MATH 375.14

## Class 14: Selected Answers

1. Suppose $\alpha, \beta \in S_{n}$. Prove that if $\alpha$ is even, then so is $\beta^{-1} \alpha \beta$.
2. Let $H$ be any subgroup of $S_{n}$. Prove: Either every element of $H$ is even or that exactly half the members of $H$ are even. Solution: If all the elements are even, done. Otherwise, let $\alpha$ be any odd permutation in $H$. You have shown in an earlier problem set that the mapping $f: H \rightarrow H$ by $f(\beta)=\alpha \beta$ is one-to-one and onto. [Caution: You need to use an odd permutation $\alpha$ in $H$ so that $\alpha \beta \in H$ by closure. An arbtrary odd permutation $\gamma$ from $S_{n}$ won't do because then we would not know whether $\gamma \beta \in H$.] But since $\alpha$ is odd, then $\beta$ is even $\Longleftrightarrow \alpha \beta=f(b)$ is odd. That is, $f$ maps the odd permuations to the even permutations of $H$ and vice versa. Therefore, there must be the same number of each.
3. a) What is the maximum order for an element in $S_{6}$ ? Solution: If $\alpha \in S_{6}$, then it can be written as a product of disjoint cycles, whose lengths sum to 6 (if we include 1-cycles for those elements fixed by $\alpha$ ). So the lengths of the disjoint cycles of such splittings are: [6], $[5,1],[4,2],[4,1,1],[3,3],[3,2,1]$, $[3,1,1],[2,2,2],[2,2,1],[2,1,1,1,1],[1,1,1,1,1,1]$. The maximum order of such a splitting (using Ruffini's Theorem) is 6 .
b) What about for $A_{6}$ ? Solution: The following are the even splittings: $[5,1],[3,3],[3,1,1],[1,1,1,1,1,1]$. The maximum order is 5 .
c) Find an element of $A_{8}$ of order 15. Solution: Use a [5,3] splitting: (12345)(678) will do.
d) Find an element of $A_{10}$ of order 21. Solution: Use a $[7,3]$ splitting: $(1234567(8,9,10)$ will do.
4. Let $\phi: \mathbf{R}^{2} \rightarrow \mathbf{R}$ by $\phi(a, b)=a b$. Determine whether $\phi$ is one-to-one and/or onto. Solutoin: $\phi$ is not injective because $\phi(1,0)=\phi(2,0)=0$. $\phi$ is onto. Let $x \in \mathbf{R}$. Then we must find $(a, b) \in \mathbf{R}^{2}$ so that $\phi(a, b)=x$. So we need $\phi(a b, b)=a b=x$. There are many choices, but the simplest is to let $(a, b)=(x, 1)$; then $\phi(x, 1)=x \cdot 1=x$.
5. Let $\phi: V_{4} \rightarrow V_{4}$ by $\phi(g)=g^{2}$ for all $g \in V_{4}$. Go back to your group table and actually figure out what $\phi(g)$ is for each element in $V_{4}$. Is $\phi$ injective? Surjective? Solution: Notice that $\phi(g)=g^{2}=e$ for all $g \in V_{4}$. So $\phi$ is neither injective nor surjective.

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
| :--- | :--- | :--- | :--- | :--- |
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

