339 Review answers [Proof #12 has an error!!]

1. G is cyclic $|G| = 42$.

Fact. There is a unique subgroup of size k when $k \mid |G|$.

Since $42 = 7\cdot 6 = 7\cdot 3\cdot 2$ There are groups of

size
42 $\langle a\rangle$
21 $\langle a^2\rangle$
14 $\langle a^3\rangle$
7 $\langle a^6\rangle$
6 $\langle a^7\rangle$
3 $\langle a^{14}\rangle$
2 $\langle a^{21}\rangle$
1 $\langle a^{42}\rangle = e$.

2. Fact in a cyclic group if $k \mid |G|$ then there are $\phi(k)$ elements of order k. [Does not depend on $|G|$].

Since $24 \mid 100!$ we have

$$\phi(24) = \phi(8\cdot 3) = \phi(2^3\cdot 3) = \phi(2^3)\cdot\phi(3) = 2^2(2-1)\times(3-1)$$
$= 8$ elements of order 24.

3. The Sec 1. The proper subgroups have order 6, 4, 3 or 2 and are

$\langle 2\rangle = \{2, 4, 6, 8, 10, 12 = 0\}$ $\langle 6\rangle = \{6, 12 = 0\}$.
$\langle 3\rangle = \{3, 6, 9, 12 = 0\}$
$\langle 4\rangle = \{4, 8, 12 = 0\}$

Notice there are $\phi(12) = 2\cdot(2-1)\times 2 = 4$ elements which have order 12 and are not in a proper subgroup.

4. a. $(1\,5\,7\,8\,9\,3\,6)(2\,4)$

b. $(1\,6)(1\,3)(1\,9)(1\,8)(1\,7)(1\,5)(2\,4)$

c. $(1\,5\,7\,8\,9\,3\,6)^{-1}(2\,4)^{-1}$ (disjoint commute).

$= (6\,3\,9\,8\,7\,5\,1)(4\,2)$

d. $|\sigma| = \underset{\text{lcm}}{\cancel{\text{prod}}}\,(c_i)$ where $\sigma = \underbrace{c_1 c_2 \cdots c_k}_{\text{disjoint}}$

$= \text{lcm}(7, 2) = 14.$

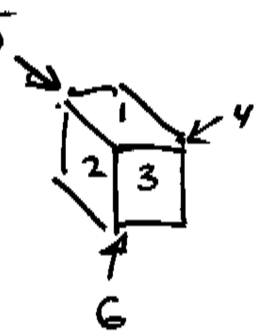
5. a. only a 3-cycle has order 3.

There are $4 \cdot 3 \cdot 2$ permutations of 4 elements with length 3

of these, each corresponds to 2 others

e.g. $(1\,2\,3) = (2\,3\,1) = (3\,1\,2)$

so there are $\dfrac{4 \cdot 3 \cdot 2}{3} = 8$ 3 cycles: $(1\,2\,3)$ $(2\,3\,4)$ $(1\,3\,2)$ $(2\,4\,3)$ $(1\,2\,4)$ $(1\,4\,2)$ $(1\,3\,4)$ $(1\,4\,3)$

6. 

$(1)(2\,3\,4\,5)(6) = (2\,3\,4\,5)$

$(1\,2\,6\,4)(3)(5) = (1\,2\,6\,4)$

$(1\,5\,6\,3)(2)(4) = (1\,5\,6\,3)$

7. Each $f(x)$ is 1-1 if $f'(x) > 0$ or $f'(x) < 0$.

all of a, b, c are 1-1

<u>But</u> c is not onto: Range $f(x) = [1, \infty)$ not $(0, \infty)$

so c fails.

However both a, b are isomorphisms as.

$$(ab)^3 = a^3 b^3 \quad \text{and} \quad \sqrt{(ab)} = \sqrt{a}\sqrt{b}$$

8. $T_g(a) = ga$ <u>so</u> consulting 5 we get.

a	$T_{(123)}(a)$
(123)	$(123)(123) = (132)$
(132)	$(123)(132) = e$
(124)	$(123)(124) = (13)(24)$ ⟵ not of order 3!
(142)	$(123)(142) = (143)$
(134)	$(123)(134) = (1)(234)$
(143)	$(123)(143) = (14)(23)$
(234)	$(123)(234) = (12)(34)$
(243)	$(123)(243) = (124)$

9. Z_9 is abelian so $aH = Ha$

$\langle 3 \rangle = \{0, 3, 6\}$. and $1 + \langle 3 \rangle = \{1, 4, 7\}$; $2 + \langle 3 \rangle = \{2, 5, 8\}$

