

REU 2005 · Discrete Mathematics · Lecture 3

Instructor: László Babai
Scribe: Eric Purdy

June 22, 2005. Last updated June 22, 2005

1 Lecture 3

1.1 Groups

Definition 1.1. A group is a monoid in which every element has an inverse.

Remember, the empty set is a semigroup, but not a monoid, since it has no identity.

The following axioms define a group G :

1. $(\forall a, b \in G)(\exists! ab \in G)$ (The product of two elements is uniquely defined.)
2. $(\forall a, b, c \in G)(a(bc) = (ab)c)$ (Multiplication is associative.)
3. $(\exists e \in G)(\forall x \in G)(ex = xe = e)$ (G has an identity element.)
4. $(\forall x \in G)(\exists y \in G)(xy = yx = e)$ (Every element of G has an inverse.)

Notation 1.2. We write x^{-1} to denote the inverse of x in a group.

We can also talk about one-sided inverses.

Definition 1.3. Let M be a monoid with identity e . y is a right inverse of x if $xy = e$. Left inverses are defined analogously.

Exercise* 1.4. If S is a semigroup with a right identity e and every element has a right inverse with respect to e (i. e., $(\forall x \in S)(\exists y \in S)(xy = e)$), then S is a group.

Lemma 1.5. Let M be a monoid. If $x \in M$ has right inverse x' and left inverse x'' then $x' = x''$.

Proof. $x' = ex' = (x''x)x' = x''(xx') = x''e = x''$ □

Exercise 1.6. Let G be a nonempty semigroup. Suppose that all linear equations in G are solvable, i. e., $(\forall a, b \in G)(\exists x, y \in G)(ax = b, ya = b)$. Then G is a group.

Definition 1.7. The left cancellation law in a semigroup S states that $(\forall a, x, y \in S)(ax = ay \implies x = y)$. The right cancellation law is defined analogously. Note that these laws do not hold in all semigroups.

Exercise 1.8. Every group satisfies both cancellation laws.

Example 1.9. $(\mathbb{N}, +)$ and $(\mathbb{N} + 1, \cdot)$ are examples of monoids in which both cancellation laws hold, but which are not groups.

Exercise 1.10. If a finite, nonempty semigroup satisfies both cancellation laws, then it is a group.

Notation 1.11. We use \mathbb{Z}_m to denote the integers modulo m .

Example 1.12. For $m = 12$, $8 \cdot 9 = 0$ and $8 + 9 = 5$ in \mathbb{Z}_{12} .

(\mathbb{Z}_m, \cdot) is a monoid with zero.

Definition 1.13. The multiplicative subgroup of \mathbb{Z}_m is

$$\mathbb{Z}_m^\times = \{x \in \mathbb{Z}_m \mid (\exists y \in \mathbb{Z}_m)(xy \equiv 1 \pmod{m})\} = \{x \in \mathbb{Z}_m \mid \gcd(x, m) = 1\}.$$

Lemma 1.14. \mathbb{Z}_m^\times is a subsemigroup of \mathbb{Z}_m in which the cancellation law holds.

Proof. $ax \equiv ay \pmod{m} \implies m \mid ax - ay \implies m \mid a(x - y)$. Since $a \in \mathbb{Z}_m^\times$, $\gcd(a, m) = 1$. Therefore, $m \mid a(x - y) \implies m \mid (x - y) \implies x \equiv y \pmod{m}$. \square

Corollary 1.15. \mathbb{Z}_m^\times is a group.

1.2 Arithmetic Functions

Definition 1.16. Euler's phi function is defined as $\varphi(m) := |\mathbb{Z}_m^\times|$. $\varphi(m)$ is equal to the number of integers between 0 and $m - 1$ that are relatively prime to m .

Example 1.17. For p a prime, k a positive integer, $\varphi(p) = p - 1$ and $\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$.

Proof. n is relatively prime to p^k if and only if it is not divisible by p . Therefore, exactly $\frac{1}{p}$ of the numbers are not relatively prime to p . This leaves $p^k \left(1 - \frac{1}{p}\right) = p^k - p^{k-1}$ numbers between 0 and p^k that are relatively prime to p^k . \square

Please review the "Basic Number Theory" handout, especially the section on arithmetic functions.

Notation 1.18. \mathbb{N}^+ denotes the positive integers, i. e., $\mathbb{N}^+ = \{1, 2, \dots\} = 1 + \mathbb{N}$.

Definition 1.19. Functions $f : \mathbb{N}^+ \rightarrow \mathbb{C}$ are called arithmetic functions.

Definition 1.20. An arithmetic function $f : \mathbb{N}^+ \rightarrow \mathbb{C}$ is multiplicative if $f(1) = 1$ and $(\forall a, b \in \mathbb{N}^+)(\gcd(a, b) = 1 \implies f(ab) = f(a)f(b))$.

Comment: We can replace the condition that $f(n) = 1$ with the condition that $f(n)$ is not always zero. If $f(x) \neq 0$ for some x , then $f(x) = f(1 \cdot x) = f(1)f(x) \implies f(1) = 1$.

Exercise 1.21. $\varphi(n)$ is multiplicative.

