Algebra 1 Homework 2
Lee Fisher
2017-09-02

- Page 22. #21: Let G be a finite group and x be an element of order n. Prove that if n is odd, then $x = x^(2k)$ for some k.

  Proof. If n is odd, then $n = 2m + 1$ for some non-negative integer m. Since x is of order n, this means $x^{2m+1} = 1$. We can multiply both sides by x on the left and arrive at $x^{2m+2} = x$, then by associativity $x^{2(m+1)} = 1$. We can set $k = m + 1$ and arrive at our conclusion. If x has odd order, then there will exist a k for which $x^{2k} = x$.

- Page 22. #25: Prove that if $x^2 = 1$ for all elements in G, then G is abelian.

  Proof. Consider two elements in G, a and b. We know $a^2 = 1$ and $b^2 = 1$. So consider two elements, a and b, and the element $(ab)^2$. We have $(ab)^2 = 1$ by definition, but also $(ab)^2 = abab = (ab)(ab)$. This means $(ab)^{-1} = ab$. We also have that $(ab)^{-1} = b^{-1}a^{-1}$, and since anything squared in G is the identity we know $a^{-1} = a$ and $b^{-1} = b$. Therefore $(ab)^{-1} = ba$ but also $(ab)^{-1} = ab$. Finally we have $ab = ba$ by transitivity.

- Page 22. #35: If x is an element of finite order n in G use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \dots x^{n-1}\}$.

  Proof. Let m be a number greater than n. By the division algorithm, $m = qn + r$ where $0 \leq r < n$. Then we have: $x^m = x^{qn+r} = (x^n)^q(x)^r = 1^q x^r = x^r$. Since $r < n$ we have $x^r \in \{1, x, x^2, \dots x^{n-1}\}$.

- Page 33. #6: Write down the cycle decomposition of every element in S_4.

  Okay: (1), (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (124), (132), (134), (142), (143), (234), (243), (1234), (1432), (1324), (1423), (1342), (1243).

- Page 33. #9: Before doing these problems I'll prove a lemma. The order of an m-cycle is m. Let $\sigma = (a_1, a_2, a_3, \dots a_m)$. Then for any i, $1 \leq i \leq m$, we have $\sigma(a_i) = a_{(i+1)\text{mod m}}$. Then extending we would have $\sigma^k(a_i) = a_{(i+k)\text{mod m}}$. This tells us that $|\sigma| = m$, because $\sigma^m(a_i) = a_{(i+m)\text{mod m}} = a_i$ and if $k < m$ then $(i + k)\text{mod m} \neq i$.

  - Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$. For which positive integers i is σ^i also a 12-cycle? Since σ has order 12 we can consider the cyclic subgroup generated by σ. This subgroup is isomorphic to $(\mathbb{Z}_12, +)$ with isomorphism $\phi : \sigma^k \to k\text{mod }12$. The question of how many powers of σ are 12-cycles is (by the lemma) the same as the question of how many generators there are of $\mathbb{Z}_12$. The numbers 1, 5, 7, and 11 will generate $\mathbb{Z}_12$. So, σ^1, σ^5, σ^7, and σ^11 will be 12-cycles.
  - Let $\tau = (1, 2, 3, 4, 5, 6, 7, 8)$. For which positive integers i is τ^i also an 8-cycle? For the same reasons as the last question σ^1, σ^3, σ^5, and σ^7 will all be 8-cycles.
  - Let $\omega = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14)$. For which positive integers i is ω^i also a 14-cycle? Again for the same reasons, σ^1, σ^3, σ^5, σ^9, σ^11, and σ^13 will all by 14-cycles.

- Page 33. #13: Show that an element has order 2 in S_n if and only if it's cycle decomposition is a product of commuting two cycles.

  Proof: $\to$ Suppose σ is an element of order 2. We know that σ is a product of commuting cycles. The order of each cycle is its length. This means that the order of σ is the least common multiple of the lengths of the commuting cycles that make up σ. Therefore, if the order of σ is 2 then the least common multiple of the cycles that make up σ must also be 2. This means σ is made up of only 2-cycles.

$\leftarrow$ Suppose σ is product of commuting 2-cycles. Then σ^2 is a product of commuting 2-cycles as well. In σ^2 every 2-cycle is repeated twice. Since the order of an m-cycle is m, and since the 2-cycles commute all the pairs of 2-cycles will cancel and we have the order of $|\sigma| = 2$.

- Page 36. #2: Write out the group tables for S_3, D_8 and Q_8.

Table 1: S_3

$\circ$	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

Table 2: D_8

$\circ$	R_0	R_{90}	R_{180}	R_{270}	V	H	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	V	H	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	V	H
R_{180}	R_{180}	R_{270}	R_0	R_{90}	H	V	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	H	V
V	V	D'	H	D	R_0	R_{180}	R_{90}	R_{270}
H	H	D	V	D'	R_{180}	R_0	R_{270}	R_{90}
D	D	H	D'	V	R_{270}	R_{90}	R_0	R_{180}
D'	D'	V	D	H	R_{90}	R_{180}	R_{90}	R_0

Table 3: Q_8

*	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1