrm{Ker}(\phi) \mapsto \phi(r)).$$

This is a ring isomorphism because

$$\begin{aligned} \bar{\phi}((r + \mathrm{Ker}(\phi))(r' + \mathrm{Ker}(\phi)) &= \bar{\phi}(rr' + \mathrm{Ker}(\phi)) = \phi(rs) = \phi(r)\phi(r') \\ &= \bar{\phi}(r + \mathrm{Ker}(\phi))\bar{\phi}(r' + \mathrm{Ker}(\phi)). \qquad \blacksquare \end{aligned}$$

Note. Every ideal A of a ring R is the kernel of a homomorphism $\phi : R \to R/A$ $(x \mapsto x + A)$.

Example 4.1 Let $R = \boldsymbol{Z}[x]$ and $A = \{f \in \boldsymbol{Z}[x] \mid f(0) = 0\}$. Then A is the kernel of

$$\phi : \boldsymbol{Z}[x] \to \boldsymbol{Z} \ (f \mapsto f(0)).$$

Since ϕ is onto, $\boldsymbol{R}[x]/A \approx \boldsymbol{Z}$. Since $\boldsymbol{Z}$ is an integral domain, A is a prime ideal of $\boldsymbol{R}[x]$. Since $\boldsymbol{Z}$ is not a field, A is not maximal.

Example 4.2 Let $R = \boldsymbol{Z}[x]$ and

$$\varphi : \boldsymbol{Z}[x] \to \boldsymbol{Z}_2 \ (a_0 + a_1 x + \cdots + a_n x^n \mapsto \overline{a_0}),$$

where for every integer a, $\overline{a}$ denotes the corresponding elements in $\boldsymbol{Z}_2$. Since φ is onto, and $\mathrm{Ker}(\varphi) = \langle 2, x \rangle$, $\boldsymbol{R}[x]/\mathrm{Ker}(\varphi) \approx \boldsymbol{Z}_2$. Since $\boldsymbol{Z}_2$ is a field, $\langle 2, x \rangle$ is a maximal ideal.

Example 4.3 [See Ex.14.22] Let $R = \boldsymbol{Z}[x]$ and

$$\psi : \boldsymbol{Z}[x] \to \boldsymbol{Z}_2[x] \ (a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n),$$

where for every integer a, $\overline{a}$ denotes the corresponding elements in $\boldsymbol{Z}_2$. Since ψ is onto, and $\mathrm{Ker}(\psi) = \langle 2 \rangle$, $\boldsymbol{R}[x]/\mathrm{Ker}(\psi) \approx \boldsymbol{Z}_2[x]$. Since $\boldsymbol{Z}_2[x]$ is an integral domain, but not a field, $\langle 2 \rangle$ is a prime ideal of $\boldsymbol{Z}[x]$, but it is not maximal.

Exercise 4.1 Prove the following evercises in Chapter 14 and Supplementary Exercises for Chapters 12–14.

1. Show that $A = \{f \in \boldsymbol{R}[x] \mid f(0) = 0\}$ is a maximal ideal in $\boldsymbol{R}[x]$. Ex.14.31
2. Show that $\boldsymbol{R}[x]/\langle x^2 + 1 \rangle$ is a field. Ex.14.28
3. $\langle x, y \rangle$ is a prime ideal in $\boldsymbol{Z}[x, y]$ but not maxima. Suppl.Ex.42
4. $\langle x, y \rangle$ is a maximal ideal in $\boldsymbol{Z}_5[x, y]$. Suppl.Ex.43
5. $\langle 2, x, y \rangle$ is a maximal ideal in $\boldsymbol{Z}[x, y]$. Suppl.Ex.44

Proposition 4.3 (Theorem 15.5, Corollaries 1, 2, 3) *Suppose R is a ring with unity.*

(i) *The mapping $\phi : \boldsymbol{Z} \to R$ $(n \mapsto n \cdot 1)$ is a ring homomorphism.*

(ii) *If $\mathrm{char}(R) = 0$, then R contains a subring isomorphic to $\boldsymbol{Z}$. If $\mathrm{char}(R) = n > 0$, then R contains a subring isomorphic to $\boldsymbol{Z}_n$.*