10.
$$\begin{aligned}
5^{22} \bmod 7 &= 5^7 \cdot 5^7 \cdot 5^7 \cdot 5 \bmod 7 \\
&= 5^7 \bmod 7 \cdot 5^7 \bmod 7 \cdot 5^7 \bmod 7 \cdot 5 \bmod 7 \\
&= 5 \bmod 7 \cdot 5 \bmod 7 \cdot 5 \bmod 7 \cdot 5 \bmod 7 \\
&= 25 \bmod 7 \cdot 25 \bmod 7 \\
&= -3 \bmod 7 \cdot -3 \bmod 7 \\
&= 9 \bmod 7 \\
&= 2.
\end{aligned}$$

11, see #1. Notice here we don't know that a subgroup a certain size will automatically exist.

12. $G = D_5$ The subgroup generated by e, r, r^3, r^4 must be closed.

$$H = \langle r \rangle \quad \text{as} \quad H \supseteq \langle r \rangle \text{ and } \langle r \rangle \subseteq H.$$

But $\langle r \rangle = \{e, r, r^2, r^3, r^4\}$ since $r^5 = e$ in D_5

13. G = group generated by $\{\overset{a}{(13)(24)}, \overset{b}{(14)(23)}\}$

a) G must be closed so we multiply

$$(13)(24)(14)(23) = (12)(34)$$

~~But $(12)(34)a$ =~~

and $(14)(23)(13)(24) = (12)(34)$

Let a, b, c be the elements. Then $|a| = |b| = |c| = 2$

and $ab = ba = c$

finally $ac = aab = b$ and $bc = bba = a$ so closed.

So $|G| = 4$.

b) $\text{stab}_G(1) = \{e\}$ — no others

$\text{orb}_G(1) = \{1, 2, 3, 4\}$ as $e(1) = 1$ $c(1) = 2$ $a(1) = 3$ and $b(1) = 4$.

1. $|a| = n$ $\langle x^r \rangle \leq \langle x^s \rangle$ (x generates a).

<u>iff</u> $|x^r|$ divides $|x^s|$, as these are cyclic groups.

but $|x^r| = \dfrac{n}{\mathrm{lcm}(n,r)}$

So we need $\dfrac{n}{\mathrm{lcm}(n,r)} \Big| \dfrac{n}{\mathrm{lcm}(n,s)}$

2. Since $\alpha\alpha^{-1} = e$ and e is even we have α, α^{-1} have the same parity. So if α even α^{-1} is too.

3. Notice that if $\alpha = (a_1 a_1')(a_2 a_2') \cdots (a_k a_k')$ (k 2-cycles)
$\beta = (b_1 b_1') \cdots (b_\ell b_\ell')$ (ℓ-2cycles)

Then $\alpha\beta$ has $k+\ell$ 2cycles.

<u>So</u> $T(\alpha\beta) = k+\ell \bmod 2 = (k \bmod 2 + \ell \bmod 2) \bmod 2$
$= T(\alpha) + T(\beta)$.

4. Use ① α may be written as a product of disjoint cycles, $\alpha = c_1 c_2 \cdots c_k$
② $|\alpha| = \mathrm{lcm}(|c_1|, |c_2|, \ldots, |c_k|)$

So if $|\alpha|$ is odd then ~~one~~ all of the $|c_i|$ is odd.

but then since $(a_1 a_2 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$

<u>or</u> $k-1$ 2-cycles. We must have c_i has

an even number of 2 cycles. or $2 \mid |c_i|$ for each i

Thus $2 \mid \mathrm{lcm}(|c_1|, \ldots, |c_k|)$

so $2 \mid |\alpha|$.

5. If $\alpha(g) = g^{-1}$ is an automorphism

Then $\alpha(ab) = \alpha(a)\alpha(b)$ so

$$(ab)^{-1} = a^{-1}b^{-1}$$

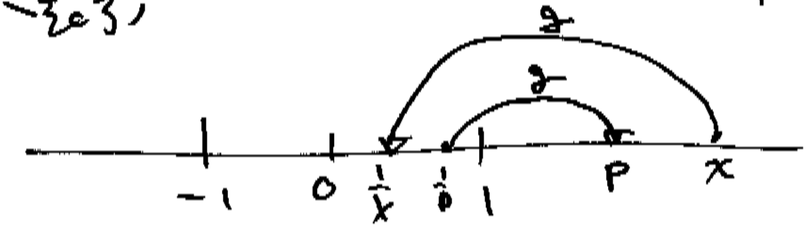
or $b^{-1}a^{-1} = a^{-1}b^{-1}$

apply to inverses $\left[\alpha(a^{-1}b^{-1}) = (b^{-1})^{-1}(a^{-1})^{-1} = ba \right.$
$\left. = \alpha(a^{-1})\alpha(b^{-1}) = ab \right]$ ✓.

