Noah Casey

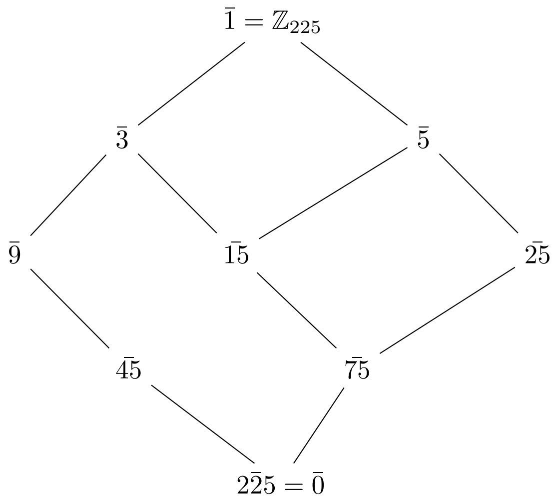
MATH 4720

Homework 3

1 For the group $\mathbb{Z}_{225}$, using bar notation, e.g. $\bar{5}$ for the element in $\mathbb{Z}_{225}$:

a Draw a subgroup diagram. Cite the theorem that allows for this to be done easily.

The theorem that allows for easy diagramming of subgroups (particularly in $\mathbb{Z}_{225}$) is Theorem G9 (ii), which states that for a cyclic group of order n, there is a one-to-one correspondence between the positive divisors of n and the set of subgroups. Hence, the positive divisors of 225 correspond to the subgroups of $\mathbb{Z}_{225}$ as the group is cyclic and of order 225.



b How many subgroups of order 15 are there? Explain briefly.

By Theorem G9 (ii), if k is a divisor of 225, then there is a unique subgroup of order $\frac{225}{k}$. If $k = 15$, then the order of the subgroup generated by k is 15. Thus, there is a single subgroup that has order 15.

c Find all of the elements that generate a subgroup of order 15.

By Theorem G9 (i), ka (additive notaion) is a generator of a group of order n if and only if $\gcd(k, n) = 1$. Hence, the k-values that generate a subgroup of order 15 must be relatively prime to 15. These are $k = \{1, 2, 3, 4, 7, 8, 11, 13, 14\}$, hence, as (we know $a = 15$ as $\bar{1}5 isageneratorofthesubgroupoforder 15 from (b)$,k15={15,30,45,60,105,120,165

2 Let G be a group with $a \in G$. Show that $o(a) = o(a^{-1})$:

Let G be finite, then $o(a) = n$ if and only if $a^n = e$, so $(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$ and $o(a^{-1}) = n$.

Now let G be an infinite group. Note that $o(a) = \infty$, so $a^n \neq e$ for any $n \in \mathbb{N}$. Now assume that $o(a^{-1}) = n$ for some $n \in \mathbb{N}$. This may be the case only if $a^n = e$ or $a^{-1} = e$. We know that the former is false as $o(a) = \infty$, so for the statment to be true, it must be the case that $a^{-1} = e$. However, $ae = a$, so this is false. Hence, $o(a^{-1}) = \infty$.

3 Show that $S_n = \langle (1\ 2), (1\ 3), ..., (1\ n) \rangle$.

We proceed by induction on arbitrary m-cycles.

Base Cases: let $m = 2$ such that we have the cycle $(a_1\ a_2)$, then this can be written as $(1\ a_1)(1\ a_2(1\ a_1))$. Now let $m = 3$, then some cycle $(a_1\ a_2\ a_3)$ may be written as $(1\ a_3)(1\ a_2(1\ a_1)(1\ a_3))$. Both of these cases give cycles as products of transpositions of the form desired.

