Artin: Rings

James Pagan

February 2024

Contents

1 Rings

1.1 Ring Axioms

A **ring** R is a set endowed with two binary operations, here denoted "+" and "×", such that if $a, b, c \in R$, the following ten axioms are satisfied:

- **Additive Axioms**
  1. **Closure**: $a + b \in R$.
  2. **Associativity**: $a + (b + c) = (a + b) + c$.
  3. **Identity**: There is $0 \in R$ such that $a + 0 = 0 + a = a$.
  4. **Invertability**: There is $-a \in R$ such that $a + (-a) = (-a) + a = 0$.
  5. **Commutativity**: $a + b = b + a$.
- **Multiplicative Axioms**
  6. **Closure**: $ab \in R$.
  7. **Associativity**: $a(bc) = (ab)c$.
  8. **Identity**: There is $1 \in R$ such that $a1 = 1a = a$.
- **Distributive Axioms**
  9. **Left Distributivity**: $a(b + c) = ab + ac$.
  10. **Right Distributivity**: $(a + b)c = ac + bc$.

Since $(R, +)$ is an Abelian group, the following properties hold for $a, b \in R$: the additive identity 0 is unique, the additive inverse $-a$ is unique, $-(-a) = a$, and $-(a + b) = -a - b$.

Theorem 1. *The following properties hold for any ring R and $a, b \in R$:*

1. *1 is the unique multiplicative inverse of R.*
2. *If a has a multiplicative inverse a^{-1}, it is unique.*
3. $a0 = 0a = a$.
4. $-a = (-1)a$.
5. $a(-b) = (-a)b = -ab$.
6. $(-a)(-b) = ab$.

Proof. (1) and (2) follow from the monoid/group axioms. For the rest:

3. As $0 + 0 = 0$, we have that $a0 = a(0 + 0) = a0 + a0$; subtracting by $a0$ yields $a0 = 0$. Similarly, $0a = 0$.
4. We have that

$$(-1)a + a = (-1)a + 1a = (-1 + 1)a = 0a = 0,$$

   so $(-1)a = -a$.
5. See that

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

   so $a(-b) = -ab$. Similarly, $(-a)b = -ab$.
6. Using (5), we find that

$$(-a)(-b) = -(a)(-b) = -(-ab) = ab,$$

   as desired.

This yields the desired six properties. □

1.2 Subrings and Ideals

A **subring** R' of R is a subset of R that is also a ring. This relation is denoted $R' \subseteq R$.

Theorem 2. *A subset R' of R is a subring if it is nonempty, closed under addition and multiplication, contains additive inverses, and contains the multiplicative identity.*

Proof. The conditions that $(R', +)$ is nonempty, closed, and contains inverses ensures that it is a group. Note that $(R', \times)$ is closed and contains the multiplicative identity.

The final properties are implied by the fact R' is a subset of R; all the elements of R' satisfy both associative and distributive laws, plus additive commutativity. We deduce that R' is a subring. □

All rings contain at least two subrings: the 0 ring and R itself.

A **ideal** $\mathfrak{a}$ of R is a subset of R that satisfies the following twokproperties:

1. **Additive**: $\mathfrak{a}$ is an additive subgroup of R.
2. **Multiplicative**: For all $a \in \mathfrak{a}$ and $x \in R$, we have $ax, xa \in \mathfrak{a}$.

All rings contain at least two ideals: one is R itself, one is a maximal ideal (Section 2.3).

Theorem 3. *If R' is both a subring and an ideal of R if and only if R' is R or 0.*

Proof. Suppose that $R' \neq 0$ is both a subring and an ideal of R. As R' is a subring, $1 \in R'$; as R' is an ideal, $a = a1 \in R'$ for all $a \in R$. Then $R' = R$. Clearly, R itself and 0 are both ideals and subrings — which yields the desired result. □

1.3 Ring Homomorphisms

A **ring homomorphism** between two rings R and R' is a mapping $\phi : R \to R'$ such that for all $a, b \in R$,

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \\ \phi(1) &= 1. \end{aligned}$$

By the group axioms, $\phi(-a) = -\phi(a)$ and $\phi(0) = 0$ for all $a \in R$. If a has a multiplicative inverse a^{-1}, then $\phi(a^{-1}) = \phi(a)^{-1}$.

The **image** of R under ϕ is the set $\{\phi(a) \mid a \in R\}$, and is denoted $\phi(R)$.

Theorem 4. *The image of any ring homomorphism $\phi : R \to R'$ is a subring of R'.*

Proof. Realize that $\phi(R)$ is nonempty, and for all $\phi(a), \phi(b) \in \phi(R)$, we have that

1. $\phi(a) + \phi(b) = \phi(ab) \in \phi(R)$.
2. $\phi(a)\phi(b) = \phi(ab) \in \phi(R)$.
3. $-\phi(a) = \phi(-a) \in \phi(R)$.
4. $\phi(1) \in R$.

