

MATH 113 HW 4: Subgroups, cyclic groups

Due in class on Thursday, September 28.

1. For each of the following statements, provide either a proof or a counterexample.

a) Let G be a group, and $a, b \in G$. If $(ab)^n = e$, then $(ba)^n = e$.

SOLUTION:

First note that if $(ab)^n = e$, then $e = (ab)^n(ab)^{-n} = (ab)^{-n}$. So we may assume that n is positive.

$$\begin{aligned}(ba)^n &= (a^{-1}aba)^n \\ &= (a^{-1}aba)(a^{-1}aba) \dots (a^{-1}aba) \\ &= (a^{-1}ababa(a^{-1}aba) \dots (a^{-1}aba) \\ &= (a^{-1}abababa)(a^{-1}aba) \dots (a^{-1}aba) \\ &= \vdots \\ &= a^{-1}(ab)^n a \\ &= a^{-1}ea \\ &= a^{-1}a \\ &= e\end{aligned}$$

(b) An element a of a group G has order n if and only if $a^n = e$ in G .

SOLUTION:

(Counterexample) Let $G = \mathbb{Z}_8$ and $a = 4$. Then $a^4 = a + a + a + a = 4 + 4 + 4 + 4 = 0 \pmod{8}$ but a has order 2.

(c) Every abelian group is cyclic.

SOLUTION:

(Counterexample) Let $G = \mathbb{Z}_3 \times \mathbb{Z}_3$. We saw in class this is not cyclic, but it is certainly abelian: $(a, b) \star (c, d) = (ac, bd) = (ca, db) = (c, d) \star (a, b)$.

(d) Every cyclic group of order > 2 has at least two distinct generators.

SOLUTION:

Let $G = \langle a \rangle$, where $a \neq e$. Since G has order greater than 2, $a^{-1} \neq a$. The group $\langle a^{-1} \rangle$ is equal to $\langle a \rangle$, since $(a^{-1})^{-1} = a \in \langle a^{-1} \rangle$.

2. Prove that if H is a finite subset of a group G and H is closed under multiplication, then H is a subgroup of G .

SOLUTION:

Let $a \in H$. Then $a^n = e$ for some $n \in \mathbb{Z}^+$. (Otherwise $\langle a \rangle$ would be an infinite subset of H , a finite set.) So $a^{-1} = a^{n-1}$. So the identity is in H , and $a^{-1} = a^{n-1} \in H$. So the inverse of a is in H . Since H is a closed subset of G with identity and inverses, H is a subgroup of G .

3. Prove that if $n \in \mathbb{Z}^+$, then $n^3 - n$ is divisible by 3.

SOLUTION:

Base case: Let $n = 1$. Then $1^3 - 1 = 0$ is divisible by 3.

Inductive Step: Assume $k^3 - k$ is divisible by 3. Then $k^3 - k = 3j$ for some $j \in \mathbb{Z}$. We want to show $(k+1)^3 - (k+1)$ is divisible by 3.

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^2 + 2k + 1)(k+1) - k - 1 \\ &= k^3 + 2k^2 + k + k^2 + 2k + 1 - k - 1 \\ &= k^3 + 3k^2 + 2k \\ &= k^3 - k + 3k^2 + 3k \\ &= (k^3 - k) + 3k^2 + 3k \\ &= 3j + 3(k^2 + k) \\ &= 3(j + k^2 + k)\end{aligned}$$

So 3 divides $(k+1)^3 - (k+1)$.

4. (a) Find all subgroups of \mathbb{Z}_{60} , their orders, and their generators.

SOLUTION:

(a) The generators of \mathbb{Z}_{60} are all the elements which are relatively prime to 60 by Corollary 6.16. Therefore any element relatively prime to $60 = 2 * 2 * 3 * 5$ will generate all of \mathbb{Z}_{60} .

The smallest element of \mathbb{Z}_{60} which is not relatively prime to 60 is 2. Therefore the subgroup $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, \dots, 56, 58\}$ has order 30 and is generated by the elements of the form $2h$, where h is relatively prime to 30. So the generators are $\{2, 14, 22, 26, 34, 38, 46, 58\}$.

Next consider $\langle 3 \rangle = \{0, 3, 6, 9, \dots, 54, 57\}$. This group has order 20 and is generated by elements of the form $3h$, where h is relatively prime to 20. Therefore the generators are $\{3, 9, 21, 27, 33, 39, 51, 57\}$.

$\langle 4 \rangle = \{0, 4, 8, 12, 16, 20, \dots, 48, 52, 56\}$, which has order 15. The generators are $\{4, 8, 16, 28, 32, 44, 52, 56\}$.

$\langle 5 \rangle = \{0, 5, 10, 15, 20, \dots, 45, 50, 55\}$, which has order 12. The generators are $\{5, 25, 35, 55\}$.

$\langle 6 \rangle = \{0, 6, 12, 18, 24, \dots, 42, 48, 54\}$, which has order 10. The generators are $\{6, 18, 42, 54\}$.

The positive integers which we have not yet appeared as generators are $\{10, 12, 15, 20, 24, 30, 36, 40, 45, 48, 50\}$

$\langle 10 \rangle = \{0, 10, 20, 30, 40, 50\}$, which has order 6. The generators are $\{10, 50\}$.

$\langle 12 \rangle = \{0, 12, 24, 36, 48\}$, which has order 5. Every element is a generator.

$\langle 15 \rangle = \{0, 15, 30, 45\}$, which has order 4. The generators are $\{15, 45\}$.