Corollary 1.22. If $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, where the p_i are distinct primes and the k_i are positive, then $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right)$.

Proof.

$$\begin{aligned} \varphi(n) &= \varphi\left(\prod_{i=1}^s p_i^{k_i}\right) = \prod_{i=1}^s \varphi(p_i^{k_i}) \\ &= \prod_{i=1}^s (p_i^{k_i} - p_i^{k_i-1}) \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^s \left(1 - \frac{1}{p_i}\right) \quad \square \end{aligned}$$

Definition 1.23. The Moebius function, $\mu(n)$, for an integer $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, where the p_i are distinct primes and the k_i are positive, is defined as:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^s & \text{if } k_1 = k_2 = \dots = k_s = 1 \\ 0 & \text{otherwise} \end{cases}$$

It is evident that μ is multiplicative.

For $f : \mathbb{N} \rightarrow \mathbb{C}$, we can define another arithmetic function $g = \sum_{d|n} f(d)$, called the *summation function* of f .

Let $h(n) = \sum_{d|n} \varphi(d)$. What is $h(n)$? Some experimentation is in order.

Experiment 1.24. We will try $n = 30$ and $n = p$, a prime.

$$\begin{aligned} h(30) &= \varphi(30) + \varphi(15) + \varphi(10) + \varphi(6) + \varphi(5) + \varphi(3) + \varphi(2) + \varphi(1) \\ &= 8 + 8 + 4 + 2 + 4 + 2 + 1 + 1 = 30 \end{aligned}$$

$$h(p) = \varphi(p) + \varphi(1) = (p-1) + 1 = p$$

These experiments suggest the conjecture that $h(n) = n$.

Exercise 1.25. $(\forall n \in \mathbb{N}^+) (\sum_{d|n} \varphi(d) = n)$.

Let $k(n) = \sum_{d|n} \mu(d)$. What is $k(n)$? Again, we will experiment with particular values of n .

Experiment 1.26. We will try $n = 30$.

$$\begin{aligned} k(30) &= \mu(30) + \mu(15) + \mu(10) + \mu(6) + \mu(5) + \mu(3) + \mu(2) + \mu(1) \\ &= -1 + 1 + 1 + 1 + -1 + -1 + -1 + 1 = 0 \end{aligned}$$

Is $k(n)$ always 0? No, because $k(1) = \mu(1) = 1$.

Exercise 1.27. $k(n) = 0$ for all $n > 1$.

Exercise 1.28. If $f : \mathbb{N}^+ \rightarrow \mathbb{C}$ is a multiplicative function, then $g = \sum_{d|n} f(d)$ is also multiplicative.

Exercise 1.29 (Möbius Inversion Formula). If $f : \mathbb{N}^+ \rightarrow \mathbb{C}$ is an arithmetic function, and $g = \sum_{d|n} f(d)$, then $f = \sum_{d|n} g(d)\mu(\frac{n}{d})$.

1.3 Subgroups and Orders

If G is a group, and $H \subseteq G$, we say H is a *subgroup* of G and write $H \leq G$ if the following conditions are met:

1. $(\forall x, y \in H)(xy \in H)$ (H is closed under multiplication)
2. $(\forall x \in H)(\exists x^{-1} \in H)(xx^{-1} = x^{-1}x = 1)$ (H is closed under inverses)
3. H contains the identity of G .

Note that this notation is ambiguous: $H \leq G$ may mean that H is a subgroup of G , or that H is a subsemigroup of G . Hopefully this will be clear from context.

Example 1.30. $(\mathbb{N}, +)$ is a subsemigroup of $(\mathbb{Z}, +)$, but it is not a subgroup of $(\mathbb{Z}, +)$. (The nonzero elements do not have inverses.)

Definition 1.31. Let H be a subgroup of a group G . A right coset of H , denoted Ha , is the set $\{ha|h \in H\}$. A left coset would be defined analogously.

Exercise 1.32. For $H \leq G$, $a, b \in G$, if $Ha \cap Hb \neq \emptyset$, then $Ha = Hb$.

Two cosets of H are either disjoint or the same; therefore, the cosets partition G into disjoint sets. If we choose one representative from each coset, and let R be the set of these representatives, we can write $G = \dot{\bigcup}_{a \in R} Ha$. (The dot over the union symbol means that the sets are disjoint.)

Definition 1.33. The index of H in G (denoted by $|G : H|$) is $|R|$, i. e., the number of right cosets.

Example 1.34. $(\mathbb{Z}, +)$ is a group. $7\mathbb{Z} \leq \mathbb{Z}$ is a subgroup of index $|\mathbb{Z} : 7\mathbb{Z}| = 7$. We can choose $\{0, 1, 2, 3, 4, 5, 6\}$ as a set of coset representatives. The cosets are $7\mathbb{Z} + i$, for $0 \leq i \leq 6$.

Corollary 1.35 (Lagrange's Theorem). $|G| = |G : H| \cdot |H|$

Proof. Each coset Ha has the same number of elements ($(ha \mapsto hb)$ is a bijection between Ha and Hb), and $H = H1$ is a coset, so the number of cosets times the number of elements in H is the number of elements in G . \square

Note: Lagrange's Theorem applies to infinite groups as well, if we know how to multiply infinite cardinals.

