MA 453 - Elements Of Algebra I

January 29, 2009

Professor Uli Walther

January 13, 2008

By the end of the course, we will be given answers to the following:

1. Is it possible to write down explicit formulas to determine the roots of a polynomial (e.g. $c_n x^n + c_{n-1} x^{n-1} + \ldots + c_o$) in the terms of the coefficients $c_n, \ldots, c_o$ in the same way as the roots of the quadratic equation as given by (allowed operations are +, -, ÷, ×, $\sqrt[k]{}$),

$$r_{1,2} = -\frac{c_1}{2c_2} \pm \sqrt{\frac{c_1^2}{4c_2^2} - \frac{c_o}{c_2}}$$

2. (Dido's Problem) Given a ruler, compass, and a cube of volume 1, can you construct a cube of twice the volume? (Given a line segment of length 1, can you construct a line segment of length $\sqrt{2}$)

3. With ruler and compass, can you disect arbitrary angles?

Math Symbols:

Symbol	
$\mathbb{N}$	naturals - 0,1,2
$\mathbb{Z}$	..., -3, -2, -1, 0, 1, 2, 3,...
$\mathbb{Q}$	rationals $\left\{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\right\}$
$\mathbb{R}$	reals
$\mathbb{C}$	complex numbers

In order to write math "sentences," we use the following logic symbols,

Symbol	
$\in$	"is element of"
$\subseteq$	"is subset of"
$\exists$	"there exists"
$\forall$	"for all"

For example, $\forall n \in \mathbb{N} \exists m \in \mathbb{N} | m = n + 1$, for all natural n, there exists a real number m, such that $m = n + 1$.

Theorem Archimedian Property

If $n \in \mathbb{N}$, $m \in \mathbb{N}$ with $n \neq 0$, then $\exists q \in \mathbb{N}$ with $n \cdot q > m$.

Theorem Well-Ordering

If you take any non-empty subset S of $\mathbb{N}$, then S has a minimal element. (Contrast: $\mathbb{Z}$ has no such minimum).

Example Proof that $\sqrt{2}$ is not rational.

If $\sqrt{2}$ were rational, then $\sqrt{2} = \frac{p}{q}$ where $p, q \in \mathbb{N}$ and $q \neq 0$. $\frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2$. p must be even, $p = 2p'$. Plugging in, $(2p')^2 = 2q^2$ or $2(p')^2 = q^2$. Thus $q = 2q'$, $2(p')^2 = (2q')^2$, or $(p')^2 = 2(q')^2$, or $\frac{p'}{q'} = \sqrt{2}$. Assuming rationality, p must exist and must be minimal. If such a p exists, however, p would not be minimal. Contradiction shows that p does not exist.

Theorem Euclid

Given $a, b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ with $a = qb + r$ with $0 \leq r < |b|$.

Example $a = 7$, $b = 2$; $7 = 3 \cdot 2 + 1$. $a = -4$, $b = 3$, $-4 = (-2) \cdot 3 + 2$.

Definition Given $a, b \in \mathbb{Z}$, there are natural numbers $l = \mathrm{lcd}(a, b)$, $g = \mathrm{gcd}(a, b)$ where $\mathrm{gcd}(a, b) = \max\{n \in \mathbb{N} | n \text{ divides } a \text{ and } b\}$, $\mathrm{lcm}(a, b) = \max\{n \in \mathbb{N} |\ a \text{ divides } n \text{ and } b \text{ divides } n\}$.

Euclidian Algorithm For $\mathrm{gcd}(a, b)$. Initialize: $a_o = a$, $b_o = b$. Iteration: Write $a_i = q_i \cdot b_i + r_i$ with $q_i, r_i \in \mathbb{Z}$ and $0 \leq r_i < |b_i|$. Reset: $a_{i+1} = b_i$, $b_{i+1} = r_i$ until $r_i = 0$. When $r_i = 0$, $\mathrm{gcd}(a, b) = b_i$.