Induction step: Now assume that some m-cycle may be written as

$$(1\ a_m)(1\ a_{m-1}) \dots (1\ a_2)(1\ a_1)(1\ a_m).$$

It remains to show that some $m + 1$-cycle can be written in a similar fashion. All we need to do is extend the m-cycle to account for this extra a_{m+1}. We know that a_{m+1} must be mapped to a_1, so we can replace the rightmost a_m with a_{m+1}. Now, we need a_m to map to a_{m+1}, so we append an a_{m+1} to the left of a_m in the cycle. The rest of the mappings are uncahnging between the two cycles, so the $m + 1$-cycle may be written as

$$(1\ a_{m+1})(1\ a_m)(1\ a_{m-1}) \dots (1\ a_2)(1\ a_1)(1\ a_{m+1}).$$

4 Let $\tau = (a_1\ a_2\ ...\ a_k)$ be a k-cycle in S_n.

a Prove that if σ is any permutation in S_n, then $\sigma\tau\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ ...\ \sigma(a_k))$.

Set $\{\sigma(a_1), \sigma(a_2), ..., \sigma(a_k)\} \in \{1, ..., n\}$. Then

$$\sigma\tau\sigma^{-1}(\sigma(a_1)) = \sigma\tau(a_1) = \sigma(a_2).$$

Now take some $a_i \in \{a_1, a_2, ..., a_k\}$. We have that

$$\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma\tau(a_i) = \sigma(a_{i+1}).$$

If $i = k$, then $i + 1 = 1$ as τ maps a_k to a_1. Now take some $m \notin \{a_1, a_2, ..., a_k\}$. Note that $\sigma\tau\sigma^{-1}(\sigma(m)) = \sigma\tau(m) = \sigma(m)$ as τ fixes m, so $\sigma\tau\sigma^{-1}$ fixes $\sigma(m)$.

b Let μ be a k-cycle. Prove that there is a permutation σ such that $\sigma\tau\sigma^{-1} = \mu$.

Assume that $\mu = (\mu_1\ \mu_2\ ...\ \mu_k)$ where $\{\mu_1, \mu_2, ..., \mu_k\} \in \{1, ..., n\}$. As we know from (a), $\sigma\tau\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ ...\ \sigma(a_k))$; thus if we set $\sigma(a_i) = \mu_i$ and fix all letters not in $\{a_1, ..., a_k\}$, then we have found a σ that satisfies the condition.

More precisely, we may set $\sigma = (a_1\ \mu_1)(a_2\ \mu_2)\dots(a_k\ \mu_k)$. This function takes any a_i and maps it to μ_i. We now handle the case in which we have cycles in the product of the form $(a_i = \mu_j\ \mu_i)\dots(a_j\ \mu_j)$. Note that if this is the case, then a_j is sent to μ_i, which is undesirable. However, if we flip the order of these transpositions to $(a_j\ \mu_j)\dots(a_i = \mu_j\ \mu_i)$, then we see that a_i is mapped to μ_i and a_j is mapped to μ_j as desired. Flipping the order of any cycles of this form gives the desired σ as

$$\mu(\sigma(a_i)) = \mu(\mu_i) = \mu_{i+1}$$

and

$$\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma\tau(a_i) = \sigma(a_{i+1}) = \mu_{i+1}.$$

5 Find all of the left and right cosets of $H = \langle(1\ 2\ 3)\rangle$ in S_4.

If you had to find the left and right cosets in S_5, how many of each would there be?

We see that $H = \{(1\ 2\ 3), (1\ 3\ 2), id\}$, so the cosets are as follows.