Now if $ab = ba$ then $(ab)^{-1} = a^{-1}b^{-1}$
so $g(ab) = \alpha(a)\alpha(b)$ and we have

g preserves the group property. It is 1-1 as
$g(a) = g(b) \Rightarrow a^{-1} = b^{-1} \Rightarrow a = b$
and onto as $g(a^{-1}) = (a^{-1})^{-1} = a$ so each a has a preimage.

For $\mathbb{R} - \{0\}, \times$ This inverts the picture



1. If $gag^{-1} = hah^{-1}$ for all a in G

Then $h^{-1}gag^{-1} = h^{-1}hah^{-1}$

or $(h^{-1}g)ag^{-1} = ah^{-1}$

or $(h^{-1}ga)g^{-1}g = ah^{-1}g$

or $(h^{-1}g)a = a(h^{-1}g)$

Since this is true for all a, we have $h^{-1}g$ is in center.

8. $|G| = 7^2 = 49$. If G is not cyclic then we must have for any a $|a| = 1$ or 7. (if 49 then G is cyclic) In either case $a^7 = e$.

9. let $|a| = 2$, $|b| = 5$ (since prime, these subgroups are cyclic.)

what is $|ab|$?

If $|ab| = 2$ then $H = \{e, ab\}$ is a subgroup of order 2 hence $H = \{e, a\}$ (the unique one) so $a = ab$ $\times$

If $|ab| = 5$ then $H = \{e, (ab), (ab)^2, (ab)^3, (ab)^4\}$
$= \{e, b, b^2, b^3, b^4, b^5\}$

so $ab = b^i$ or $a = b^{i-1}$ $\times$ as $|a| = 2$
$|b^{i-1}| = 1$ or 5

so $|ab| = 10$ (it must divide $|G|$) and $G = \langle ab \rangle$.

8.

10. $H \subsetneq G$ implies

$G:H > 1$ but $|G| = |H| \times G:H$ so $|H| = p, q$ or 1.

In the first two cases H is cyclic, as it has prime order. In last case $H = e$ so it too is cyclic.

11. Sure. There are groups with the following

$G = \{e, a, b, c, d, e, f, g, h\}$ $\quad (|G| = 2^3 = 8)$

and $|a| = 2$ if $a \neq e$

and so. $\{e, a\}$ is a subgroup for each element (even e)

So there are atleast 8 subgroups.

However it is also true (ch 8) that $\{e, a, b, ab\}$ will be a subgroup.

oops

12. $\boxed{\text{If } G \text{ is Abelian}}$ then we must have.

$(e a_1 a_2 \cdots a_{2k})(e a_1 a_2 \cdots a_{2k}) = e$

as each a_i has an inverse. If it is not a_i itself it cancels twice, if it is a_i it cancels once.

So $|\cancel{H}| = |e a_1 a_2 \cdots a_{2k}| = 1$ or 2. But $2 \nmid |G|$ so it must be 1.

But what if G is not abelian?

Oops. I'll leave this one for later as I don't have a proof or a counterexample

13. If $|G| = p^n$ and $|Z(G)| = p^{n-1}$ then we have

p cosets $Z, a_1Z, a_2Z, \dots a_{p-1}Z$ for some a_i in G.

Set $a = a_1$. Claim $a_iZ = a^iZ$ (is possible)

Why. Define a group operation on $H = \{eZ, a_1Z, \dots a_{p-1}Z\}$

by $aZ \times bZ = abZ$ (same coset).

Is this well defined? Yes. If az is any element in aZ and bz' any one in bZ then $(az)(bz') = ab(zz')$ is in abZ.

Also $eZ = Z$ is the ~~inverse~~ identity

$a^{-1}Z$ is the inverse of aZ

and the operation is associative because G is.

So $|H| = p$ is cyclic; $\{H\} = \langle aZ \rangle$ so

$H = \{Z, aZ, a^2Z, \dots, a^{p-1}Z\}$.

any element in G is then written a^iz with $0 \le i \le p-1$ and z in Z. So if $b = a^iz$, $c = a^jz'$ then ~~$bc =$~~

$bc = a^iza^jz' = a^ia^jzz' = a^ja^izz' = a^jz'a^iz = cb$. So G is Abelian