

8 Irreducibility

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-10-03

For polynomials, irreducibility depends on the coefficients that are acceptable in the factors. We present probably the two best known techniques for identifying irreducible polynomials.

8.0 Basic Sieve Theory

The *sieve of Eratosthenes* is a method of determining the primes less than a given number n . List the integers from 2 to n . The smallest entry 2 is prime. Cross out the multiples of 2 from our list. The smallest remaining entry 3 is prime because it is not divisible by any smaller prime. Cross out the multiples of 3. Repeat. Using this method, Table 8.1 lists the prime integers less than 100.

The Greek polymath, [Eratosthenes of Cyrene](#) (276BCE–194BCE), is famous for his work on prime numbers and for measuring the diameter of the earth.

2	3	4	5	6	7	8	9	10	
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	

Table 8.1: The 25 prime integers less than 100

For any prime integer p , this method also allows one to uncover the irreducible polynomials in $\mathbb{F}_p[x]$. List all polynomials by degree and then cross out products. Table 8.2 enumerates the irreducible polynomials of degree at most 4 in $\mathbb{F}_2[x]$.

$\emptyset$	1	x	$x+1$
x^2	x^2+1	x^2+x	x^2+x+1
x^3	x^3+1	x^3+x	x^3+x+1
x^3+x^2	x^3+x^2+1	x^3+x^2+x	x^3+x^2+x+1
x^4	x^4+1	x^4+x	x^4+x+1
x^4+x^2	x^4+x^2+1	x^4+x^2+x	x^4+x^2+x+1
x^4+x^3	x^4+x^3+1	x^4+x^3+x	x^4+x^3+x+1
$x^4+x^3+x^2$	$x^4+x^3+x^2+1$	$x^4+x^3+x^2+x$	$x^4+x^3+x^2+x+1$

Table 8.2: The irreducible polynomials in $\mathbb{F}_2[x]$ having small degree

8.0.1 Remark. Since $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, the quotient $K := \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$ is a field. If α denotes the image of x in K , then $\{1, \alpha\}$ forms a basis of K over $\mathbb{F}_2$. Hence, the field K has four elements; namely $\{0, 1, \alpha, 1 + \alpha\}$.

8.0.2 Theorem. Let p be a prime integer. Setting N_d to be the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ having degree d , we have

$$\sum_{d|n} d N_d = p^n.$$

Proof. Consider the formal power series $\sum_g t^{\deg(g)}$ in $\mathbb{Z}[[t]]$ where the sum is over all monic polynomials g in $\mathbb{F}_p[x]$. The total number of monic polynomials g in $\mathbb{F}_p[x]$ of degree n is p^n , so

$$\sum_g t^{\deg(g)} = \sum_{n=0}^{\infty} p^n t^n = \frac{1}{1-pt}.$$

As the ring $\mathbb{F}_p[x]$ is a unique factorization domain, we obtain

$$\sum_g t^{\deg(g)} = \prod_f (1 - t^{\deg(f)})^{-1} = \prod_{d=1}^{\infty} (1 - t^d)^{-N_d}$$

where the middle product is over all monic irreducible polynomials f in $\mathbb{F}_p[x]$. It follows that

$$\frac{1}{1-pt} = \prod_{d=1}^{\infty} (1 - t^d)^{-N_d}.$$

Taking logarithms gives

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{p^n t^n}{n} &= -\log(1-pt) = -\sum_{d=1}^{\infty} N_d \log(1-t^d) \\ &= \sum_{d=1}^{\infty} \sum_{e=1}^{\infty} d N_d \frac{t^{de}}{de} = \sum_{n=1}^{\infty} \frac{t^n}{n} \left(\sum_{de=n} d N_d \right), \end{aligned}$$

and comparing coefficients gives the desired equation. $\square$

8.0.3 Definition. For any positive integer n , the *Möbius function* μ has values in $\{-1, 0, 1\}$ depending on the prime factorization of n :

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes,} \\ 0 & \text{if } n \text{ is divisible by a square greater than 1.} \end{cases}$$

8.0.4 Corollary. Let p be a prime integer. When N_n denotes the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ having degree n , we have

$$N_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

The corollary follows from the proposition by the Möbius inversion formula, which was introduced by [August F. Möbius \(1832\)](#).