Example $a = 47$, $b = 65$; $a_o = 65$, $b_o = 65$. I1: $47 = 0 \cdot 65 + 47$, $a_1 = 65$, $b_1 = 47$. I2: $65 = 1 \cdot 47 + 18$, $a_2 = 47$, $b_2 = 18$. I3: $47 = 2 \cdot 18 + 11$, $a_3 = 18$, $b_3 = 11$. I4: $18 = 1 \cdot 11 + 7$, $a_4 = 11$, $b_4 = 7$. I5: $11 = 1 \cdot 7 + 4$, $a_5 = 7$, $b_5 = 4$. I6: $7 = 1 \cdot 4 + 3$, $a_6 = 4$, $b_6 = 3$. I7: $4 = 1 \cdot 3 + 1$, $a_7 = 3$, $b_7 = 1$. I8: $3 = 3 \cdot 1 + 0$ END.

Note if $a, b \in \mathbb{N}$, not zero,

$$\mathrm{lcm}(a, b) = \frac{a \cdot b}{\mathrm{gcd}(a, b)}$$

To illustrate, $a = 2^0 \cdot 3^2 \cdot 5^1 = 45$, $b = 2^4 \cdot 3^1 \cdot 5^0 = 48$. We claim that $\mathrm{lcm}(a, b) \cdot \mathrm{gcd}(a, b) = a \cdot b$.

$$\left(2^{\max(0,4)} \cdot 3^{\max(2,1)} \cdot 5^{\max(1,0)}\right)\left(2^{\min(0,4)} \cdot 3^{\min(2,1)} \cdot 5^{\min(1,0)}\right) = a \cdot b$$

This only works for two numbers. If we try to apply this to some a, b, and c we will be sadly disappointed.

Definition We say that a number $n \in \mathbb{N}$ is irreducible if an equation $a \cdot b = n$ (with $a, b \in \mathbb{N}$), either $a = 1$ or $b = 1$. We say that n is **prime** if "n divides $a \cdot b$" only happens if $n|a$ or $n|b$

Fact Within the integers, "prime" and "irreducible" are the same.

Proof Prime $\Rightarrow$ irreducble. Let n be prime, and assume that $a \cdot b = n$, $(a, b \in \mathbb{N})$. Then $n|ab$ and as n prime, $n|a$ or $n|b$. If $n|a$, $a = qn$. So $n = ab = qbn$, so $qb = 1 \Rightarrow q, b = 1$. Similarly, $n|b \Rightarrow a = 1$.

Corollary of Euclid If $a > b$, $\gcd(a,b) = \gcd(b, a-b) = \ldots$. So, $\gcd(a,b)$ is a linear combination of a, b : $\gcd(a,b) = xa + yb$ with $x, y \in \mathbb{Z}$.

January 15, 2008

Theorem $\gcd(a,b)$ is a linear combination of a and b: $\gcd(a,b) = ax + by$ where x and y are integers (because of Euclidian Alogrith).

So let p be irreducible and suppose $p|a \cdot b$. Need to sho: $p|a$ or $p|b$. Suppose p does not divide a, then $\gcd(p,a)$ is not p, hence 1 as p is irreducible. So,

$$1 = x \cdot p + y \cdot a$$

with $x, y \in \mathbb{Z}$. So,

$$b \cdot 1 = x \cdot b \cdot p + y \cdot a \cdot b$$

This says that p divides the RHS, so $p|b$. Similarly, if p does not divide b, then $p|a$.

Fermat's Last Theorem It is not possible to obtain $a^n = b^n + c^n$ for $a, b, c > 0$ and $n > 2$.

Modular Arithmetic is a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value — the modulus. The basic idea is to choose an integer $n \in \mathbb{Z}$ and equate it with 0. Let's say that $n = 12$. "Survivors" are 0,1,...,11 in some sense.

Definition "$\mathbb{Z}$ modulo n $\mathbb{Z}$" Let $n \in \mathbb{Z}$ then let $\mathbb{Z}/n\mathbb{Z}$ stand for the n families of numbers $\{\ldots, -n, 0, n, 2n, \ldots\}$, $\{\ldots, -n+1, 1, n+1, 2n+1, \ldots\}$, $\{\ldots, -n-1, -1, n-1, 2n-1, \ldots\}$.

Theorem Things in $\mathbb{Z}/n\mathbb{Z}$ can be added, subtracted, multiplied, and (in lucky cases) divided.

