UMA205: Introduction to Algebraic Structures

Naman Mishra

January 2024

Contents

Lecture 21: Wed 28 Feb '24

Corollary .0.1. *Let* $a, b \in \mathbb{Z}$*. If* $(a, b) = (d)$*, then* $d = \gcd(a, b)$*.*

Proof. Since $a, b \in (d)$, d is a common divisor of both a and b. Let c be another common divisor. Then $c \mid ax + by$, so $c \mid d$. Thus d is the greatest common divisor. $\square$

Notation. We will write (a, b) for the gcd of a and b. Whether this refers to the gcd or the ideal will (should) be clear from the context.

Definition .0.2 (Coprime)**.** Two integers are said to be *coprime* if their only common divisors are ± 1.

Thus a and b are coprime iff $(a, b) = 1$. There is a generalization of this to other rings, where instead of ± 1 we say that two elements are coprime if their only common divisors are *units*.

Proposition .0.3. *Suppose* $(a, b) = 1$ *and* $a \mid bc$*. Then* $a \mid c$*.*

Proof. There exist x, y such that $ax + by = 1$. Then $c = cax + cby$. But $a \mid cb$, so $a \mid c$. $\square$

Corollary .0.4. *If* p *is a prime and* $p \mid bc$*, then* $p \mid b$ *or* $p \mid c$*. Equivalently, if* $p \nmid b$ *and* $p \nmid c$*, then* $p \nmid bc$*.*

Proof. Since p is a prime, its only divisors are ± 1 and $\pm p$. Thus, either $(p, b) = 1$ or $p \mid b$. If $p \mid b$, then we are done. Otherwise, by the previous proposition, $p \mid c$. $\square$

Corollary .0.5. *Suppose* p *is a prime and* $a, b \in \mathbb{Z}$*. Then* $\operatorname{ord}_p(ab) = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$*.*

Proof. Let $\alpha = \operatorname{ord}_p(a)$, $\beta = \operatorname{ord}_p(b)$ so that $a = p^\alpha a'$ and $b = p^\beta b'$ where $p \nmid a', b'$. Then $ab = p^{\alpha+\beta} a'b'$. By the previous corollary, $p \nmid cd$. Thus $\operatorname{ord}_p(ab) = \alpha + \beta$. $\square$

Lemma .0.6 (Existence of prime factorization)**.** *Every integer $n \neq 0, \pm 1$ has a prime factorization.*

Proof. Let n be the smallest positive integer without a prime factorization. Then n is not prime, so $n = ab$ for some $a, b \in \mathbb{Z}$. But $a, b < n$ have prime factorizations, so n has a prime factorization.

If every positive integer has a prime factorization, then so will the negative of any such integer, by taking an additional factor of -1. $\square$

Theorem .0.7 (Fundamental theorem of arithmetic)**.** *Every integer $n \neq 0$ has a unique prime factorization.*

Proof. Write n as

$$n = (-1)^{\epsilon(n)} \prod_{\substack{p \text{ prime} \\ p>0}} p^{a(p)}.$$

For any prime q, apply ord_q to both sides. Then

$$\operatorname{ord}_q(n) = \epsilon(n) \operatorname{ord}_q(-1) + \sum_p^q a(p) \operatorname{ord}_q(p)$$

by corollary .0.5. But by the definition of ord_q, $\operatorname{ord}_q(-1) = 0$ and $\operatorname{ord}_q(p) = \delta_{pq}$. Thus $a(q) = \operatorname{ord}_q(n)$ is uniquely determined. $\square$

.1 In Other Rings

Definition .1.1 (Field)**.** A *field* is a commutative ring with identity $1 \neq 0$, where all non-zero elements have multiplicative inverses.

Example. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, finite fields $\mathbb{F}_q$, where q is a prime power.

Definition .1.2 (Ring of polynomials)**.** For a field k, $k[x]$ is the *ring of polynomials* in x with coefficients from k. There is a notion of divisibility in $k[x]$. We thus write $f \mid g$ if $g = fp$ for some $p \in k[x]$.

A non-constant polynomial p is *irreducible* if $q \mid p$ only when q is constant or a multiple of p.

Examples.

- $3 \mid 1 + x$.
- Linear polynomials are always irreducible.
- $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{C}[x]$.

