

Instructor: Miklos Abert

Scribe: Justin Noel

June 19, 2006 .

1. LECTURE 1

1.1. Unique Factorization. We will first recall some facts about the number theory for the integers and then we will generalize this to a more abstract setting.

Notation 1.1. \mathbb{Z} represents the integers and \mathbb{N} represents the natural numbers (note that $0 \in \mathbb{N}$).

Axiom 1.2 (Well-ordered). *Every non-empty subset of \mathbb{N} has a minimal element.*

Definition 1.3. $a|b$ if $\exists c$ s.t. $ac = b$.

Definition 1.4. p is a prime, if $c|p \iff c = \pm 1$ or $\pm p$ and $p \neq \pm 1$.

Lemma 1.5. p is a prime, $n \neq 0 \implies \exists k \geq 0$ s.t. $p^k|n$ and $p^{k+1} \nmid n$.

Definition 1.6. $\text{ord}_p n = k$ where k is as above.

Theorem 1.7 (Unique factorization).

$$n = (-1)^{\varepsilon(n)} \prod_{\text{primes } p>0} p^{\text{ord}_p n}$$

We will prove this below.

Lemma 1.8 (Division with remainder). *For $a, b \in \mathbb{Z}$, $b > 0 \implies \exists q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < b$.*

Proof. Consider $S = \{a - bx | x \in \mathbb{Z}\}$ and find a way to apply the well-ordered axiom for \mathbb{N} to define the value of r . \square

Definition 1.9. If $a_1, \dots, a_n \in \mathbb{Z}$ then we define the *ideal*

$$(a_1, \dots, a_n) = \{a_1x_1 + \dots + a_nx_n | x_i \in \mathbb{Z}\}.$$

Lemma 1.10. $\forall a, b \in \mathbb{Z}, \exists d \in \mathbb{Z}$ s.t. $(a, b) = (d)$.

Proof. Apply the well-ordered axiom to the set (a, b) to obtain a number d . Show that the definition of the ideal gives $(d) \subseteq (a, b)$. Then use division with remainder to show that $(a, b) \subseteq (d)$ hence $(d) = (a, b)$. \square

Definition 1.11. For $a, b \in \mathbb{Z}$, d is a *gcd* of a and b if $d|a$ and $d|b$ and if $c|a$ and $c|b$ then $c|d$.

Lemma 1.12. $(a, b) = (d) \iff d$ is a *gcd* of a and b .

Definition 1.13. For $a, b \in \mathbb{Z}$, m is a *lcm* of a and b if $a|m$ and $b|m$ and if $a|c$ and $b|c$ then $m|c$.

Corollary 1.14. $(a) \cap (b) = (m) \iff m$ is a *lcm* of a and b .

Lemma 1.15. If $a|bc$ and $(a, b) = 1 \implies a|c$.

Proof. Since $(a, b) = 1$, $\exists x, y$ s.t. $ax + by = 1$. Multiplying by c we get $acx + bcy = c$. Show that a divides both summands on the left to get the answer. \square

Corollary 1.16. If p is prime $p|bc \implies p|b$ or $p|c$.

Proof. $(p, b) = 1$ or p . From either case the result follows. \square

Corollary 1.17. If p is prime, $a, b \in \mathbb{Z} \implies \text{ord}_p ab = \text{ord}_p a + \text{ord}_p b$.

Proof. Let $\alpha = \text{ord}_p a$ and $\beta = \text{ord}_p b$ so $a = p^\alpha a'$ and $b = p^\beta b'$ where $p \nmid a'$ and $p \nmid b'$. Then just multiply. \square

Proof. Theorem 1.7, Unique Factorization. We claim $|n|$ is a product of primes: if not take a minimal counterexample. Either n is prime or isn't. If it is we are done. Otherwise $n = n_1 n_2$ with $n_1, n_2 < n$. This gives us a contradiction.

So, $n = (-1)^{\varepsilon(n)} \prod_{p>0} p^{a(p)}$. Let q be a prime, then $\text{ord}_q n = \varepsilon(n) \cdot \text{ord}_p(-1) + \sum_{p>0} a(p) \text{ord}_q p$. Then almost all of the summands are zero except for when $q = p$ in which case we get $\text{ord}_q n = a(q)$. This gives us the desired formula. \square

Definition 1.18. $\mathbb{R}[x]$ = set of polynomials with real coefficients, i.e.

$$\mathbb{R}[x] = \{a_n x^n + \dots + a_0 \mid a_i \in \mathbb{R}\}$$

Definition 1.19. If $f(x) = a_n x^n + \dots + a_0$ with $a_n \neq 0$ then $\deg f = n$. We set $\deg 0 = -\infty$.

Proposition 1.20. $\deg(f \cdot g) = \deg f + \deg g$ and $\deg(f + g) \leq \max(\deg f, \deg g)$.

We can now apply all of the above with $\mathbb{R}[x]$ instead of \mathbb{Z} . We see that the prime elements are the irreducible polynomials such as $x + 3$ and $x^2 + 1$. In the division with remainder theorem we have to make some changes. Everything works up to multiplication by constants and the condition $b > 0$ must be replaced with b being a monic polynomial (i.e. a polynomial whose highest degree term has coefficient 1). The condition $0 \leq r < b$ will be replaced with the condition $\deg 0 \leq \deg r < \deg b$.

