

Artin: Factoring

James Pagan

February 2024

Contents

| | | |
|----------|---|----------|
| 1 | Unique Factorization Domains | 2 |
| 1.1 | Terminology | 2 |
| 1.2 | Definition | 3 |
| 2 | Principal Ideal Domains | 3 |
| 2.1 | Definition | 3 |
| 2.2 | Relation with Unique Factorization Domains | 4 |
| 2.3 | Greatest Common Divisor | 5 |
| 3 | Euclidean Domain | 6 |
| 3.1 | Definition | 6 |
| 3.2 | Relation with Principal Ideal Domains | 6 |
| 4 | The Polynomial Ring $\mathbb{Z}[x]$ | 7 |
| 4.1 | Primitive Polynomials | 7 |
| 5 | The Gaussian Integers $\mathbb{Z}[i]$ | 8 |
| 5.1 | A Euclidean Domain | 8 |
| 5.2 | Gaussian Primes | 9 |
| 5.3 | Sums of Two Squares | 11 |

1 Unique Factorization Domains

1.1 Terminology

Let R be an integral domain. Before we introduce unique factorization domains, we must define several terms for $a, b \in R$:

1. a **divides** b if $(b) \subseteq (a)$.
2. a is a **proper divisor** of b if $(b) \subset (a) \subset R$.
3. a and b are **associates** if $(a) = (b)$.
4. a is **irreducible** if $(a) \subset R$ and there is no principal ideal (c) such that $(a) \subset (c) \subset R$.
5. p is a **prime element** if $p \neq 0$ and (p) is prime.

These may be equivalently expressed ideal-free (AbstractAlgebra/homework3.tex):

1. a **divides** b if $b = aq$ for some $q \in R$.
2. a is a **proper divisor** of b if $b = aq$ and neither a nor q is a unit.
3. a and b are **associates** if each divides the other — that is, $b = ua$ for some unit u .
4. a is **irreducible** if it has no proper divisors — its only divisors are units and associates.
5. p is a **prime element** if $p \neq 0$ and p divides ab implies p divides a or p divides b .

A **size function** is a mapping $\sigma : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$.

Theorem 1. *Let R be an integral domain. Then all prime elements of R are irreducible.*

Proof. Suppose that p is prime and that $(p) \subseteq (c) \subset R$. Hence there exists x such that $p = cx$, so $cx \in (p)$. We have two possibilities: $c \in (p)$ or $x \in (p)$.

Suppose for contradiction that $x \in (p)$. Then $x = py$ for some y — substituting into the above equality yields

$$p = c(py) \implies p(1 - cy) = 0.$$

Since $p \neq 0$, we have $1 = cy$ — hence c is a unit and $(c) = R$, a contradiction. We must have $c \in (p)$, so $(c) = (p)$. We conclude that (p) is irreducible. \square

1.2 Definition

A **unique factorization domain** R is an integral domain if for every nonzero $x \in R$, there exists a unit u and irreducible elements p_1, \dots, p_n such that

$$x = up_1 \cdots p_n,$$

and this factorization is unique in the following sense: if there exists a second factorization

$$x = wq_1 \cdots q_m,$$

then $n = m$ and there exists a bijection such that $(p_i) = (q_j)$ for each paired i, j (that is, p_i and q_j associate).

Theorem 2. *Every irreducible element in a unique factorization domain is prime.*

Proof. Suppose that (p) is not prime — then there exist $a, b \notin (p)$ such that $ab \in (p)$. Thus we have $(p) \subset (a)$. Since a is a nonunit, $(a) \subset R$, so

$$(p) \subset (a) \subset R.$$

Hence (p) is not irreducible. Taking the contrapositive yields the desired result. \square

Hence, we could equivalently define unique factorization as decomposition to *prime* elements. In this sense, factorization in R “terminates” if and only if R satisfies the ascending chain condition for principal ideals; namely, the chain

$$x \subseteq \bigcap_{i=1}^{\infty} (p_i) \subseteq \bigcap_{i=2}^{\infty} (p_i) \subseteq \bigcap_{i=3}^{\infty} (p_i) \subseteq \cdots$$

is stationary. This is the terminology favored by Artin.

2 Principal Ideal Domains

2.1 Definition

A **principal ideal domain** is an integral domain in which all ideals are principal. It is clear that all such domains are Noetherian.