Lemma .1.3. *Every non-constant polynomial is a product of irreducible polynomials.*

Proof idea. Same as for $\mathbb{Z}$, but we use induction on the degree of the polynomial. $\square$

Definition .1.4 (Monic polynomial)**.** A polynomial is *monic* if its leading coefficient is 1.

Definition .1.5 (Order)**.** Let $f, p \in k[x]$, p irreducible. Then $\mathrm{ord}_p(f) = a$ if $f = p^a q$ for some $q \in k[x]$ and $p \nmid q$.

Theorem .1.6 (Unique factorization of polynomials)**.** *Let $f \in k[x]$. Then we can write*

$$f = c \prod_p p^{a(p)}$$

where the product runs over all monic irreducible polynomials, $a(p) = \mathrm{ord}_p(f)$ and $c \in k$.

Lecture 22: Fri 01 Mar '24

Definition .1.7 (Integral domain)**.** An *integral domain* is a commutative ring with no zero divisors.

For integral domains, the cancellation law holds. $ac = bc \wedge c \neq 0 \implies a = b$.

Example. $\mathbb{Z}$, $k[x]$.

Definition .1.8 (Euclidean domain)**.** A *Euclidean domain* is an integral domain R together with a function $\lambda \colon R^* \to \mathbb{N}$ such that if $a, b \in R$ with $b \neq 0$, there exist $c, d \in R$ with $a = cb + d$, then either $d = 0$ or $\lambda(d) < \lambda(b)$.

Recall that for $a_1, \ldots, a_n \in R$,

$$(a_1, \ldots a_n) = \{x_1 a_1 + \ldots x_n a_n \mid x_1, \ldots, x_n \in R\}$$

is the ideal generated by $a_1, \ldots, a_n$.

Definition .1.9 (Principal ideals)**.** If an ideal I can be written as $I = (a_1, \dots, a_n)$, we say I is *finitely generated.* If $I = (a)$, we say that I is a *principal ideal.* An integral domain is called a *principal ideal domain* (PID) if all finitely generated ideals are principal.

Example. $\mathbb{Z}$ is a PID.

Proposition .1.10. *Every Euclidean domain is a principal ideal domain.*

Proof. Let I be an ideal in a Euclidean domain R. Consider the set $\{\lambda(b) \mid b \in I^*\} \subseteq \mathbb{N}$. So there exists a minimal element $a \in I^*$ such that $\lambda(a) \le \lambda(b)$ for all $b \in I^*$.

We claim that $I = (a) = Ra = \{ra \mid r \in R\}$. Since $a \in I$ and I is an ideal, $Ra \subseteq I$. Let $b \in I$. Then there exist $q, r \in R$ such that $b = qa + r$ with $r = 0$ or $\lambda(r) < \lambda(a)$. But $r = b - qa \in I$. Since $\lambda(a)$ is minimal, $r = 0$, which gives $b = qa \in Ra$ and $I \subseteq Ra$. $\square$

The converse is false, but it is hard to find a counterexample.

Definition .1.11. Let R be a principal ideal domain.

- For $a \in R$, $b \in R^*$, we say that *a divides b* (denoted $a \mid b$) if $b = ac$ for some $c \in R$. In other words, $(b) \subseteq (a)$.
- An element $u \in R$ is called a *unit* if $u \mid 1$. In other words, $(u) = R$.
- Two elements $a, b \in R$ are called *associates* if $a = bu$ for some unit $u \in R$. In other words, $(a) = (b)$.
- A non-unit $p \in R$ is called a *prime* if $p \neq 0$ and for all $a, b \in R$, $p \mid ab$ only if $p \mid a$ or $p \mid b$. In other words, if $ab \in (p)$, then $a \in (p)$ or $b \in (p)$.

Exercise .1.12. *Prove the "in other words" above.*

.1.1 Unique factorization for PIDs

- Show that the greatest common divisor of $a, b \in R$ exists and is unique up to associates, and $(a, b) = (d)$.
- We can find for every a and p prime, the *order* $\mathrm{ord}_p(a)$, which satisfies $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$.

Let S be a set of primes in R satisfying

(i) every prime in R is associate to some prime in S, and

(ii) no two primes in S are associates.