Example $n = 2$. We have 2 families in $\mathbb{Z}/2\mathbb{Z}$, $\{\ldots, -2, 0, 2, 4, \ldots\} \to 0 + 2\mathbb{Z}$, $\{..., -3, -1, 1, 3, 5, \ldots\} \to 1 + 2\mathbb{Z}$. One will note that there are an infinite representations of these two families. In adding the families together,

$+$	$\mathbf{0+2\mathbb{Z}}$	$\mathbf{1+2\mathbb{Z}}$
$\mathbf{0+2\mathbb{Z}}$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$\mathbf{1+2\mathbb{Z}}$	$1+2\mathbb{Z}$	$0+2\mathbb{Z}$

Multiplying,

$\times$	$\mathbf{0+2\mathbb{Z}}$	$\mathbf{1+2\mathbb{Z}}$
$\mathbf{0+2\mathbb{Z}}$	$0+2\mathbb{Z}$	$0+2\mathbb{Z}$
$\mathbf{1+2\mathbb{Z}}$	$0+2\mathbb{Z}$	

Fact Addition, subtraction, multiplication in $\mathbb{Z}/n\mathbb{Z}$ can be done by "representatives":

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

then,

$$a' + b' = a + kn + b + ln$$

$$a' + b' = (a + b) + n \cdot (k + l)$$

Similarly for multiplication,

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z}$$

where $(a + n\mathbb{Z})$ is referred to as the "coset of a."

Example Is $a = 743126882431$ divisible by 9? Note that a is divisible 9 if and only if $a + 9\mathbb{Z} = 0 + 9\mathbb{Z}$. What is a?

$$a = 1 \cdot 10^0 + 3 \cdot 10^1 + 4 \cdot 10^2 + \ldots + 7 \cdot 10^{11}$$

$10 \equiv 1$, mod 9. So, $100 \equiv 10 \cdot 10 \equiv 1 \cdot 1 = 1$ and $10^k = 10^{k-1} \cdot 10 \equiv 1 \cdot 1 = 1$. Note that we call "$\equiv$" congruent. So,

$$a \equiv 1 \cdot 1 + 3 \cdot 1 + 4 \cdot 1 + \ldots + 7 \cdot 1$$

$a = 49$ which is the class 4. So the class/coset of a is the class of 4, not the class of 0 which is the condition that needs to be met to be divisible by 9. Therefore, 9 does not divide a.

Fact An integer is divislbe by 9 if and only if the sum of its digits in decimal expansion expansion is divisible by 9.

a is divisble by 11 if and only if the alternating sum of the digits is divisible by 11.

Example Divisibility by 7. $10^0 = 1 \equiv 1$, $10^1 = 10 \equiv 3$, $10^2 = 100 \equiv 2$, $10^3 \equiv 6$, $10^4 \equiv 4$, $10^5 \equiv 5$, $10^6 \equiv 1$. So, for example, if I take $7144285019 \equiv 3$.

GROUPS

Definition A group G is a set with an operation $\star$ such that 1.) $a \star b$ is in G, 2.) $a \star (b \star c) = (a \star b) \star c$ (associativity), 3.) there is a special element 1_G for which $a \star 1_G = a$ and $a = 1_G \star a$ (identity), 4.) for all $a \in G$ there is an "inverse" b such that $a \star b = 1_G = b \star a$ (of course as a changes so does b).

January 20, 2009

Note that in most discussion, $\star$ is merely a placeholder for an operation. In many examples, the star will be replaced with a real arithmetic operation. Recall that $(G, \star)$ is a group if and only if

- G is a set with a binary operation $\star : G \star G \to G$
- slt $(ab)\,c = a\,(bc)$
- $\exists 1_G \in G$ with $1_G \cdot g = g \cdot 1_G = g \forall g$
- $\forall g \in G \exists g^{-1}$ with $gg^{-1} = 1$

Examples

- $(\mathbb{Z}, +)$; know: $a + (b + c) = (a + b) + c$, identity $=$ 0, inverse $=$ negative.

- $(\mathbb{Z}/n,+)$; $\mathbb{Z}/n = \{0+n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$, where $i{+}n\mathbb{Z} = \{\ldots, i-2n, i-n, i, i+n, i+2n, \ldots\}$ and $(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $+$; identity $= 0$; inverse $=$ negative

- $(\mathbb{Q}\setminus\{0\}, \times)$; we know $a(bc) = (ab)c$; identity $= 1$; inverse $=$ inverse (note: $a \neq 0$, $b \neq 0 \Rightarrow ab \neq 0$).