Motivated by this we will now develop a general framework, which will retain most of the nice properties of the integers listed above.

Definition 1.21. A commutative ring R with unit is an *integral domain* if $ab = 0 \implies a = 0$ or $b = 0$. This is equivalent to the cancellation rule:

$$ax = bx \implies x = 0 \text{ or } a = b.$$

Definition 1.22. R is a *Euclidean domain* if R is an integral domain with a function $\lambda : R \setminus \{0\} \rightarrow \mathbb{N}$ s.t. $\forall a, b$ with $b \neq 0$, there $\exists q, r$ s.t.

$$a = bq + r \text{ with } \lambda(r) < \lambda(b).$$

Definition 1.23. $I \subseteq R$, with $I \neq \emptyset$, is an *ideal* if $a, b \in I \implies a - b \in I$ and if $r \in R$ and $a \in I$ then $ra \in I$.

Definition 1.24. I is a *principal ideal* if $I = (a) = aR = \{a \cdot x \mid x \in R\}$.

Lemma 1.25. If R is a Euclidean domain, $I \triangleleft R \implies \exists a$ s.t. $I = aR$.

Proof. Hint: Let a be the smallest element in I . Use λ to make sense of the word, smallest. \square

Definition 1.26. R is a *principal ideal domain (PID)* if every ideal is principal.

Definition 1.27. For $a, b \in R$, $a \mid b$ if $\exists c$ such that $ac = b$. In other words $(b) \subseteq (a)$.

Definition 1.28. An element $u \in R$ is a *unit* if $u \mid 1$. In other words $(u) = R$ or u^{-1} exists.

Definition 1.29. We write $a \sim b$ (a and b are associates) if $a = ub$ for some unit u . In other words $(a) = (b)$.

Definition 1.30. An element $p \in R$ is *irreducible* if $a|p \implies a \sim p$ or a is a unit.

Definition 1.31. If $p \in R$ such that $p \neq 0$ and p is not a unit then p is *prime* if $p|ab \implies p|a$ or $p|b$. In other words, $ab \in (p) \implies a \in (p)$ or $b \in (p)$.

Lemma 1.32. If R is a PID then p irreducible $\iff p$ is prime.

Proof. It is easy to see prime \implies irreducible.

For the other direction, without loss of generality, suppose $p|ab$ and $p \nmid a$. We have $(a, p) = (d) \implies d$ is a unit or $d \sim p \implies (a, p) = R$. Now we have $(ab, pb) = (b) \implies (b) \subseteq (p) \implies p|b$. \square

Definition 1.33. A ring R satisfies the *ascending chain condition (ACC)* if for every chain of ideals $(a_1) \subseteq (a_2) \subseteq \dots$ there exists k such that $(a_k) = (a_{k+i}) \forall i > 0$.

Lemma 1.34. If R is a PID, then it satisfies the ACC.

Proof. Let $I = \bigcup (a_i)$. Then I is an ideal $\implies I = (a)$ and $a \in (a_k)$ for some k which implies $(a) = (a_k)$. \square

Definition 1.35. A ring is *Noetherian*, if it satisfies the ACC. This is equivalent to the condition that every ideal is finitely generated (Try to prove this!).

Lemma 1.36. R is a PID \implies every non-unit element is divisible by a non-unit irreducible.

Proof. Assume $a \in R$ is a non-unit. If $a \in R$ is not irreducible it decomposes into a product a_1b_1 , with a_1 and b_1 not units. If a_1 is not irreducible we can decompose it as a similar product. Proceeding in this way we can repeatedly factor a into a product of more and more terms. If this process didn't terminate we can construct an ascending chain of ideals: Suppose that we can decompose the first term a_1 indefinitely, then we have $a = a_1b_1 = a_2b_2b_1 = a_3b_3b_2b_1 = \dots$ which gives us $(a) \subset (a_1) \subset (a_2) \subset (a_3) \subset \dots$. This chain must stabilize, which means for some k , a_k is irreducible. \square

Lemma 1.37. R is a PID \implies every element is a product of irreducibles.

Proof. If $a \in R$ is a unit we are done. If not we can use Lemma 1.36 to write $a = a_1b_1$ with a_1 an irreducible non-unit and b_1 a non-unit. If b_1 is irreducible then we are done. If not we can apply the lemma again to b_1 , which gives us $a = a_1a_2b_2$. As long as b_n is decomposable we continue in this way and write $a = a_1a_2 \dots a_nb_n$ where the a_i are irreducible. This process must terminate, otherwise we can get an ascending chain of ideals $(a) \subset (b_1) \subset (b_2) \subset \dots$. When this chain stabilizes at b_k we have that b_k is irreducible and we are done. \square

Theorem 1.38 (Unique Factorization Theorem for PID's). Let P be a set of primes in R such that for any prime $p \in R$ there exists a $q \in P$ such that $p \sim q$, and such that no two primes in R are associated. Then $\forall a \neq 0$

$$a = u \prod_{p \in P} p^{i_p}$$

where u is a unit and the i_p are natural numbers.

Proof. Put it together from the above. \square