8.0.5 Theorem. Let p be a prime integer and, for some positive integer d , set $q := p^d$. Every monic irreducible polynomial of degree d in $\mathbb{F}_p[x]$ is a factor of $x^q - x$. The irreducible factors of $x^q - x$ in $\mathbb{F}_p[x]$ are precisely the monic irreducible polynomials in $\mathbb{F}_p[x]$ whose degree divides d .

There are effective algorithms for factoring in $\mathbb{F}_p[x]$; for instance, the [Berlekamp algorithm](#) and [Cantor-Zassenhaus algorithm](#).

Sketch of proof. Since $(d/dx)(x^q - x) = qx^{q-1} - 1 = -1$, this monic polynomial has no multiple roots. Hence, its splitting field has q elements. $\square$

8.0.6 Example. In $\mathbb{F}_2[x]$, we have

$$\begin{aligned} x^8 - x &= x(x+1)(x^3+x+1)(x^3+x^2+1) \\ x^{16} - x &= x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1). \end{aligned}$$

In $\mathbb{F}_3[x]$, we have

$$x^9 - x = x(x+1)(x-1)(x^2+1)(x^2+x-1)(x^2-x-1). \quad \diamond$$

8.1 Irreducibility Criteria

We can, in some circumstances, identify an irreducible polynomial without finding all of the irreducible polynomials of lower degree.

8.1.1 Example. Is $f(x) = x^3 + 6x^2 + 7$ in $\mathbb{Z}[x]$ irreducible? Yes, it is irreducible. Otherwise, the cubic polynomial f would have linear factor and its root would divide 7. However, we have $f(1) = 14$, $f(-1) = 12$, $f(7) > 0$, and $f(-7) = (-1)(49) + 7 < 0$. $\diamond$

8.1.2 Proposition. *Let R be a commutative ring and consider*

$$f := a_n x^n + \cdots + a_1 x + a_0$$

in $R[x]$. Suppose that $\langle p \rangle$ is a prime ideal in R that does not contain a_n . The image of f in $R/\langle p \rangle[x]$ being irreducible implies that the polynomial f is irreducible in $R[x]$.

Proof. The canonical ring homomorphism $R \rightarrow R/\langle p \rangle$ induces a ring homomorphism $\varphi: R[x] \rightarrow R/\langle p \rangle[x]$. When $f = gh$ in R , it follows that $\varphi(f) = \varphi(g)\varphi(h)$. The assumption that $\langle p \rangle$ does not contain a_n implies that $\deg(\varphi(g)) = \deg(g)$ and $\deg(\varphi(h)) = \deg(h)$. Hence, reducibility of the polynomial f leads to the reducibility of $\varphi(f)$. $\square$

8.1.3 Example. Is $x^4 + 15x^3 + 7$ in $\mathbb{Q}[x]$ irreducible? Its image in $\mathbb{F}_5[x]$ is $x^4 + 2$. By evaluating $x^4 + 2$ at all five elements in $\mathbb{F}_5$, we see that it has no root in $\mathbb{F}_5$. Suppose that there exists a, b, c , and d in $\mathbb{F}_5$ such that $x^4 + 2 = (x^2 + ax + b)(x^2 + cx + d)$. It follows that $a + c = 0$, $ac + b + d = 0$, $ad + bc = 0$, and $bd = 2$. Since $c = -a$, we have $0 = ad + bc = a(d - b)$, so $a = 0$ or $d = b$. We consider these two cases separately.

$(a = 0)$ It follows that $c = 0$. The equations $b + d = 0$ and $bd = 2$ imply that $d = -b$, $-b^2 = 2$, and $b^2 = 3$. However, $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, and $4^2 = 1$, so there is no element b in $\mathbb{F}_5$ such that $b^2 = 3$.

$(b = d)$ It follows that $b^2 = 2$. This is again impossible because the only perfect squares in $\mathbb{F}_5$ are 0, 1, and 4.