Theorem .1.13 (Unique factorization theorem)**.** *Let R be a principal ideal domain and S be as above. Then for all $a \in R^*$, we can write*

$$a = u \prod_{p \in S} p^{e(p)}$$

where $e(p) = \operatorname{ord}_p(a)$ and u is a unit. Further, this is unique.

Definition .1.14 (Unique factorization domain)**.** A domain R for which unique factorization holds is called a *unique factorization domain* (UFD).

Examples.

- $\mathbb{Z}$ is a UFD.
- $k[x_1, \ldots, x_n]$ is a UFD but not a PID.
- $\mathbb{Z}[\sqrt{3}i]$ is a ring. It is also an integral domain by virtue of being a subring of $\mathbb{C}$. $2, 1 \pm \sqrt{3}i$ are primes (absolute value 2 is minimal). The only units are ± 1, so no two are associates of each other. But $4 = 2 * 2 = (1 + \sqrt{3}i)(1 - \sqrt{3}i)$. Thus $\mathbb{Z}[\sqrt{3}i]$ is not a UFD.
- $\mathbb{Z}[\sqrt{7}]$ has $6 = 2 * 3 = (\sqrt{7} + 1)(\sqrt{7} - 1)$. But 2 and 3 are not prime! (exercise) $\mathbb{Z}[\sqrt{7}]$ does turn out to be a UFD.

Fact .1.15 (Gauss' conjecture)**.** *Let d be a square-free positive integer. Consider $\mathbb{Q}[i\sqrt{d}]$. The subring of algebraic integers in it is a UFD iff d is a* Heegner *number. That is,*

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

If $d = 1$, this subring is $\mathbb{Z}[i]$. But if $d = 3$, it is $\mathbb{Z}[e^{i\pi/3}]$, not $\mathbb{Z}[i\sqrt{3}]$.

Lecture 23: Mon 04 Mar '24

Examples (UFD)*.*

- $\mathbb{Z}[i]$, the *Gaussian integers*.
- $\mathbb{Z}[\omega]$, the *Eisenstein integers*, where $\omega = e^{\frac{2\pi i}{3}}$.

Proposition .1.16. $\mathbb{Z}[i]$ *is a Euclidean domain.*

Proof. Define $\lambda\colon \mathbb{Z}[i] \to \mathbb{N}$ as $\lambda(a+ib) = a^2+b^2$. Let $\alpha = a+ib$, $\gamma = c+id \neq 0$. Write $\frac{\alpha}{\gamma} = r+is$, where $r, s \in \mathbb{Q}$. Choose $m, n \in \mathbb{Z}$ such that $|r-m| \leq \frac{1}{2}$ and $|s-n| \leq \frac{1}{2}$. Let $\delta = m+in$. Then $\lambda(\frac{\alpha}{\gamma} - \delta) = (r-m)^2 + (s-n)^2 \leq \frac{1}{2}$. Define $\rho = \alpha - \gamma\delta$, Either $\rho = 0$, or

$$\begin{aligned}\lambda(\rho) &= \lambda(\gamma)\lambda\left(\frac{\alpha}{\gamma} - \delta\right)\\ &\leq \frac{1}{2}\lambda(\gamma)\\ &< \lambda(\gamma).\end{aligned}$$

□

Corollary .1.17. *$\mathbb{Z}[i]$ is a PID and hence a UFD.*

Exercise .1.18. *Prove that $\mathbb{Z}[\omega]$ is a Euclidean domain.*

Chapter I

The Study of Primes

Theorem I.0.1 (Euclid)**.** *There are infinitely many primes in* $\mathbb{Z}$*.*

Proof. Suppose not. Label the positive primes $p_1, p_2, \ldots, p_n$. Define $N = p_1 p_2 \ldots p_n + 1$. Clearly, N is not divisible by any p_i. But N must be a product of primes. This is a contradiction. $\square$

Remark. Check out the proofs of this theorem in *Proofs from THE BOOK*.