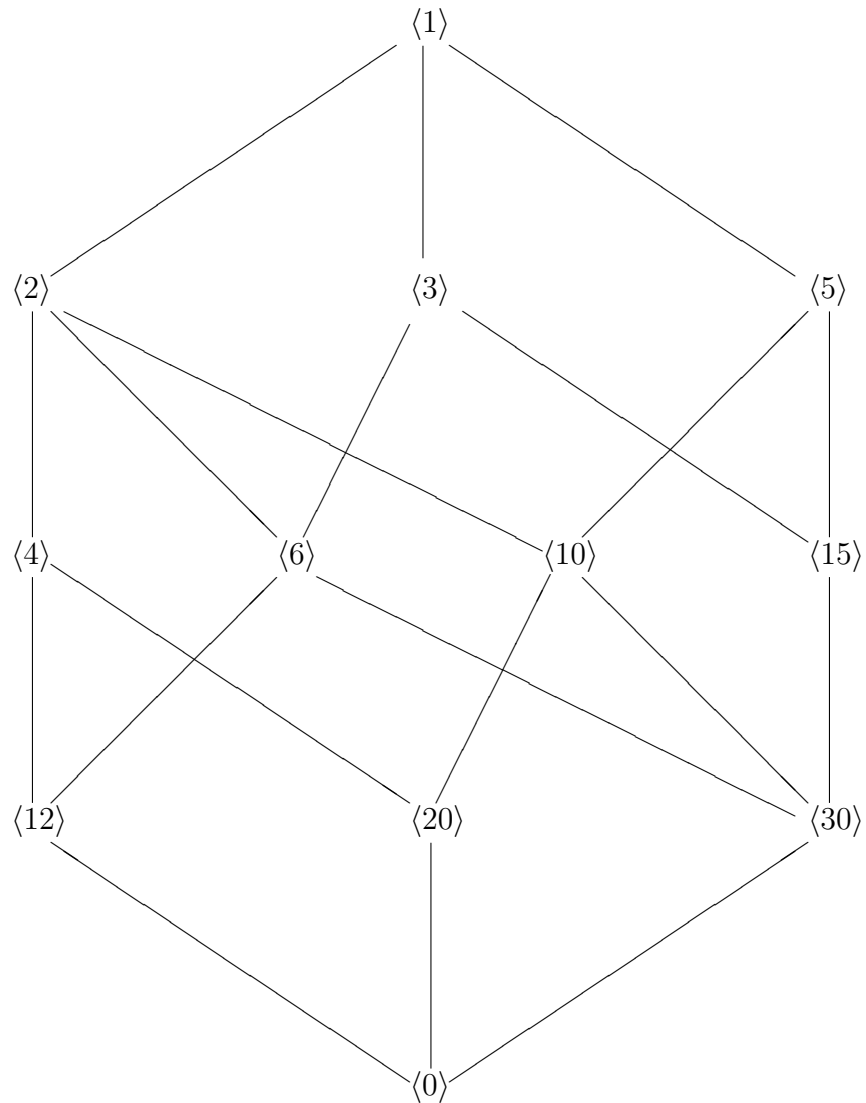
$\langle 20 \rangle = \{0, 20, 40\}$, which has order 3. The generators are $\{20, 40\}$.

$\langle 30 \rangle = \{0, 30\}$, which has order 2 and just one generator 30.

Since every element appears as the generator for one of these subgroups, the above listed groups, the trivial subgroup, and the improper subgroup are all the possible subgroups of \mathbb{Z}_{60} .

(b) Draw the subgroup diagram for \mathbb{Z}_{60} . (Note: It is okay for the lines to cross, as long as it is clear what the lines are connecting.)

SOLUTION:



5. Let $p, q \in \mathbb{Z}^+$ be two different prime numbers.

(a) How many generators are there for the group \mathbb{Z}_{pq} ? (Explain your answer.)

SOLUTION:

The generators of \mathbb{Z}_{pq} are the elements which are relatively prime to pq . These are all the elements except multiples of p and multiples of

q . There are q multiples of p and p multiples of q , with $pq = 0$ being double counted. Therefore there are $p + q - 1$ non-generators.

Since there are pq total elements, the number of generators is $pq - p - q + 1$.

(b) How many generators are there for the group \mathbb{Z}_{p^2} ? (Explain your answer.)

SOLUTION:

Again, we will count the non-generators. There are p elements which are multiples of p in \mathbb{Z}_{p^2} , so there are $p^2 - p$ generators.

6. Use the Euclidean Algorithm to find the greatest common divisor of the following pairs of integers.

(a) 24 and 9.

SOLUTION:

$$\begin{aligned}24 &= 2 * 9 + 6 \\9 &= 1 * 6 + 3 \\6 &= 2 * 3\end{aligned}$$

So $\gcd(24, 9) = 3$.

(b) 11391 and 5673.

SOLUTION:

$$\begin{aligned}11391 &= 2 * 5673 + 45 \\5673 &= 126 * 45 + 3 \\45 &= 15 * 3\end{aligned}$$

So $\gcd(11391, 5673) = 3$.

(c) 116 and -84 .

SOLUTION:

$$116 = -2 * (-84) + 52$$

$$-84 = -2 * 52 + 20$$

$$52 = 2 * 20 + 12$$

$$20 = 1 * 12 + 8$$

$$12 = 1 * 8 + 4$$

$$8 = 2 * 4$$

So $\gcd(116, -84) = 4$.