Having established that the polynomial $x^4 + 2$ is irreducible in $\mathbb{F}_5[x]$, Proposition 8.1.2 shows that $x^4 + 15x^3 + 7$ is irreducible in $\mathbb{Z}[x]$ and Lemma 7.3.2 shows that it is irreducible in $\mathbb{Q}[x]$. $\diamond$

8.1.4 Theorem (Schönemann–Eisenstein Criterion). *Let R a domain and let $f := a_0 + a_1 x + \cdots + a_n x^n$ in $R[x]$ be a primitive polynomial of positive degree n . When there exists a prime ideal P in R such that*

(leading coefficient) $a_n \notin P$,

(trailing coefficients) $a_0, a_1, \dots, a_{n-1} \in P$, and

(constant term) $a_0 \notin P^2$,

the polynomial f is irreducible in $R[x]$.

Theodor Schönemann (1846) first published a version of this criterion whereas **Gotthold Eisenstein (1850)** published a somewhat different version in the same journal. **David A. Cox (2011)** explores the history.

Proof. Suppose that $f = gh$ for some g and h in $R[x]$ having positive degree. Set $g := b_0 + b_1x + \cdots + b_rx^r$ and $h := c_0 + c_1x + \cdots + c_sx^s$ where $\deg(g) = r$ and $\deg(h) = s$. It follows that $a_0 = b_0c_0 \in P$. As P is a prime ideal, we have $b_0 \in P$ or $c_0 \in P$. Having both b_0 and c_0 belong to P would imply that $a_0 \in P^2$ contradicting our hypotheses. Thus, we may assume that $b_0 \in P$ and $c_0 \notin P$. If every coefficient of g was in P , then every coefficient of f would also be in P again contradicting our hypothesis. Let b_i be the first coefficient of g such that $b_i \notin P$. Since $a_i = b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i$, we obtain the equation $b_ic_0 = a_i - b_{i-1}c_1 - \cdots - b_0c_i$. Every element on the right side of this equation lies in P . However, this implies that $b_ic_0 \in P$. As P is prime, either $b_i \in P$ or $c_0 \in P$ which is a contradiction. $\square$

The following special case is most convenient.

8.1.5 Corollary. *Let R be a unique factorization domain with fraction field K and consider $f := a_0 + a_1x + \cdots + a_nx^n$ in $R[x]$. When there exists an irreducible element p in R such that*

(leading coefficient) p does not divide a_n ,

(trailing coefficients) p divides a_i for all $0 \leq i \leq n-1$, and

(constant term) p^2 does not divide a_0 ,

the polynomial f is irreducible in $K[x]$.

Proof. Theorem 8.1.4 shows that the polynomial f is irreducible in $R[x]$ and Lemma 7.3.2 shows that f is irreducible in $K[x]$. $\square$

8.1.6 Example. Is $x^5 - 6x^4 + 3$ in $\mathbb{Q}[x]$ irreducible? Yes, simply apply Corollary 8.1.5 with $p = 3$. $\diamond$

The original impetus for the Schönemann–Eisenstein Criterion was the following application.

8.1.7 Corollary. *For any prime integer p , the polynomial*

$$f := x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

Proof. Since $(x-1)f(x) = x^p - 1$, the substitution $x \mapsto y+1$ yields

$$yf(y+1) = (y+1)^p - 1 = y^p + \binom{p}{1}y^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-1}y.$$

We have $\binom{p}{i} = p(p-1)\cdots(p-i+1)/i!$. When $i < p$, the prime p is not a factor of $i!$, so $i!$ divides the product $(p-1)\cdots(p-i+1)$ which implies that $\binom{p}{i}$ is divisible by p . Dividing the expansion of $yf(y+1)$ by y shows that $f(y+1)$ satisfies the hypothesis of Corollary 8.1.5. Therefore, the polynomial $y^{p-1} + \binom{p}{1}y^{p-2} + \binom{p}{2}y^{p-3} + \cdots + \binom{p}{p-1}$ is irreducible and it follows that f also is. $\square$

8.2 Exercises

8.2.1 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

- i. All three of the polynomials $x^2 + 1$, $x^2 + x - 1$, and $x^2 - x - 1$ are irreducible in $\mathbb{F}_3[x]$.
- ii. The polynomial $x^4 - 6x^3 + 12x^2 - 3x + 9$ in $\mathbb{Z}[x]$ is irreducible.