(iii) *If F is a field of characteristic 0, F contains a subfield isomorphic to $\boldsymbol{Q}$.*

Proof. (iii) Let S is a subring isormophic to $\boldsymbol{Z}$ and let $T = \{ab^{-1} \mid a, b \in S, b \neq 0\}$. Then T is isomorphic to $\boldsymbol{Q}$. (Exercise 63) ∎

Theorem 4.4 (Theorem 15.6) *Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D.*

Proof. Let $S = \{(a, b) \mid a, b \in D, b \neq 0\}$. We define an equivalence relation on S by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Let F denote the set of equivalence classes of S and write x/y for the equivalence class containing (x, y). Define addition and multiplication on F as follows.

$$a/b + c/d = (ad + bc)/(bd) \quad \text{and } a/b \cdot c/d = (ac)/(bd).$$

Then these operations are well-defined and F becomes a field.

Finally the mapping

$$\phi : D \to F \ (x \mapsto x/1)$$

is a ring isomorphism from D to $\phi(D)$. ∎

abc conjecture For a positive integer n, the radical of n, denoted $\mathrm{rad}(n)$, is the product of the distinct prime factors of n. For example

$$\mathrm{rad}(16) = \mathrm{rad}(4) = 2,\ \mathrm{rad}(17) = 17,\ \mathrm{rad}(18) = \mathrm{rad}(24) = 2 \cdot 3 = 6.$$

If a, b, and c are coprime positive integers such that $a + b = c$, it turns out that "usually" $c < \mathrm{rad}(abc)$. The abc conjecture deals with the exceptions. Specifically, it states that for every $\epsilon > 0$ there exist only finitely many triples (a, b, c) of positive coprime integers with $a + b = c$ such that

$$c > \mathrm{rad}(abc)^{1+\epsilon}.$$

An equivalent formulation states that for any $\epsilon > 0$, there exists a constant K such that, for all triples of coprime positive integers (a, b, c) satisfying $a + b = c$, the inequality

$$c < K \cdot \mathrm{rad}(abc)^{1+\epsilon}$$

holds. A third formulation of the conjecture involves the quality $q(a, b, c)$ of the triple (a, b, c), defined by:

$$q(a, b, c) = \frac{\log(c)}{\log(\mathrm{rad}(abc))}.$$

For example

- $q(4, 127, 131) = \log(131)/\log(\mathrm{rad}(4 \cdot 127 \cdot 131)) = \log(131)/\log(2 \cdot 127 \cdot 131) = 0.46820....$
- $q(3, 125, 128) = \log(128)/\log(rad(3 \cdot 125 \cdot 128)) = \log(128)/\log(30) = 1.426565....$

A typical triple (a, b, c) of coprime positive integers with $a + b = c$ will have $c < \mathrm{rad}(abc)$, i.e. $q(a, b, c) < 1$. Triples with $q > 1$ such as in the second example are rather special, they consist of numbers divisible by high powers of small prime numbers. The *abc* conjecture states that, for any $\epsilon > 0$, there exist only finitely many triples (a, b, c) of coprime positive integers with $a + b = c$ such that $q(a, b, c) > 1 + \epsilon$. Whereas it is known that there are infinitely many triples (a, b, c) of coprime positive integers with $a + b = c$ such that $q(a, b, c) > 1$, the conjecture predicts that only finitely many of those have $q > 1.01$ or $q > 1.001$ or even $q > 1.0001$, etc...

Example 4.4 [Example 9 (Theorem of Gersonides)] *If* $2^m - 3^n = \pm 1$, *then*

$$(2^m, 3^n) = (2, 1), (2, 3), (4, 3), (8, 9).$$

Case 1. $2^m = 3^n + 1$.
$3^n + 1 \equiv 4$ or $2 \pmod 8$. Thus $m \leq 2$.
Case 2. $2^m = 3^n - 1$.
$3^n - 1 \equiv 2, 8, 10,$ or $0 \pmod{16}$. Thus $m \leq 2$. $n \not\equiv 1, 2, 3$. $3^{4k} - 1 \equiv 0 \pmod 5$.