Exercise I.0.2. *There are infinitely many monic irreducible polynomials in* $k[x]$*, assuming* k *is infinite.*

Proof. $x + a$ for each $a \in k$. $\square$

I.1 Arithmetic Functions

- $\nu(n)$ = number of positive divisors of n.
- $\sigma(n)$ = sum of positive divisors of n.
- The *Möbius function*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not square-free} \\ (-1)^{\#\text{ prime factors of } n} & \text{otherwise} \end{cases}$$

- The *Euler totient function*

$$\phi(n) = \#\{1 \leq m \leq n \mid \gcd(m, n) = 1\}$$

Examples.

- $\nu(3) = 2$, $\sigma(3) = 4$, $\mu(3) = -1$, $\phi(3) = 2$.
- $\nu(6) = 4$, $\sigma(6) = 12$, $\mu(6) = 1$, $\phi(6) = 2$.
- $\sigma(28) = 56$, since it is a perfect number.

Proposition I.1.1. *Write n as $n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$ in terms of its prime factors. Then*

(i) $\nu(n) = (a_1 + 1)(a_2 + 1) \dots (a_l + 1)$.

(ii) $\sigma(n) = (1 + p_1 + \dots p^{a_l}) \dots (1 + p_l + \dots + p_l^{a_l})$.

Proof. For the first part, every l-tuple $(b_1, \dots, b_l)$ can be transformed bijectively to a divisor of n.

For the second, write

$$\begin{aligned} \sigma(n) &= \sum_{d|n} d \\ &= \sum_{\substack{0 \le b_i \le a_i \\ 1 \le i \le l}} p_1^{b_1} \dots p_l^{b_l} \\ &= \prod_{i=1}^{l} \sum_{0 \le b_i \le a_i} p_i^{b_i} \\ &= \prod_{i=1}^{l} \frac{p_i^{a_i+1} - 1}{p_i - 1}. \end{aligned}$$

□

Proposition I.1.2. $\sum_{d|n} \mu(d) = \delta_{n,1}$.

Proof. True for $n = 1$. For $n > 1$, write n as $p_1^{a_1} \dots p_l^{a_l}$. Since $\mu(d) = 0$ whenever d is not square-free, we have

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{\substack{b_i \in \{0,1\} \\ 1 \le i \le l}} \mu(p_1^{b_1} \dots p_l^{b_l}) \\ &= \sum_{k=0}^{l} \binom{l}{k} (-1)^k \\ &= (1 - 1)^k \\ &= 0 \end{aligned}$$

□

Definition I.1.3 (Dirichlet convolution)**.** Let $f, g \colon \mathbb{N}^* \to \mathbb{C}$. Then the *Dirichlet convolution* of f and g is

$$(f \circ g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$$

Exercise I.1.4. $(f \circ g) \circ h = f \circ (g \circ h)$.

Let $\varepsilon(n)$ be the multiplicative identity. That is, $\varepsilon(n) = \delta_{n,1}$. Check that $f \circ \varepsilon = \varepsilon \circ f = f$. Let $\mathbb{1}$ be the constant function $\mathbb{1}(n) = 1$ for all n. Then $f \circ \mathbb{1} = \mathbb{1} \circ f = \sum_{d|\cdot} f(d)$.

Lemma I.1.5. $\mathbb{1} \circ \mu = \mu \circ \mathbb{1} = \varepsilon$.

Proof. First,

$$\begin{aligned}(\mathbb{1} \circ \mu)(1) = (\mu \circ \mathbb{1})(1) &= \sum_{d|1} \mu(d) \\ &= \mu(1) \\ &= 1.\end{aligned}$$

For $n > 1$,

$$\begin{aligned}(\mathbb{1} \circ \mu)(n) = (\mu \circ \mathbb{1})(n) &= \sum_{d|n} \mu(d) \\ &= 0\end{aligned}$$

by proposition I.1.2. □

Theorem I.1.6 (Möbius inversion formula)**.** *Let* $F(n) = \sum_{d|n} f(d)$. *Then* $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d})$.

Proof. Note that $F = f \circ \mathbb{1}$. So

$$\begin{aligned}\sum_{d|\cdot} \mu(d)F\left(\frac{\cdot}{d}\right) &= F \circ \mu \\ &= (f \circ \mathbb{1}) \circ \mu \\ &= f \circ (\mathbb{1} \circ \mu) \\ &= f \circ \varepsilon \\ &= f\end{aligned}$$

□