8.2.2 Problem. Determine all of the monic irreducible polynomials of degree 3 over $\mathbb{F}_3$.

8.2.3 Problem. Prove that

$$\frac{\mathbb{F}_3[x]}{\langle x^3 - x - 1 \rangle} \cong \frac{\mathbb{F}_3[x]}{\langle x^3 - x^2 + x + 1 \rangle}.$$

8.2.4 Problem. Factor $x^4 + 1$ into irreducibles in $\mathbb{F}_2[x]$, $\mathbb{F}_7[x]$, $\mathbb{F}_{13}[x]$, $\mathbb{F}_{17}[x]$, and $\mathbb{Q}[x]$.

8.2.5 Problem. Consider $f := xz - yw$ in $\mathbb{Z}[w, x, y, z]$.

- i. Prove that $\langle f \rangle$ is a prime ideal in $\mathbb{Z}[w, x, y, z]$.
- ii. Prove that $\mathbb{Z}[w, x, y, z]/\langle f \rangle$ is not a unique factorization domain.

Can the false statements be salvaged in some way? In other words, can one find a closely related nontrivial true statement.

Part III

Module Theory

Modules

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-10-31

Over a commutative ring, modules remedy the asymmetry between ideals and quotients by providing a common generalization for both.

8.3 Modules over a Commutative Ring

A module is an algebraic structure on a pair of underlying sets with four binary operations. Although modules can be defined over an arbitrary ring, we focus on modules over a commutative ring.

8.3.1 Definition. Let R be a commutative ring. An R -**module** is an additive abelian group V with a **scalar multiplication** $R \times V \rightarrow V$ such that, for any ring elements r and s in R and any module elements u and v in V , we have the following:

$$\begin{aligned} (\text{associativity}) \quad (rs)v &= r(sv) \quad \text{and} \quad 1_R v = v, \\ (\text{distributivity}) \quad r(u+v) &= ru + rv \quad \text{and} \quad (r+s)v = rv + sv. \end{aligned}$$

Like most multiplication operations, scalar multiplication $R \times V \rightarrow V$ simply denoted by $(r, v) \mapsto rv$.

We also assume that left and right scalar multiplication agree: for any r in R and any v in V , we have $rv = vr$.

8.3.2 Example. For any field K , the definitions of a K -vector space and a K -module are identical. $\diamond$

8.3.3 Example. Every abelian group is a $\mathbb{Z}$ -module in a unique way. For any positive integer n and any element g in an abelian group G , we have $0_{\mathbb{Z}}g = 0_G$, $(-n)g = -(ng)$, and $ng = \underbrace{g + g + \cdots + g}_{n \text{ summands}}$. $\diamond$

8.3.4 Example. Every ring R is an R -module where multiplication in the ring and scalar multiplication coincide. $\diamond$

8.3.5 Example. For any nonnegative integer n , the set $R^n := \prod_{i=1}^n R$ of n -tuples of elements in R forms an R -module with the addition and scalar multiplication defined componentwise. $\diamond$

8.3.6 Example. Every ideal in R is an R -module. $\diamond$

8.3.7 Example. A ring homomorphism $\varphi: R \rightarrow S$ makes S into an R -module. For any ring element r in R and any module element v in S , we have $rv := \varphi(r)v$. $\diamond$

8.3.8 Lemma (Basic properties). Let V be an R -module

(multiplication by 0) For any element v in V , we have $0_R v = 0_V$.

(multiplication by -1) When $-v$ denotes the additive inverse of the element v in V , we have $(-1)(-v) = v$.

Compare with Lemma 5.0.8.

Proof. The additive identity in the ring R and distributivity in the module V gives $0_R v = (0_R + 0_R) v = 0_R v + 0_R v$. Adding the additive inverse $-0_R v$ to both sides yields $0_R v = 0_V$.

Multiplication by 0_R and the defining properties of the module V establish that $0_V = (0_R)(-v) = (-1 + 1)(-v) = (-1)(-v) + (-v)$. Adding the additive inverse v to both sides yields $v = (-1)(-v)$. $\square$

8.3.9 Definition. Let V and W be R -modules. A map $\varphi: V \rightarrow W$ is an R -**module homomorphism** or R -**linear** if, for any r and s in R and any u and v in V , we have $\varphi(ru + sv) = r\varphi(u) + s\varphi(v)$.