Theorem 3. *Let R be a principal ideal domain. Then all nonzero prime ideals of R are maximal.*

Proof. Let (p) be a prime ideal contained in the maximal ideal (m) . Supposing for contradiction that

$$(p) \subset (m) \subset R,$$

we obtain that (p) is not irreducible, which contradicts Theorem 1. Hence $(p) = (m)$, so (p) is maximal. \square

Four helpful facts about principal ideal domains are as follows:

1. If $\mathfrak{a}_1 = (a_1)$ and $\mathfrak{a}_2 = (a_2)$ are principal ideals, then $\mathfrak{a}_1\mathfrak{a}_2 = (a_1a_2)$. This holds in any commutative ring.
2. Prime ideals cannot contain other prime ideals: if $(p_1) \subset (p_2)$ are prime, then the fact

$$(p_1) \subset (p_2) \subset R$$

implies that (p_1) is not irreducible — a contradiction.

3. All prime ideals are relatively prime. This is because if (p_1) and (p_2) are prime, we have

$$(p_1) \subseteq (p_1) + (p_2) \subseteq R$$

We cannot have $(p_1) = (p_1) + (p_2)$ by Fact 2; thus since (p_1) is irreducible, we conclude that $(p_1) + (p_2) = R$.

4. If $(p_1), \dots, (p_n)$ are prime ideals, then

$$(p_1) \cap \dots \cap (p_n) = (p_1) \times \dots \times (p_n) = (p_1 \cdots p_n).$$

2.2 Relation with Unique Factorization Domains

Theorem 4. *All principal ideal domains are unique factorization domains.*

Proof. Let R be a principal ideal domain and select $x \in R$. Then since R is Noetherian, factoring terminates: each ascending chain of principal ideals is stationary.

Let $(p_1), \dots, (p_n)$ be the prime ideals which contain x . By Fact 4, we deduce that $x \in (p_1p_2 \cdots p_n)$. Thus we can write x in the form

$$x = u_1p_1 \cdots p_n.$$

If u_1 is contained in prime ideals, then they must be among $(p_1), \dots, (p_n)$. Hence we can express u_1 as a product of some p_1, \dots, p_n times u_2 . Repeating ad nauseam, we obtain a sequence u_1, u_2, \dots which yields the stationary chain

$$(x) \subseteq (u_1) \subseteq (u_2) \subseteq \dots.$$

Hence there must exist $n \in \mathbb{Z}_{>0}$ such that $(u_n) = (u_{n+1}) = \dots$. Thus we have $u_n = u \cdot u_{n+1}$ for some unit u . Recursive substitution into our expression for x yields

$$x = up_1^{e_1} \cdots p_n^{e_n},$$

which completes the existence portion of the proof. As per uniqueness, suppose that

$$up_1 \cdots p_n = x = wq_1 \cdots q_m$$

A quick induction on $\max\{m, n\}$ yields that since two primes on either side must be adjoints, we can divide and yield a number which factors uniquely. This completes the proof. \square

2.3 Greatest Common Divisor

Let R be an integral domain, and select $a, b \in R$. A **greatest common divisor** of a and b is an element $d \in R$ such that:

1. $d \mid a$ and $d \mid b$.
2. $c \mid a$ and $c \mid b$ implies $c \mid d$.

It is clear that GCDs are unique up to association by Condition 2 — thus we can speak of *the* GCD. If the only greatest common divisors of a and b are units, we set $\gcd(a, b) = 1$ and call a, b **relatively prime**.

Theorem 5. *Suppose R is a principal ideal domain. Then the generator of the ideal (a, b) is the greatest common divisor of a, b .*

Proof. It is clear that $a, b \in (d)$ implies $d \mid a$ and $d \mid b$. We need only demonstrate the second condition. Thus, suppose $c \mid a$ and $c \mid b$ — hence $(a) \subseteq (c)$ and $(b) \subseteq (c)$. Thus

$$(d) = (a) + (b) \subseteq (c),$$

so $c \mid d$. We conclude that $\gcd(a, b) = d$. \square

It is now easy to demonstrate that $\gcd(a_1, a_2, \dots, a_n) = \gcd(a_1, \gcd(a_2, \dots, a_n))$. This yields the following lemma:

Lemma 1 (Bézout's Identity). *If R is a principal ideal domain and $\gcd(a_1, \dots, a_n) = d$, there exist integers b_1, \dots, b_n such that $d = a_1b_1 + \dots + a_nb_n$.*

Much simpler than the proof in your 2nd Contest Math Notebook, right?