Hence, $\phi(R)$ is a subring of R'. □

The **kernel** of R under ϕ is the set $\{a \in R \mid \phi(r) = 0\}$ and is denoted $\operatorname{Ker}\phi$.

Theorem 5. $\operatorname{Ker}\phi$ *is an ideal of* R*.*

Proof. Since ϕ is a homomorphism of the Abelian groups $(R, +)$ and $(R', +)$, the kernel of ϕ is an Abelian group with respect to addition. We need only verify the multiplicative condition; for all $a \in R$ and $k \in \operatorname{Ker}\phi$,

$$\phi(ak) = \phi(a)\phi(k) = 0\phi(a) = 0 = \phi(a)0 = \phi(a)\phi(k) = \phi(ak).$$

Then $ak \in \operatorname{Ker}\phi$. Thus, $\operatorname{Ker}\phi$ is an ideal. □

Categories of group homomorphisms — like monomorphisms, epimorphisms, isomorphisms, endomorphisms, automorphisms — have equivalent formulations for ring homomorphisms. An isomorphism between R and R' is denoted the same as groups:

$$R \cong R'.$$

We can extend the notion of a quotient group to a ring R with an ideal $\mathfrak{a}$ as follows, yielding a **quotient ideal**:

Theorem 6. *The quotient group* $R\,/\,\mathfrak{a}$ *is a ring under the product* $(a+\mathfrak{a})(b+\mathfrak{a}) = ab+\mathfrak{a}$ *for* $a, b \in R$*.*

Proof. The quotient group $R\,/\,\mathfrak{a}$ exists, since $\mathfrak{a}$ is an additive subgroup of R and all subgroups of Abelian groups are normal. We must demonstrate that the product is well-defined.

Suppose $a + \mathfrak{a} = a' + \mathfrak{a}$ and $b + \mathfrak{a} = b' + \mathfrak{a}$. Then since $a - a' \in \mathfrak{a}$ and $b - b' \in \mathfrak{a}$,

$$ab - a'b \in \mathfrak{a} \qquad \text{and} \qquad a'b - a'b' \in \mathfrak{a}.$$

Thus, $ab - a'b' \in \mathfrak{a}$ and $ab + \mathfrak{a} = a'b' + \mathfrak{a}$. Then the product is well-defined. Proving that the product is closed and associative is trivial; the multiplicative identity of $R\,/\,\mathfrak{a}$ is $1 + \mathfrak{a}$, and the distributivity with addition is trivial — so $R\,/\,\mathfrak{a}$ is a ring. □

The canonical mapping $\phi : R \to R\,/\,\mathfrak{a}$ is thus a surjective homomomorphism with kernel $\mathfrak{a}$. A similar definition exists for the quotient of two ideals — say, $\mathfrak{a}\,/\,\mathfrak{b}$ for $\mathfrak{a} \supseteq \mathfrak{b}$.

1.4 Isomorphism Theorems

All three Isomorphism Theorems and the Correspondence Theorem have their equivalencies for rings.

Theorem 7 (First Isomorphism Theorem)**.** *For all homomorphisms $\phi : R \to R'$ with kernel $\mathfrak{k}$,*

$$R \,/\, \mathfrak{k} \cong \phi(R)$$

by the mapping $\psi(a + \mathfrak{k}) = \phi(a)$.

Proof. We must first demonstrate that ψ is a homomorphism. If $a, b \in R$, then the following three identities hold:

1. $\psi(a + b + \mathfrak{k}) = \phi(a + b) = \phi(a) + \phi(b) = \psi(a + \mathfrak{k}) + \psi(b + \mathfrak{k})$.
2. $\psi(ab + \mathfrak{k}) = \phi(ab) = \phi(a)\phi(b) = \psi(a + \mathfrak{k})\psi(b + \mathfrak{k})$.
3. $\psi(1 + \mathfrak{k}) = \phi(1)$.

Thus, ψ is a homomorphism. For all $\phi(a) \in \phi(R)$, realize that $\psi(a + \mathfrak{k}) = \phi(a)$; thus ψ is surjective. Finally, let $\psi(a + \mathfrak{k}) = \psi(b + \mathfrak{k})$; then $\phi(a) = \phi(b)$, so

$$\phi(a - b) = \phi(a) - \phi(b) = 0.$$

Hence, $a - b \in \mathfrak{k}$ and $a + \mathfrak{k} = b + \mathfrak{k}$. We conclude that ψ is injective, implying the desired isomorphism. □

The Correspondence Theorem expands upon the result of the First Isomorphism Theorem.