8.3.10 Example. For any field K , being K -module homomorphism is equivalent to being a linear transformation of vector spaces. $\diamond$

8.3.11 Example. Every group homomorphism of abelian groups is a $\mathbb{Z}$ -module homomorphism. $\diamond$

8.3.12 Example. Let V and W be R -modules. The set $\text{Hom}_R(V, W)$ of R -module homomorphisms from V to W forms an R -module. For any φ and ψ in $\text{Hom}_R(V, W)$, any r and s in R , and any v in V , we have $(r\varphi + s\psi)(v) = r\varphi(v) + s\psi(v)$. $\diamond$

8.3.13 Example. An R -linear map $\varphi: R \rightarrow V$ is uniquely determined by the image $\varphi(1_R)$. It follows that, for any R -module V , there exists a canonical isomorphism $\text{Hom}_R(R, V) \cong V$ defined, for any φ in $\text{Hom}_R(R, V)$, by $\varphi \mapsto \varphi(1_R)$. $\diamond$

8.3.14 Example. Given R -module homomorphisms $\varphi: V \rightarrow V'$ and $\psi: W \rightarrow W'$, there are induced R -module homomorphisms

$$\begin{aligned} \text{Hom}(\varphi, W): \text{Hom}_R(V', W) &\rightarrow \text{Hom}_R(V, W) \\ \text{Hom}(V, \psi): \text{Hom}_R(V, W) &\rightarrow \text{Hom}_R(V, W'), \end{aligned}$$

defined, for any θ' in $\text{Hom}_R(V', W)$ and any θ in $\text{Hom}_R(V, W)$, by $(\text{Hom}(\varphi, W))(\theta') := \theta' \circ \varphi$ and $(\text{Hom}(V, \psi))(\theta) := \psi \circ \theta$. $\diamond$

8.3.15 Example. For any R -module V , the composition of R -module homomorphisms defines a noncommutative ring structure on the R -module $\text{Hom}_R(V, V)$. The multiplicative unit is the identity map $\text{id}_V: V \rightarrow V$. An R -module homomorphism from V to itself is also called an **endomorphism** of V and $\text{End}_R(V) := \text{Hom}_R(V, V)$. $\diamond$

8.3.16 Proposition. An R -module homomorphism is an isomorphism if and only if the underlying map of sets is bijective.

Proof. Suppose that the R -linear map $\varphi: V \rightarrow W$ is an isomorphism. The underlying map of sets has an inverse, so it is bijective.

Conversely, suppose that underlying map φ is bijective. There exists a map $\psi: W \rightarrow V$ such that $\varphi \circ \psi = \text{id}_W$ and $\psi \circ \varphi = \text{id}_V$. It remains to prove that this map of sets is R -linear. Since φ is an R -module homomorphism, it follows that, for any r and s in R , and any v and w in W , we have

$$\varphi(r\psi(v) + s\psi(w)) = r\varphi(\psi(v)) + s\varphi(\psi(w)) = rv + sw,$$

so $r\psi(v) + s\psi(w) \in V$ is the unique element that φ sends to $rv + sw$. By definition, this implies $\psi(rv + sw) = r\psi(v) + s\psi(w)$. $\square$

The composition of R -module homomorphisms is again an R -module homomorphism. The identity map on any R -module is an R -module homomorphism.

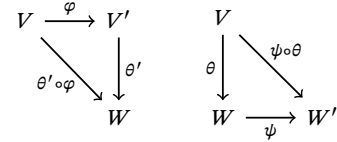


Figure 8.1: Commutative diagrams arising from Example 8.3.14

Multiplication by a fixed ring element r in R , also called **homothety by r** , gives an R -module endomorphism defined, for any v in V , by $v \mapsto rv$.

Compare with Proposition 2.0.6 and Remark 5.1.2.

8.4 Isomorphism Theorems

For a third time, there are basic results describing some universal features of homomorphisms, quotients, and subobjects.

Throughout this chapter, the underlying ring R is commutative.

8.4.1 Definition. A subset U of an R -module V is a **submodule** if the restriction of addition and scalar multiplication on V induces an R -module structure on U .