3 Euclidean Domain

3.1 Definition

An integral domain R is a **Euclidean domain** if there exists a size function σ such that $a \in R$ and *nonzero* $b \in R$ implies the existence of $q, r \in R$ such that $a = bq + r$, where $\sigma(r) < \sigma(b)$. It is clear that \mathbb{Z} is a Euclidean domain.

Theorem 6. *All fields are Euclidean domains.*

Proof. Let R be a field, and select $a, b \in F$. Then

$$a = b \left(\frac{a}{b} \right) + 0.$$

If σ is an arbitrary size function on R , then the caveat of remainder zero ensures that the above equations dictate a valid Euclidean division. \square

For a field F , the ring $F[x]$ is a Euclidean domain. I proved this in my contest algebra notes.

3.2 Relation with Principal Ideal Domains

Theorem 7. *All Euclidean domains are principal ideal domains.*

Proof. Let R be a Euclidean domain with size function σ and let $\mathfrak{a} \subseteq R$ be an ideal. If $\mathfrak{a} = 0$, then \mathfrak{a} is principal; otherwise, the Well-Ordering Theorem guarantees that there exists a nonzero element $a \in \mathfrak{a}$ of minimal size.

Let $b \in \mathfrak{a}$. Then there exist $q, r \in R$ such that

$$b = aq + r,$$

where $\sigma(r) < \sigma(a)$. Since a is minimal, we must have $r = 0$, in which case $b \in (a)$. We conclude that $\mathfrak{a} = (a)$, so all ideals of R are principal. \square

Corollary 1. *All ideals in a Euclidean domain are generated by the element of smallest size.*

We have thus attained a sequence of types of rings:

$$\text{rings} \subseteq \text{commutative rings} \subseteq \text{integral domains} \subseteq \text{UFDs} \subseteq \text{PIDs} \subseteq \text{EDs} \subseteq \text{fields}.$$

4 The Polynomial Ring $\mathbb{Z}[x]$

We have proved the following facts about polynomial rings: for any field F ,

1. $F[x]$ is a Euclidean domain.
2. $F[x_1, \dots, x_n]$ is a unique factorization domain and Noetherian.

Polynomial rings over arbitrary commutative rings obey significantly fewer restrictions. This section characterizes the polynomial ring $\mathbb{Z}[x]$. There are two main tools in its study: first is the embedding

$$\mathbb{Z}[x] \subset \mathbb{Z}[x],$$

and second is reduction modulo some prime p : the mappings $\psi : \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$.

4.1 Primitive Polynomials

The following lemma is quite obvious:

Lemma 2. *Let $f(x) = a_n x^n + \dots + a_0$ have integer coefficients. Then the following are equivalent:*

1. p divides each a_i .
2. p divides f in $\mathbb{Z}[x]$
3. f lies in the kernel of ψ_p .

A polynomial $f \in \mathbb{Z}[x]$ is called **primitive** if the GCD of its coefficients is 1.

Lemma 3. *Let $f(x) = a_n x^n + \dots + a_0$ have integer coefficients. Then the following are equivalent:*

1. f is primitive.
2. f is not divisible by any prime p .
3. $\psi_p(f) \neq 0$ for all primes p .

Observe that an integer $n \in \mathbb{Z}[x]$ is a prime element if and only if it is prime. Thus $fg \in (p)$ implies that $f \in (p)$ or $g \in (p)$: stated differently, $p \mid fg$ implies $p \mid f$ or $p \mid g$.

Lemma 4 (Gauss' Lemma). *The product of primitive polynomials is primitive.*

Proof. Suppose that fg is not primitive; then $p \mid fg$ for some prime integer p . Thus $p \mid f$ or $p \mid g$, so one of f and g must not be primitive. Taking the contrapositive yields the desired result. \square

That would be an insanely long number theory problem, in terms of a crazy sequence of equations — and yet it falls so elegantly to the properties of prime ideals!