- Similarly, $(\mathbb{R}\setminus\{0\}, \times)$, $(\mathbb{C}\setminus\{0\}, \times)$

- Let G be a group such as $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$. Let $G^{m,n}$ be the $m \times n$ matrices with entries in G. $(G^{m,n},+)$ is a group. Identity $= m \times n$ matrix of zeros; inverse $=$ matrix with "negatived" entries.

- Let $GL(n,\mathbb{Q}) = n \times n$ matrices with rational entries, with matrix multiplication as operation, and with det $\neq 0$. We know that $A(BC) = (AB)C$; identity $=$ indentity matrix; inverse $=$ matrix inverse

- **Symmetry groups**: Consider an equilateral triangle with vertices a, b, c.

Let's consider the collection of all rigid motions that transform the triangle into itself. These are: [1] 2 rotations by 120^o, l and r, [2] not doing anything, call it 1, [3] 3 flips, where each flips fixes one of the corners a, b, or c and flips the triangle on the axis drawn from the triangle vertex perpendicular to the opposing side. Together they form symmetry $\mathrm{sym}(\triangle) = \{1, l, r, a, b, c\}$. This is all of the possibilities, because $3! = 6$. We make this a group by composing motions.

Multiplication table for $\mathrm{sym}(\triangle)$, where the $i-j$ entry $= i \star j$:

	1	**r**	**l**	**a**	**b**	**c**
1	1	r	l	a	b	c
r	r	l	1	b	c	a
l	l	1	r	c	a	b
a	a	c	b	1	l	r
b	b	a	c	r	1	l
c	c	b	a	l	r	1

Note that in each row and each column, each element shows exactly once. Why? In any column we are looking at products of the form $g \times g_o$, where g_o is the column index and g runs through the group. What this means is that g_o represents the column and g represents the row.

Suppse that some element x does not show in this column. This means that some other element shows at least twice. What this tells us is for some g_o and two different g I get the same result, call it y. $gg_o = y \Rightarrow g\left(g_o g_o^{-1}\right) = y g_o^{-1}$, or $g = y g_o^{-1}$, similarly $g' = y g_o^{-1}$. We can conclude then that $g = g'$and thus nothing can be repeated, and nothing is missing.

Note that in many cases,

$$g \times g' \neq g' \times g$$

Multiplication tables are symmetric if and only if $gg' = g'g$ in all cases.

Definition $(G, \times)$ is *Abelian* (commutative) if the multiplication table is symmetric (means: you can reorder factors in a product.)

Abelian $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$; vector spaces, $(G^{m,n}, +)$ where $G = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$; $(\mathbb{Z}/n\mathbb{Z}, +)$

Non-Abelian sym$(\triangle)$; most symmetry groups; $G|(\mathbb{Q}, n)$ and $G|(\mathbb{R}, n)$, $Gl(\mathbb{C}, n)$.

Case study on inverting mod(n). Zeros are not admissable!

$n = 2$: $1 + 2\mathbb{Z}$ = odd numbers.

Question Can we make $\{1 + 2\mathbb{Z}\}$ at multiplicative group? Yes.

	1
1	1

$n = 3$: $1 + 3\mathbb{Z}$; $2 + 3\mathbb{Z}$

	1	**2**
1	1	2
2	2	1

$n = 4$: $\bar{1} = 1 + 4\mathbb{Z}$, $\bar{2}$, $\bar{3}$, $\bar{4}$

	1	**2**	**3**
1	1	-	3
2	-	-	-
3	3	-	1

In general, starting with $\mathbb{Z}/n\mathbb{Z}$, remove $\bar{0}$ and all cosets of numbers that have a common gcd with n. If we do this, we are left with a set called $U(u)$ or $(\mathbb{Z}/n\mathbb{Z})^{\times}$ (the "units mod n"). Why do they make a group?

- If $\gcd(a, n) = \gcd(b, n) = 1$, then $\gcd(a \star b, n) = 1$. So $U(u) \cdot U(n) \subseteq U(n)$.
- Associativity follows from $\mathbb{Z}$ group.
- Identity: $1 + n\mathbb{Z}$
- Inverse: assuming $\gcd(a, n) = 1$ we need a b with $\gcd(b, n) = 1$ and $\bar{a} \cdot \bar{b} = \bar{1}$.

Recall Euclidian algorithm and its consequence,

$$\gcd(\alpha, \beta) = x\alpha + y\beta$$

with $x, y \in \mathbb{Z}$. So, $1 = xa + yn$; thus $\bar{x}\bar{a} = \bar{1} - \overline{yn}$, $\bar{x} = \bar{a}^{-1}$ and $\overline{yn} = \bar{0}$.