Compare with Definition 1.2.1 and Definition 5.0.10.

8.4.2 Proposition. Let V be an R -module. A nonempty subset U is a submodule of V if and only if, for any r and s in R , and any u and v in U , the R -linear combination $ru + sv$ belongs to U .

Proof. Any R -module is, by definition, closed under addition and scalar multiplication, so it is closed under R -linear combinations.

Suppose that subset U is closed under R -linear combinations. Since $(1)u + (-1)v = u - v$ belongs to U for any u and v in U , Lemma 1.2.2 shows that U is an additive abelian group. The subset U is closed under scalar multiplication because $ru + 0v = ru$ lies in U for any r in R and any u and v in U . Finally, associativity and distributivity are inherited from V , so U is an R -module. $\square$

8.4.3 Example. In any R -module V , the set $\{0\}$ is a submodule. $\diamond$

8.4.4 Example. Submodules of the R -module R^1 are ideals. $\diamond$

8.4.5 Lemma. Let V be an R -module. For any family $\{U_j \mid j \in J\}$ of submodules in V , the intersection $U := \bigcap_{j \in J} U_j$ is a submodule of V . $\square$

Compare with Lemma 1.2.8 and Lemma 8.4.5.

8.4.6 Definition. Let V be an R -module. For any subset U of V , the **submodule of V generated by U** , denoted by $\langle U \rangle$, is the intersection of all submodules of V that contain U . A module V is **finitely generated** if $V = \langle U \rangle$ for some finite subset $U \subseteq V$. Moreover, V is **cyclic** if $V = \langle U \rangle$ for some subset U having cardinality 1.

8.4.7 Example. For any ring R , the R -modules R^1 is cyclic, generated by the multiplicative identity element. $\diamond$

8.4.8 Proposition. Let $\varphi: V \rightarrow W$ be an R -linear map. The image

$$\text{Im}(\varphi) := \{w \in W \mid \text{there exists } v \in V \text{ such that } \varphi(v) = w\}$$

of φ is a submodule of its target W , and the kernel

$$\text{Ker}(\varphi) := \{v \in V \mid \varphi(v) = 0\},$$

of φ is a submodule of its source V .

Corollary 2.0.10 implies that an R -module homomorphism is injective if and only if its kernel is trivial.

Proof. For any v' and w' in $\text{Im}(\varphi)$, there exists v and w in V such that $\varphi(v) = v'$ and $\varphi(w) = w'$. For any r and s in R , we have

$$\varphi(rv + sw) = r\varphi(v) + s\varphi(w) = rv' + sw',$$

so $\text{Im}(\varphi)$ is a submodule of W . Similarly, for any r and s in R , and any u and v in $\text{Ker}(\varphi)$, we have

$$\varphi(ru + sv) = r\varphi(u) + s\varphi(v) = r0 + s0 = 0,$$

so $\text{Ker}(\varphi)$ is a submodule of V . $\square$

8.4.9 Definition. Let U be a submodule of an R -module V . The quotient group V/U inherits an R -module structure from V defined, for any r in R and any v in V , by $r(v + U) := rv + U$. This operation also makes the canonical map $\pi: V \rightarrow V/U$ into an R -linear map.

As $v + U = u + U \Leftrightarrow v - u \in U$, we see that $rv - ru = r(v - u) \in U$ and $rv + U = ru + U$. Hence, scalar multiplication on the quotient is well-defined.

8.4.10 Example. For any ring R and any ideal I in R , the quotient R^1/I is a cyclic R -module generated by $\pi(1_R)$. $\diamond$

8.4.11 Definition. For any R -linear map $\varphi: V \rightarrow W$, its *cokernel* is defined to be the quotient module $\text{Coker}(\varphi) := W/\text{Im}(\varphi)$.

8.4.12 Proposition. Let $\varphi: V \rightarrow W$ be an R -module homomorphism. For any submodule V' of V and any submodule W' of W satisfying the condition $\varphi(V') \subseteq W'$, the induced map $\bar{\varphi}: V/V' \rightarrow W/W'$ defined, for any v in V , by $\bar{\varphi}(v + V') := \varphi(v) + W'$ is R -linear.