5 The Gaussian Integers $\mathbb{Z}[i]$

Since $\mathbb{Z}[i]$ is isomorphic to $\mathbb{Z}[x] / (x^2 + 1)$, we can use tools from polynomial rings to study Gaussian integers.

5.1 A Euclidean Domain

Theorem 8. $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. Using the norm $\|a + bi\| = a^2 + b^2$, we will divide $a + bi$ by $c + di$. It is easy to deduce that there exist rationals r, s such that

$$\frac{a + bi}{c + di} = r + si.$$

Approximate r and s by integers: namely define $n, m \in \mathbb{Z}$ such that $|r - n| \leq \frac{1}{2}$ and $|s - m| \leq \frac{1}{2}$. Then we can express the above as

$$r + si = (n + mi) + (r - n) + i(s - m).$$

Expanding this out, we obtain a rather messy equation:

$$a + bi = (n + ni)(c + di) + ((r - n) + i(s - m))(c + di).$$

All that remains to be proven is that the right-most term has a norm less than $c + di$, which is equivalent to showing that $(r - n) + i(s - m)$ has a norm less than one:

$$\|(r - n) + i(s - m)\| = (r - n)^2 + (s - m)^2 \leq \frac{1}{4} + \frac{1}{4} < 1.$$

This completes the proof. □

5.2 Gaussian Primes

An irreducible element in $\mathbb{Z}[i]$ is called a **Gaussian prime**. It is clear that π is a Gaussian prime if and only if $\bar{\pi}$ is a Gaussian prime.

Theorem 9. *Let π be a Gaussian prime. Then $\pi \cdot \bar{\pi}$ is either a prime integer or the square of a prime integer.*

Proof. Let the integer $\pi \cdot \bar{\pi}$ have prime factorization $p_1 \dots p_n$; further factor each p_i under the Gaussian integers. This will generate n or more Gaussian primes; thus n is at most two. If $n = 1$, then $\pi \cdot \bar{\pi}$ is a prime integer.

Suppose that $n = 2$, and $p_1 p_2$ factors in $\mathbb{Z}[i]$ as $\pi \cdot \bar{\pi}$. Then p_1 divides one of π or $\bar{\pi}$; hence $\bar{p}_1 = p_1$ divides the other, so $p_1^2 \mid \pi \cdot \bar{\pi}$. We conclude that $p_1 = p_2$. □

The following theorem characterizes the reverse direction:

Theorem 10. *Let p be a prime integer. Then p is either a Gaussian prime or factors as $\pi \cdot \bar{\pi}$ for some Gaussian prime π .*

Proof. Suppose that p is not a Gaussian prime, and let $p = \pi z$ for some Gaussian prime π and Gaussian integer z . It is clear that $z = n\bar{\pi}$ for some $n \in \mathbb{Z}$; we must have $n = 1$ so that p is prime. Hence $p = \pi \cdot \bar{\pi}$. □

The following two theorems prepare for the debut of Fermat's Two-Square Theorem.

Theorem 11. *Let p be a prime integer. Then the following are equivalent:*

1. p is a Gaussian prime.
2. $\mathbb{Z}[i] / (p)$ is a field.
3. $x^2 + 1$ is irreducible in $\mathbb{Z}_p[x]$.

Proof. From the properties of Euclidean domains, it is clear that

$$p \text{ is a Gaussian prime} \iff (p) \text{ is maximal} \iff \mathbb{Z}[i]/(p) \text{ is a field.}$$

Thus (1) and (2) are equivalent. For the equivalency of (2) and (3), we have

$$\begin{aligned} \mathbb{Z}[i]/(p) \text{ is a field} &\iff (\mathbb{Z}[x]/(x^2 + 1))/(p) \text{ is a field} \\ &\iff \mathbb{Z}_p[x]/(x^2 + 1) \text{ is a field} \\ &\iff (x^2 + 1) \text{ is maximal in } \mathbb{Z}_p[x] \\ &\iff x^2 + 1 \text{ is irreducible in } \mathbb{Z}_p[x]. \end{aligned}$$

The last equivalency follows from the fact that \mathbb{Z}_p is a field, so $\mathbb{Z}_p[x]$ is a Euclidean Domain. \square

The following result belongs to classical number theory, enlightened by Abstract Algebra:

Theorem 12. *Let p be an odd prime. Then the following two facts hold:*

1. \mathbb{Z}_p^\times contains an element of order 4 if and only if $p \equiv 1 \pmod{4}$.
2. $x \in \mathbb{Z}_p$ has order 4 if and only if $x^2 \equiv -1 \pmod{p}$.