January 22, 2009

PERMUTATIONS

Definition Given n labelled objects such as $\{1, \ldots, n\}$, a permutation (on n elements) is an ordering of these n objects.

Note There are $n! = n(n-1)(n-2)\ldots 2 \cdot 1$ such permutations. The ways of writing permutations: standard notation (5,4,1,2,3) or []; cycle notation (1,5,3)(2,4)

Note Irredundant cycle notation if and only if each number/object occurs precisely once. Redundant if not irredundant.

Example What is the composition of permutations from right to left of $(1, 2, 3)$?

$$(1, 2, 3) \stackrel{(1,3)}{\rightarrow} (3, 2, 1) \stackrel{(1,2)}{\rightarrow} (2, 3, 1)$$

This operation is written as (12) (13). The order of a permutation. Suppose we fix one permutation (1,4,5)(2,3) $= \sigma$. After two executions of this permutation, we have (1,4,5)(2,3)(1,4,5)(2,3) = (1,5,4)

Definition The **order of a permutation** σ is the smallest number $\text{ord}(\sigma) \geq 1$ such that $\text{ord}(\sigma)$ iterations of σ combine to the identity permutation.

Example $\text{ord}((1, 4, 5)(2, 3)) = 6$.

Theorem Suppose σ is given in irredundant cycle notation, $\sigma = c_1 \cdot c_2 \cdot \ldots \cdot c_k$. Let l_i be the length of cycle c_i. Then $\text{ord}(\sigma) = \text{lcm}(l_1, \ldots, l_k)$.

Remark Book says "disjoint cycle notation" for "irredundant cycle notation."

Definition A **transposition** is a 2-cycle.

Theorem Any permutation can be achieved by a composition of 2-cycles (not disjoint usually).

Proof We need to show that any cycle is a composition of 2-cycles. Use induction: let l be the length of the cycle. $(a) = (l, a)(l, a)$, so $l = 1$. For $l = 2$, there is nothing to do. For $l > 2$:

$$(a_1, a_2, a_3, \ldots, a_l) = (a_1, a_3, a_4, \ldots, a_l)(a_1, a_2)$$

Question Given σ, how many 2-cycles can be used to write σ as their product? This is a bad question because $\sigma = \sigma(1, 2)(1, 2) \cdots$. A better question would be, can we say anything about the number of 2-cycles used to produce σ?

Definition The **disorder** of σ is the number of pairs $\{i, j\}$ with $1 \leq i < j \leq n$, such that $\sigma(i) > \sigma(j)$.

Example If $\sigma(1, 2, 3, 4, 5) =$ 2,4,5,1,3. $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 5$, $\sigma(4) = 1$, $\sigma(5) = 3$.

Pair	In order after σ?
1,2	yes
1,3	yes
1,4	no
1,5	yes
2,3	yes
2,4	no
2,5	no
3,4	no
3,5	no
4,5	yes

Definition σ is *odd* (-1) if its disorder is odd, and *even* (+1) if its disorder is even. The "parity" of σ.

Note Any 2-cycle is odd. For the order 1 2 $3 \ldots i \ldots j \ldots n$ permutes to 1 $2 \ldots j \ldots i \ldots n$. Who is out of order? Even: all pairs of numbers (a, i) with $i < a < j$; all pairs of numbers $(a, j)$with $i < a < j$. The collection of all permutations falls into even and odd choices. Every 2-cycle is odd.

Fact Suppose you compose 2 permutations σ and τ. The parity of the product behaves as follows,

	σ odd (-1)	σ even (+1)
τ odd (-1)	even (+1)	odd (-1)
τ even (1)	odd (-1)	even (+1)

"Parity is a homomorphism, it respects products." In particular, the number of even and odd permutations is the same. Taking any permutation and composing it with two $\bullet (1, 2)$ yields identity.

Definition The collection of all permutations of n elements is called the **symmetric group** S_n.

January 27, 2009

SUBGROUPS

Suppose that $(G, \star)$ is a group, we want to study the existence and structure of subsets of G that are groups in their own right.