As $v + U = u + U \Leftrightarrow v - u \in U$, we see that $rv - ru = r(v - u) \in U$ and $rv + U = ru + U$. Hence, scalar multiplication on the quotient is well-defined.

Proof. By Corollary 2.3.14, it suffices to verify that $\bar{\varphi}$ is compatible with scalar multiplication. For any r in R and any v in V , we have

$$\begin{aligned}\bar{\varphi}(r(v + V')) &= \bar{\varphi}(rv + V') = \varphi(rv) + W' \\ &= r\varphi(v) + W' = r(\varphi(v) + W') = r\bar{\varphi}(v + V').\end{aligned}\quad \square$$

8.4.13 First Isomorphism Theorem. Let $\varphi: V \rightarrow W$ be an R -module homomorphism with $K := \text{Ker}(\varphi)$. The induced map $\tilde{\varphi}: V/K \rightarrow \text{Im}(\varphi)$ defined, for any v in V , by $\tilde{\varphi}(v + K) = \varphi(v)$ is an R -module isomorphism.

Proof. By Theorem 3.0.1, it suffices to verify that $\tilde{\varphi}$ is compatible with scalar multiplication. For any r in R and any v in V , we have

$$\begin{aligned}\tilde{\varphi}(r(v + K)) &= \varphi(rv) + K = r\varphi(v) + K \\ &= r(\varphi(v) + K) = r\tilde{\varphi}(v + K).\end{aligned}\quad \square$$

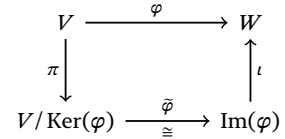


Figure 8.2: The commutative diagram for the First Isomorphism Theorem

8.4.14 Second Isomorphism Theorem. For any submodules U and W , there is an R -module isomorphism $(U + W)/W \xrightarrow{\cong} U/(U \cap W)$. $\square$

It suffices to verify that the group isomorphism in Theorem 3.0.4 is compatible with scalar multiplication.

8.4.15 Third Isomorphism Theorem. Let V be an R -module. For any submodules U and W of V satisfying $U \subseteq W$, there exists an R -module isomorphism $V/W \xrightarrow{\cong} (V/U)/(W/U)$. $\square$

It suffices to verify that the group isomorphism in Theorem 3.0.5 is compatible with scalar multiplication.

8.4.16 Correspondence Theorem. Let U be a submodule of the an R -module V . The canonical R -module homomorphism $\pi: V \rightarrow V/U$ induces a bijection between the set of all submodules of V containing U and the set of all submodules of V/U . $\square$

Compare with Theorem 3.0.6 and Theorem 8.4.16.

8.5 Exercises

8.5.1 Problem. A module is *simple* if it is not the zero module and if it has no proper submodule.

- i. Let V be a simple R -module. Show that V is cyclic.
- ii. Prove *Schur's Lemma*: If $\varphi : V \rightarrow W$ is a homomorphism between simple R -modules, then either φ is zero or an isomorphism.
- iii. Demonstrate that the set of endomorphisms, which are denoted by $\text{End}_R(V) := \text{Hom}_R(V, V)$, on a simple R -module V forms a field where multiplication is given by composition of functions and addition is defined pointwise.

8.5.2 Problem. Let R be domain and let V be an R -module. An element v in V is a *torsion element* if there is a nonzero element r in R such that $rv = 0$. Let $\tau(V)$ be the set of torsion elements of V . A module V is *torsion* if $\tau(V) = V$ and it is *torsion-free* if $\tau(V) = 0$.

- i. Show that $\tau(V)$ is a submodule of V .
- ii. Prove that $V/\tau(V)$ is torsion-free.
- iii. For any R -module homomorphism $\varphi : V \rightarrow W$, demonstrate that $\varphi(\tau(V)) \subseteq \tau(W)$.
- iv. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$ -module.