Proof. We start with (1). Since \mathbb{Z}_p is a finite field, $\mathbb{Z}_p^\times \cong C_{p-1}$. Thus \mathbb{Z}_p^\times has an element of order 4 if and only if $4 \mid p-1$, which entails $p \equiv 1 \pmod{4}$.

For (2), suppose $x \in \mathbb{Z}_p$ has order 4. Then

$$(x^2 + 1)(x^2 - 1) = x^4 - 1 = 0.$$

Since $\mathbb{Z}_p[x]$ is a Euclidean domain, one of these polynomials must be 0; since x does not have order 2, we deduce $x^2 + 1 = 0$. The reverse direction is easy to prove. \square

The following theorem is the culmination of this entire section:

Theorem 13 (Fermat's Two-Square Theorem). *Let p be a prime integer. Then the following are equivalent:*

1. p is the product of complex conjugate Gaussian primes.
2. $p = 2$ or p is congruent to 1 modulo 4.
3. p is a sum of two integer squares.
4. -1 is a quadratic residue modulo p .

Proof. It is easy to see that (1) and (3) are equivalent. The equivalence of (2) and (4) is established by Theorem 12.

Suppose (3), observe that the squares modulo 4 are 0 and 1; therefore, $p = a^2 + b^2$ must be 0, 1, or 2 modulo 4. Hence p is either $2 = 1^2 + 1^2$ or a prime congruent to 1 (mod 4), which is (2).

Suppose (4). Define x such that $x^2 \equiv -1 \pmod{p}$. Then $x^4 \equiv 1 \pmod{p}$, so the polynomial $x^4 + 1$ is reducible in the Euclidean domain $\mathbb{Z}_p[x]$. By the converse of Theorem 11, p cannot be a Gauss prime — hence by Theorem 10, it is the product of a Gauss prime and its conjugate. This entails (1).

We conclude that (1), (2), (3), and (4) are equivalent conditions. \square

This stunning and challenging theorem falls elegantly to the mechanics of Abstract Algebra. Isn't that fucking amazing?

5.3 Sums of Two Squares

The following content is not in Artin, but it answers a classical theorem from Number Theory:

Theorem 14. *Let $n = 2^m p_1^{e_1} \cdots p_j^{e_j} q_1^{f_1} \cdots q_k^{f_k}$ be the prime factorization of n , with $p_i \equiv 1 \pmod{4}$ and $q_i \equiv 3 \pmod{4}$. Then n is a sum of two squares if and only if all f_i are even.*

Proof. Suppose that f_i are all even. Note that products of sums of squares are sums of squares: by Diophantus' Identity,

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

Thus each $q_i^{f_i}$ is a square; the primes p_i are sums of squares by Theorem 13. Thus their product $p_1^{e_1} \cdots p_j^{e_j} q_1^{f_1} \cdots q_k^{f_k}$ is a prime. Observe that 2^m is either a square or a sum of squares (namely $2^{m-1} + 2^{m-1}$); thus n is a sum of squares.

Suppose that n is a sum of squares. Then $n = \alpha \cdot \bar{\alpha}$ for some $\alpha \in \mathbb{C}[i]$; factoring each α in the Gaussian integers, we attain that

$$n = \alpha \cdot \bar{\alpha} = (\pi_1 \cdots \pi_j)(\bar{\pi}_1 \cdots \bar{\pi}_j)$$

for Gaussian primes π_i . Suppose for contradiction that some f_k is odd; then

$$\nu_{q_k} \left(\frac{n}{q_k^{f_k-1}} \right) = 1.$$

Hence q divides exactly one of α or $\bar{\alpha}$. Without loss of generality, let $q \mid \alpha$. Since $q_k \equiv 3 \pmod{4}$, it is a Gaussian prime; thus by Euclid's lemma, $q_k = \pi_i$ for some i . Hence

$$q_k = \bar{q}_k = \bar{\pi}_i \mid \bar{\alpha}.$$

This yields the desired contradiction. We deduce that each f_i must be even. \square

The second part of that proof was fully original — it impressed the TA Mohammad. Nobody likes Mohammad.