Theorem 8 (Correspondence Theorem)**.** *There is a one-to-one correspondence between ideals of $\phi(R)$ and ideals of R that contain $\mathfrak{k}$.*

Proof. For an ideal $\mathfrak{a}'$ of $\phi(R)$, define $\mathfrak{a} = \{a \in R \mid \phi(a) \in \mathfrak{a}'\}$. By the Correspondence Theorem for groups, $\mathfrak{a}$ is an additive subgroup of R. For all $a \in \mathfrak{a}$ and $b \in R$, we have $\phi(a) \in \mathfrak{a}'$; thus

$$\phi(ab) = \phi(a)\phi(b) \in \mathfrak{a}'$$

since $\mathfrak{a}'$ is an ideal. Thus $ab \in \mathfrak{a}$, so $\mathfrak{a}$ is an ideal of R. Since $0 \in R'$, we have that $\mathfrak{k}$ is a subideal of $\mathfrak{a}$. It is now relatively trivial to establish a one-to-one correspondence. □

Corollary 1. *There is a one-to-one correspondence between ideals of $R \,/\, \mathfrak{a}$ and ideals of R that contain $\mathfrak{a}$.*

The two remaining Isomorphism Theorems will be proven at another time.

1.5 Assorted Rings

We will consider the following three types of rings in this section:

1. A **commutative ring** is a ring R such that $ab = ba$ for all $a, b \in R$.

2. An **integral domain** is a nonzero commutative ring R such that $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in R$.

3. A **field** is a commutative division ring.

Note that integral domains and fields must be nonzero. **Henceforth, all rings we shall define are commutative unless stated otherwise.**

Theorem 9. *All finite domains are fields.*

Proof. Let R be a finite domain. Then for nonzero $a \in R$, consider the set

$$\{a, a^2, \ldots, a^{|R|+1}\}.$$

By the Pigeonhole Principle, two elements of this set must be equal: $a^i = a^j$ for $i, j \in \{1, \ldots, n\}$ with $i < j$. Thus $a^j(a^{i-j} - 1) = 0$, so $a^{i-j} = 1$ and $a^{i-j-1} = a^{-1}$. Since all nonzero elements of R are invertible, we conclude that R is a field. $\square$

Theorem 10. *R is a field if and only if the only ideals of R are 0 and R itself.*

Proof. Let R be a field and let $\mathfrak{a}$ be nonzero ideal of R. Then for $a \in \mathfrak{a}$,

$$R = (a) \subseteq \mathfrak{a} \subseteq R.$$

Thus, $\mathfrak{a} = R$. Now, suppose that the only ideals of R are 0 and R itself; then for all nonzero $a \in R$,

$$(a) = R,$$

where (a) denotes the principal ideal (Section 2.1). Thus, there exists $a^{-1} \in R$ such that $aa^{-1} = 1$, so R is a field. $\square$

An element $a \in R$ is a **unit** if it is invertible. It is trivial to verify that all the units of R constitute a multiplicative Abelian group (non-units form a commutative semigroup!)

2 Miscellaneous Artin Shenanigans

Polynomial Rings

Let R be a ring. The **polynomial ring** $R[x_1, \ldots, x_n]$ denotes the ring of all polynomials with variables $x_1, \ldots, x_n$ and coefficents in R.

Theorem 11. *Suppose R is a ring, and let $f, g \in R[x]$ such that the leading coefficent of g is a unit. Then there exists $q, r \in R[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

with $\deg r < \deg g$.

Corollary 2. *If F is a field, then $F[x]$ is a Euclidean domain.*

If R is a Unique Factorization Domain, then so is $R[x]$. The Remainder Theorm holds in a general ring: the remainder dividing $f(x)$ by $(x - \alpha)$ is $f(\alpha)$.

Homomorphisms and Ideals

Theorem 12 (Substitution Principle)**.** *Let $\phi : R \to R'$ be a homomorphism, and select $\alpha_1, \ldots, \alpha_n \in R'$ arbitrarily. Then there exists a unique homomorphism*

$$\Phi : R[x_1, \ldots, x_n] \to R'$$

that agrees with ϕ on constant polynomials and sends x_i to α_i.