Bibliography

- Arnold, Vladimir I. 1998. *On teaching mathematics*, Russian Math. Surveys 53, no. 1, 229–236.
- Cayley, Arthur. 1854. *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$* , Phil. Mag. (4) 42, no. 7, 40–47.
- . 1893. *Note on the so-called quotient G/H in the theory of groups*, Amer. J. Math. 15, no. 4, 387–388.
- Cauchy, Augustin Louis. 1844. *Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*, Exercices d'analyse et de physique mathématique 3, 151–252.
- Chevalley, Claude. 1943. *On the theory of local rings*, Ann. of Math. (2) 44, 690–708.
- Cox, David A. 2011. *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first*, Amer. Math. Monthly 118, no. 1, 3–21.
- Dedekind, Richard. 1871. *Supplement X*, in *Vorlesungen über Zahlentheorie* by Peter Gustav Lejeune Dirichlet, Braunschweig: Vieweg.
- de Groot, Johannes. 1959. *Groups represented by homeomorphism groups*, Math. Ann. 138, 80–102.
- Dyck, Walther. 1882. *Gruppentheoretische Studien*, Math. Ann. 20, no. 1, 1–44.
- Eisenstein, Gotthold. 1850. *Über die Irreducibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39, 160–179.
- Frucht, Roberto. 1939. *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. 6, 239–250.
- Galois, Évariste. 1846. *Œuvres Mathématiques*, J. Math. Pures Appl. XI, 381–444.
- Granville, Andrew. 2024. *It is not "Bézout's identity"*. available at [arXiv:2406.15642](https://arxiv.org/abs/2406.15642) [math.HO].
- Hilbert, David. 1890. *Über die Theorie der algebraischen Formen*, Mathematische Annalen 36, 473–534.
- . 1897. *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4, no. I–XVIII, 175–546.
- Hodges, Wilfrid. 1979. *Krull implies Zorn*, J. London Math. Soc. (2) 19, no. 2, 285–287.
- Jordan, Camille. 1861. *Mémoire sur le nombre des valeurs des fonctions*, Journal de l'École polytechnique 22, 113–194.
- . 1870. *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris. 667 p.
- Klein, Felix. 1884. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig.
- Krull, Wolfgang. 1929. *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Math. Ann. 101, no. 1, 729–744.
- Lagrange, Joseph-Louis. 1771. *Suite des réflexions sur la résolution algébrique des équations. Section troisième. De la résolution des équations du cinquième degré & des degrés ultérieurs*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 5, no. 4, 138–254.
- . 1795. *Leçon Cinquième. Sur l'usage des courbes dans la solution des problèmes*, Leçons Élémentaires sur les Mathématiques. Republished in Serret, Joseph-Alfred, ed. (1877). *Oeuvres de Lagrange*. Vol. 7. Gauthier-Villars. pp. 271–287.
- Miller, George Abram. 1910. *On a method due to Galois*, The Quarterly Journal of Pure and Applied Mathematics 41, 382–384.
- Möbius, August F. 1832. *Über eine besondere Art von Umkehrung der Reihen*, J. Reine Angew. Math. 9, 105–123.
- Noether, Emmy. 1921. *Idealtheorie in Ringbereichen*, Math. Ann. 83, no. 1-2, 24–66.
- . 1927. *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96, no. 1, 26–61.
- Novikov, Pëtr Sergeevich. 1955. *Ob algoritmičeskoj nerazrešimosti problemy toždestva slov v teorii grupp*, Izdat. Akad. Nauk SSSR, Moscow. Trudy Mat. Inst. Steklov. no. 44.

- Poonen, Bjorn. 2019. *Why all rings should have a 1*, Math. Mag. 92, no. 1, 58–62.
- Sabidussi, Gert. 1960. *Graphs with given infinite group*, Monatsh. Math. 64, 64–67.
- Schönemann, Theodor. 1846. *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32, 93–105.
- Smith, Henry J. S. 1861. *On systems of linear indeterminate equations and congruences*, Philos. Trans. Roy. Soc. . 151, 293–32.
- Sylow, Ludwig. 1872. *Théorèmes sur les groupes de substitutions*, Math. Ann. 5, no. 4, 584–594.
- Waring, Edward. 1779. *Problems concerning interpolations*, Philosophical Transactions of the Royal Society 69, 59–67.
- Wielandt, Helmut. 1959. *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. 10, no. 1, 401–402.
- Zorn, Max. 1935. *A remark on method in transfinite algebra*, Bull. Amer. Math. Soc. 41, no. 10, 667–670.