Left cosets	**Right cosets**
$idH = H$	$Hid = H$
$(1\ 2)H = \{(1\ 2), (2\ 3), (1\ 3)\}$	$H(1\ 2) = \{(1\ 2), (2\ 3), (1\ 3)\}$
$(1\ 4)H = \{(1\ 4), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4)\}$	$H(1\ 4) = \{(1\ 4), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}$
$(2\ 4)H = \{(2\ 4), (1\ 4\ 2\ 3), (1\ 3\ 4\ 2)\}$	$H(2\ 4) = \{(2\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4)\}$
$(3\ 4)H = \{(3\ 4), (1\ 2\ 4\ 3), (1\ 4\ 3\ 2)\}$	$H(3\ 4) = \{(3\ 4), (1\ 2\ 3\ 4), (1\ 3\ 4\ 2)\}$
$(1\ 2\ 4)H = \{(1\ 2\ 4), (1\ 4)(2\ 3), (1\ 3\ 4)\}$	$H(1\ 2\ 4) = \{(1\ 2\ 4), (1\ 3)(2\ 4), (2\ 4\ 3)\}$
$(1\ 4\ 2)H = \{(1\ 4\ 2), (2\ 3\ 4), (1\ 3)(2\ 4)\}$	$H(1\ 4\ 2) = \{(1\ 4\ 2), (1\ 4\ 3), (1\ 4)(2\ 3)\}$
$(1\ 4\ 3)H = \{(1\ 4\ 3), (1\ 2)(3\ 4), (2\ 4\ 3)\}$	$H(1\ 3\ 4) = \{(1\ 3\ 4), (2\ 3\ 4), (1\ 2)(3\ 4)\}$

Also note that each coset $aH = bH = cH = \{a, b, c\}$, so each coset above may be relabeled using any of the elements in the set.

In S_5, there are 5! elements. Each coset of H has a size of 3, and as cosets are equivalence relations, they parition the set. Hence, there will be $\frac{5!}{3} = 40$ left cosets of H in S_5; likewise, there will be 40 right cosets.

6 Do the computations without need for a calculator

a Use FLT to "primality test" the number 35 for primeness

Note that 35 does not divide 6, so we may use $a = 6$ as specified in Fermat's Little theorem. If 35 is a candidate for a prime number, then $6^{34} \equiv 1 \pmod{35}$. We see that $6^2 = 36 \equiv 1 \pmod{35}$, so $6^{34} \equiv (6^2)^{17} \equiv 1^{17} \equiv 1 \pmod{35}$. Thus, we cannot claim that 35 is not prime based on FLT. However, the implication only claims that if 35 is prime, then $6^{34} \equiv 1 \pmod{35}$, but the implication doesn't go the other way, so we cannot say with certainty that 35 is prime (in fact, one can see that it is not).

b Verify that Euler's theorem holds for $n = 35$ and $a = 2$

Clearly, $\gcd(35, 2) = 1$ as 2 does not divide 35. Thus, by Euler's theorem, $2^{\varphi(35)} \equiv 1 \pmod{35}$. We verify this by first determining $\varphi(35)$. Recall that the Euler-phi function with $n = 35$ is defined as $\varphi(35) = |\{k | \gcd(k, 35) = 0\}|$ where $1 \leq k < 35$. The set of numbers less than 35 that are relatively prime with 35 are $\{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$ and the size of this set is 24. Thus, $\varphi(35) = 24$ and it must be the case that $2^{24} \equiv 1 \pmod{35}$. We verify this by noting that $2^{24} \equiv (2^3)^8 \equiv (8)^8 \equiv (8^2)^4 \equiv 64^4 \equiv 29^4 \equiv (-6)^4 \equiv 36^2 \equiv 1^2 \equiv 1 \pmod{35}$. Thus, Euler's theorem holds for $n = 35$ and $a = 2$.

7 Let G be a finite group. Suppose G has subgroups of order 8, 90, and 220. What can you say about the order of G?

By Corollary G14 (Lagrange's Theorem), the order of subgroup H of G divides the order of G. So, we can say that $|G|$ is a multiple of 8, 90, and 220. Furthermore, we may find the minimum order of G. Let $|G| = n$. As $90|n$, $n \geq 90$. However, $8 \nmid 90$, but 8 and 90 both divide 180, and this is the smallest number that both divide. Now since $220|n$, $n \geq 220$, but $180 \nmid 220$. Thus, we find the smalles number that both divide; note that both divide $(18)(22)(10)$ as $180|(180)(22)$ and $220|(18)(220)$. Thus, $|G| = (k18)(l22)(n10)$ for some $k, l, n \in \mathbb{N}$.

Sources

- Python: for confirming numerical computations.
- Stack Exchange: understanding why a permutation can be written as a product of transpositions.