	1	r	l	a	b	c
1	1	r	l	a	b	c
r	r	l	1	b	c	a
l	l	1	r	c	a	b
a	a	c	b	1	l	r
b	b	a	c	r	1	l
c	c	b	a	l	r	1

Find the sym($\triangle$). Recall that to be a group, the following conditions must be met:

- $H \star H \subseteq H$
- Associative
- H should contain 1
- for $h \in H$, H should contain h^{-1}

Subgroups

- $\{1\}$
- $\{1, a, b, c, l, r\}$
- $\{1, l, r\}$
- $\{1, a\}$, $\{1, b\}$, $\{1, c\}$
- $\{1, a, b, l, c, r\}$

To find the sym($\triangle$): $\{1\}$, G, $\{1, l, r\}$, $\{1, a\}$, $\{1, b\}$, $\{1, c\}$

Definition A group G is called cyclic if it can be viewed as the collection of all powers of a single element g.

Example Which groups are cyclic? $\{1\} = \langle 1 \rangle$, $\{1, a\} = \langle a \rangle$, $\{1, b\} = \langle b \rangle$, $\{1, c\} = \langle c \rangle$, $\{1, l, r\} = \langle l \rangle = \langle r \rangle$. On the other hand, we conclude that G is not cyclic. G needs 2 generators for example a and b.

Lemma If $g \in (G, \star)$, then its $\langle g \rangle$powers for a subgroup.

Proof Notation: let $g^k = g \cdot \ldots \cdot g$. We need to show that [1] $\langle g \rangle$ is closed under $\times$, [2] $1 \in \langle g \rangle$, and [3] each element of $\langle g \rangle$ has an inverse in $\langle g \rangle$. To [1] $g^k \cdot g^l = g^{k+l}$, [2] take g^0=1, and [3] the inverse to g^k is g^{-k}. Note that $g^{-k} = \left(g^{-1}\right)^k$.

Example $(G, \star) = (\mathbb{Z}, +)$. $\langle 2 \rangle$=$\{\ldots, -4, -2, 0, 2, \ldots\}$.

Recall ord(g)= smallest positive k, such that $g^k = 1$. If no such k exists, then ord$(g) = \infty$.

Example sym($\triangle$), ord$(a) = 1$, ord$(l) = 3$, ord$(1) = 1$, in $(\mathbb{Z}, +)$, ord$(2) = \infty$.

Lemma Suppose ord$(g) < \infty$, then $\left\{k \in \mathbb{Z} | g^k = 1\right\}$= $\mathbb{Z} \cdot \operatorname{ord}(g)$.

Example In sym($\triangle$) ,$\left\{k \in \mathbb{Z} | l^k = 1\right\}$=$3 \cdot \mathbb{Z}$

Proof Let k be such that $g^k = 1$. By Euclid, $k = q \cdot \operatorname{ord}(g) + r$, $0 \leq r <$ ord(g). So, $1 = g^k = g^{q \cdot \operatorname{ord}(g) + r}$= $\left[g^{\operatorname{ord}(g)}\right]^q \cdot g^r$= $1 \cdot g^r \Rightarrow g^r = 1$. As $r <$ord(g), we much have $r = 0$, therefore, $k = q \cdot \operatorname{ord}(g)$.

Lemma $g^i = g^j$ if and only if $i - j$ is a multiple of ord(g).

Proof If $g^i = g^j$, then $g^{i-j} = 1$ and so if $i - j$ is divisible by the ord(g). Conversely, if $i - j$ is divisible by ord(g)then $i = j + n \cdot \operatorname{ord}(g)$ and so $g^i = g^{j + n \cdot \operatorname{ord}(g)}$= $g^j \cdot \left(g^{\operatorname{ord}(g)}\right)^n = g^j$.

Theorem Pick $g \in (G, \star)$. Then either $\mathrm{ord}(g) = \infty$ and $\langle g \rangle$ is not quite equal $(\mathbb{Z}, +)$ or $\mathrm{ord}(g) = k < \infty$ and $\langle g \rangle$ is not quite equal to $(\mathbb{Z}/k\mathbb{Z}, +)$. In both cases, the identification is

$$g^n \leftrightarrow n \text{ (or } n \mathrm{mod} k\mathbb{Z})$$

$$g^n \cdot g^m = g^{n+m} \leftrightarrow n + m$$

This is know as the **morphism law**.

Example In sym($\triangle$), $\langle a \rangle$ supposedly equals $(\mathbb{Z}/2\mathbb{Z}, +)$.