Corollary 1.36. If G is a finite group, and $H \leq G$, then $|H|$ divides $|G|$.

Definition 1.37. A cyclic group is a group that is generated by one element, i. e., $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$, where $a^0 := 1$ and $a^{-k} := (a^{-1})^k$.

Definition 1.38. The order of a is the order of the subgroup $\langle a \rangle$.

Example 1.39. In \mathbb{Z}_7^\times , the order of 2 is 3, since $\langle 2 \rangle = \{1, 2, 4\}$. The order of \mathbb{Z}_7^\times is 6, so we see once again that the order of a subgroup divides the order of the group.

Exercise 1.40. $\text{ord}(a)$ is the smallest positive integer k such that $a^k = 1$.

Exercise 1.41. $a^k = 1 \iff \text{ord}(a) \mid k$. (This is true also if we define $\text{ord}(a)$ to be 0 for elements of infinite order.)

Exercise 1.42. $a^k = a^\ell \iff k \equiv \ell \pmod{\text{ord}(a)}$ (Hint: use Exercise 1.41)

Exercise 1.43. If $ab = ba$ then $\frac{\text{lcm}(\text{ord}(a), \text{ord}(b))}{\text{gcd}(\text{ord}(a), \text{ord}(b))} \mid \text{ord}(ab) \mid \text{lcm}(\text{ord}(a), \text{ord}(b))$. (The first of these assertions is more difficult to prove.) (Hint: use Exercise 1.41)

Exercise 1.44. If $\text{gcd}(\text{ord}(a), \text{ord}(b)) = 1$, then $\text{ord}(ab) = \text{ord}(a) \text{ord}(b)$. (Hint: use Exercise 1.41)

Corollary 1.45. If G is a finite group, then $a^{|G|} = 1$ for every $a \in G$.

Proof. Let $H = \langle a \rangle$. By Lagrange's Theorem $\text{ord}(a) = |H|$ divides $|G|$. By Exercise 1.41, this implies that $a^{|G|} = 1$. \square

The “yo-yo” picture which described the possible finite cyclic semigroups also applies to cyclic groups, except that the “yo-yo” must instead be a circle.

Corollary 1.46 (Euler-Fermat Congruence). If $\text{gcd}(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof. Apply Corollary 1.45 to the group $G = \mathbb{Z}_m^\times$. \square

Corollary 1.47 (Fermat's Little Theorem). Let p be a prime. If $\text{gcd}(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Fermat's Little Theorem has very significant applications to cryptography.

1.4 n th Roots of Unity

Definition 1.48. An n -th root of unity is $z \in \mathbb{C}$ such that $z^n = 1$.

Notation 1.49. $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

The n -th roots of unity form a subgroup of \mathbb{C}^\times , which we will denote by C_n . C_n is cyclic. It is generated by $\omega_1 = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$.

We can write the n -th roots of unity as $\omega_j = \cos\left(\frac{2\pi j}{n}\right) + i \sin\left(\frac{2\pi j}{n}\right)$, where j runs from 0 to $n - 1$.

Exercise 1.50. $\langle \omega_j \rangle = C_n$ if and only if $\gcd(j, n) = 1$.

Thus C_n has $\varphi(n)$ generators.

Exercise 1.51. Use C_n to solve Exercise 1.25

Exercise 1.52. z is an n -th root of unity $\iff \text{ord}(z) | n$. (Hint: Exercise 1.41).

Definition 1.53. If $\text{ord}(z) = n$, we call z a primitive n -th root of unity.

Exercise 1.54. There are $\varphi(n)$ primitive n -th roots of unity.

Exercise 1.55. $\sum_{j=0}^{n-1} \omega_j = 0$

Exercise* 1.56. Let $S_n := \sum' \omega_j$, where the sum runs over all j relatively prime to n . (So the sum has $\varphi(n)$ terms.) What is S_n ? (Experiment, conjecture, prove!)

Exercise 1.57. S_n is multiplicative.

Definition 1.58. The n -th cyclotomic polynomial (denoted $\Phi_n(x)$), is defined as $\Phi_n(x) = \prod' (x - \omega)$, where the product extends over all primitive n -th roots of unity ω .

The degree of $\Phi_n(x)$ is $\varphi(n)$.

Example 1.59. Some examples of primitive roots of unity and cyclotomic polynomials. Let $e(x) = \cos(x) + i \sin(x)$.

n	primitive n -th roots	$\Phi_n(x)$
1	1	$x - 1$
2	-1	$x + 1$
3	$e(1/3), e(2/3)$	$x^2 + x + 1$
4	$i, -i$	$x^2 + 1$
5	$e(1/5), e(2/5), e(3/5), e(4/5)$	$x^4 + x^3 + x^2 + x + 1$
6	$e(1/6), e(5/6)$	$x^2 - x + 1$

Exercise 1.60. $\Phi_n(x) \in \mathbb{Z}[x]$

Exercise 1.61.** $\Phi_n(x)$ is irreducible over \mathbb{Q} .