6. a) Let $\alpha=\left(a_{1} a_{2} \ldots a_{k}\right)$ be a $k$-cycle. Prove that $\alpha$ is odd if and only if $k$ is even. Solution: We saw in class that $\alpha=\left(a_{1} a_{k}\right) \ldots\left(a_{1} a_{3}\right)\left(a_{2} a_{1}\right)$ is a product of $k-1$ transpositions. Therefore, $\alpha$ is odd if and only if $k-1$ is odd if and only if $k$ is even.
b) Prove that $\alpha$ is odd if and only if $|\alpha|$ is even. Solution: As seen in class, the order of a $k$-cycle is just its length. So $|\alpha|$ is even if and only if $k$ is even and from the previous part $k$ is even if and only if $\alpha$ is odd.
c) OK, here's the hard part on the homework: Now let $\beta$ be any element of $S_{n}$. Prove that if $\beta$ is odd, then $|\beta|$ is even. Hint: First use Theorem 5.1. Then show at least one of the cycles must be even in length. Then use Ruffini's Theorem. Solution: We can write $\beta$ as a product of $n$ disjoint cycles, say $\beta=\alpha_{1} \alpha_{2} \cdots \alpha_{n}$. Let $k_{i}$ be the length of $\alpha_{i}$. First use a proof by contradiction to show that some $k_{i}$ is even in length. Assume not. Then by part (a), all the $k_{i}$ are odd, so all the $\alpha_{i}$ are even. So $\beta \in A_{n}$ and therefore $\beta$ is even. This contradicts that we are given that $\beta$ is odd. So some $k_{i}$ must be even. But then by Ruffini's Theorem,

$$
|b|=\operatorname{lcm}\left(k_{1} k_{2} \cdots k_{n}\right)
$$

must be even since $k_{i} \mid \operatorname{lcm}\left(k_{1} k_{2} \cdots k_{n}\right)$ and $k_{i}$ is even.

## Optional Mastery and Review Exercises

7. Let $G$ be a group and let $H$ be a subgroup of $G$. Let $a$ be some fixed element of $G$. Define the set $a H a^{-1}$ to be $\left\{a h a^{-1} \mid h \in H\right\}$. Show that $a H a^{-1}$ is a subgroup of $G$. Solution: Closure: Let $a h_{1} a^{-1}, a h_{2} a^{-1} \in$ $a H a^{-1}$. Then $h_{1}, h_{2} \in H$. So

$$
\left(a h_{1} a^{-1}\right)\left(a h_{2} a^{-1}\right)=a\left(h_{1} h_{2}\right) a^{-1} \in a H a^{-1} .
$$

because $H$ is a subgroup so $h_{h} h-2 \in H$. Inverses: Let $a h a^{-1} \in a H a^{-1}$. Must show ( $\left.a h a^{-1}\right)^{-1} \in a H a^{-1}$. But $h^{-1} \in H$. So

$$
\left(a h a^{-1}\right)^{-1}=a h^{-1} a^{-1} \in a H a^{-1} .
$$

8. Suppose $G$ is a group of order 16. If $G$ has 5 elements for which $x^{4}=e$, can $G$ be cyclic? Explain. Solution: If $G$ were cyclic of order 16, the elements whose order were were 4,2 and 1 would satisfy this condition. Now if $\langle y\rangle=G$, then these elements would be $y^{4}, y^{12}, y^{8}$, and $e$. So it is impossible.
9. Extra Credit: For those who have taken probability: Show that $A_{5}$ has 24 elements of order 5 and 20 elements of order 3. Solution: Note that the only elements of order 5 in $S_{5}$ are 5 -cycles. But all 5 -cycles are even, so all 5 -cycles are in $A_{5}$. There are, of course, $5=120$ ! ways to fill in the 5 -cycle ( $a_{1}, a_{2}, a_{3}, a_{4}, a_{5}$ ) with the numbers 1 through 5 . But notice that

$$
\left(a_{1}, a_{2}, a_{3}, a_{4}, a_{5}\right)=\left(a_{5}, a_{1}, a_{2}, a_{3}, a_{4}\right),
$$

and, in fact, there are 5 different ways to write ( $a_{1}, a_{2}, a_{3}, a_{4}, a_{5}$ ) as a 5 -cycle, depending on which element yo start with. So the number of 5 -cycles is $5!/ 5=4!=24$. Similarly, the only order 3 elements in $S_{5}$ are 3 -cycles which are even so in $A_{5}$. But a there are $5 \cdot 4 \cdot 3=60$ ways to fill in a 3 -cycle ( $a_{1}, a_{2}, a_{3}$ ) with the numbers 1 through 5 . Each such such cycle can be written 3 different ways so there are $60 / 3=20$ different such.