Proof. Defining Φ as the map which sends 1 to 1 and x_i to α_i, it is easy to show that Φ is a homomorphism. The unqiueness of Φ follows from the fact these elements generate the totality of $R[x_1, \ldots, x_i]$, hence its image is unique. □

The next theorem illustrates the use of the Substitution Principle:

Theorem 13. *Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$ be sets of variables. Then $R[x, y] \cong R[x][y]$ which sends the variables to themselves.*

Proof. Let $\phi : R \to R[x][y]$ be an embedding. The Substitution Principle guarantees that there exists a homomorphism $\Phi : R[x, y] \to R[x][y]$ by mapping each variable to itself. To demonstrate that Φ is bijective, we may simply demonstrate an inverse. □

Theorem 14. *Let R be a ring. There exists a unique homomorphism $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = 1 + \cdots + 1$, added n times, and $\phi(-n) = -\phi(n)$.*

The proof of the above assertion is relatively trivial. Here are some neat fun facts:

Theorem 15. *Any homomorphism $\phi : F \to R$ is injective.*

Proof. The kernel of ϕ is an ideal of F. It cannot be F itself, since ϕ must map 1 to 1; thus $\operatorname{Ker} \phi = 0$, so ϕ is injective. □

The next result concerns adjoining elements:

Theorem 16. *Suppose the leading coefficent of $f \in R[x]$ is a unit. Then $R[x] \,/\, (f)$ contains constants and polynomials of degree strictly less than f.*

Product Rings

In the following theorem, let R be a ring with ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$; define a homomorphism

$$\phi : R \to \prod_{i=1}^{n} R \,/\, \mathfrak{a}_i$$

by $\phi(a) = (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$.

Theorem 17. *The following two properties of ϕ hold:*

1. *ϕ is injective if and only if $\cap \mathfrak{a}_i = 0$.*
2. *ϕ is surjective if and only if $\mathfrak{a}_i$ and $\mathfrak{a}_\mathfrak{i}$ are relatively prime whenever $i \neq j$.*

Proof. For (1), the following sequence of claims is easy to verify:

$$\begin{aligned} k \in \operatorname{Ker} \phi &\iff \phi(k) = 0 \\ &\iff k \in \mathfrak{a}_i \text{ for each } i \in \{1, \ldots, n\} \\ &\iff k \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n. \end{aligned}$$

Thus, $\operatorname{Ker} f = 0$ if and only if $\cap \mathfrak{a}_i = 0$. Now for (2): suppose that ϕ is surjective. For $\mathfrak{a}_i$ and $\mathfrak{a}_j$, there exists $a \in R$ such that $\phi(a)$ returns $(\ldots, 0, 1, 0, \ldots)$, where 1 is in the i-th place. Then $a - 1 \in \mathfrak{a}_i$ and $a \in \mathfrak{a}_j$, so

$$1 = (1 - a) + a \in (\mathfrak{a}_i + \mathfrak{a}_j),$$

so $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are relatively prime. Now, suppose that $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are relatively prime for each $i \neq j$. We need only show that the element $(\ldots, 0, 1, 0, \ldots)$ lies in the image of ϕ; the 1 may be anywhere by similarity, so we can generate all elements of $\prod R / \mathfrak{a}_i$.

For each $i \in \{1, \ldots, n\}$, we have $\mathfrak{a}_i$ and $\prod_{j \neq i} \mathfrak{a}_j$ are coprime; thus there exists a_i in the former and a in the latter such that

$$a_i + a = 1.$$

Thus, $a \in (1 + \mathfrak{a}_i)$. We conclude that $\phi(a) = (\ldots, 0, 1, 0, \ldots,)$, from which we construct as aforementioned and demonstrate the surjectivity of ϕ. $\square$

In other words, one can express R is a direct product if relatively prime, mutually exclusive ideals may be located.

Theorem 18. *Let $e \in R$ be idempotent. Then $e' = 1 - e$ is idempotent, $e' + e = 1$, and $ee' = 0$.*

The proof of the above is trivial. It is easy to deduce that (e) is a ring with identity e; it is *not* a subring unless $e = 1$. Thus we can demonstrate that $R \cong (e) \times (e')$.

Artin describes the process by which fields of fractions may be constructed. We leave such technical machinery out of this document; I have already proven that $S^{-1}R$ is a ring of fractions.

Maximal Ideals

In the interest of time, I will not prove Krull's Theorem here. It is clear that the maximal ideals of $\mathbb{Z}$ are (p) for prime p. The following theorem is relatively easy to observe:

Theorem 19. *Let $R[x]$ be a Principal Ideal Domain. Then the maximal ideals of $R[x]$ are precisely the ideals generated by monic irreducible polynomials.*

Since the irreducible polynomials in $\mathbb{C}[x]$ are $(x - \alpha)$ for $\alpha \in \mathbb{C}$, there is a bijection between maximal ideals in $\mathbb{C}[x]$ and points in $\mathbb{C}$.

Theorem 20 (Weak Nullstellensatz)**.** *There exists a bijection between maximal ideals of* $\mathbb{C}[x_1, \ldots, x_n]$ *and points in* $\mathbb{C}^n$*.*

Proof. Select $(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ abitrarily. We may use the substitution map from $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$ defined by $x_1 \to \alpha_1$; it is easy to prove that the map is surjective, so its kernel is a maximal ideal.

It is harder to prove that all maximal ideals are the kernel of such a map. We ommmit the proof from here in the interest of brevity. $\square$