MTH 310.003 **Spring 2018**

Group Exercise Solutions

HW 11/26

#2a. PROPOSITION: Inverses are unique in a group: that is, if $ab = ba = e$ and $ac = ca = e$, then $b = c$.
Proof: Hypothesis: For group elements a, b, c, suppose $ab = ba = e$ and $ac = ca = e$. Then we have:

$$b \overset{\text{(i)}}{=} be \overset{\text{(ii)}}{=} b(ac) \overset{\text{(iii)}}{=} (ba)c \overset{\text{(iv)}}{=} ec \overset{\text{(v)}}{=} c,$$

where: (i) is by the identity axiom; (ii) is by hypothesis; (iii) is by associativity; (iv) is by hypothesis; and (v) is by identity. Conclusion: $b = c$ by transitivity of equality.

#2b. PROPOSITION: The inverse of an inverse is the original element: $(a^{-1})^{-1} = a$.
First Proof: Hypothesis: a is a group element. The inverse of a^{-1} is the unique element $b = (a^{-1})^{-1}$ satisfying $a^{-1}b = e$. But $a^{-1}a = e$, so $b = a$. Conclusion: $(a^{-1})^{-1} = a$.

Second Proof: We compute:

$$(a^{-1})^{-1} \overset{\text{(i)}}{=} e(a^{-1})^{-1} \overset{\text{(ii)}}{=} (aa^{-1})(a^{-1})^{-1} \overset{\text{(iii)}}{=} a(a^{-1}(a^{-1})^{-1}) \overset{\text{(iv)}}{=} ae \overset{\text{(v)}}{=} a,$$

where: (i) is by the identity axiom; (ii) is by the inverse axiom; (iii) is by associativity; (iv) is by inverses; and (v) is by identity. Conclusion: $(a^{-1})^{-1} = a$.

#3. PROPOSITION: Let $a \in G$ have finite order $k = \mathrm{ord}(a)$. Then $a^i = e$ if and only if k divides i.
First Proof: Suppose $k = \mathrm{ord}(a)$, which means k is the smallest positive number with $a^k = e$. Now, if $i = kn$, we have $a^i = a^{kn} = (a^k)^n = e^n = e$.

Conversely, suppose $a^i = e$. Using the division algorithm, write $i = kn + r$ for $0 \leq r < k$. Then we have:

$$e = a^i = a^{kn+r} = a^{kn}a^r = ea^r = a^r.$$

That is, $a^r = e$ for $r < k$; but k is the smallest *positive* value with $a^k = e$, so this can only mean $r = 0$. That is, $i = kn$.

We conclude that $a^i = 0$ if and only if $i = kn$, i.e. k divides i.

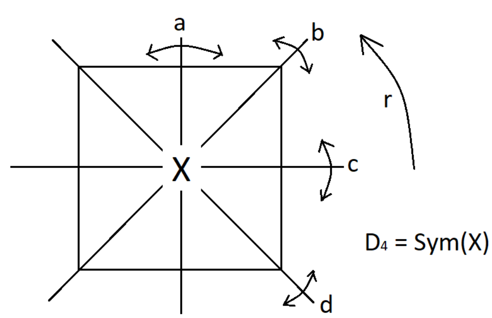
Second Proof: Let $I = \{i \in \mathbb{Z} \text{ with } a^i = e\}$. I claim I is an ideal, closed under addition and under multiplication by $\mathbb{Z}$. Indeed, if $i, j \in I$, so that $a^i = a^j = e$, then $a^{i+j} = a^i a^j = e^2 = e$, so $i+j \in I$. Also if $i \in I$, $n \geq 0$, then $a^{in} = a^i \cdots a^i = e^n = e$, and $a^{i(-n)} = (a^i)^{-1} \cdots (a^i)^{-1} = (e^{-1})^n = e$, so $i(\pm n) \in I$.

Now, we know that any ideal of $\mathbb{Z}$ is principal, meaning $I = (\ell) = \{\ell n,\ n \in \mathbb{Z}\}$ for some integer $\ell \geq 0$. We know $I \neq (0)$, since I contains $k > 0$, so we have $\ell > 0$, and ℓ is the smallest positive element of I. But by hypothesis, the smallest positive element of I is $\text{ord}(a) = k$, so we conclude $\ell = k$ and $I = (k) = \{kn \text{ for } n \in \mathbb{Z}\}$. That is, $a^i = e \ \Leftrightarrow\ i \in I \ \Leftrightarrow\ i = kn \ \Leftrightarrow\ k$ divides i.

HW 11/28-30

#3a. Consider the dihedral group $D_4 = \{e, r, r^2, r^3, a, b, c, d\}$, with the relations:

$$r^4 = e, \quad a^2 = e, \quad b = ar = r^3 a, \quad c = ar^2 = r^2 a, \quad d = ar^3 = ra.$$



Besides $H = \{e\}$ and $H = G$, the non-trivial subgroups and their cosets are:

- $H_1 = \langle a \rangle = \{1, a\},\ eH \cup rH \cup r^2H \cup r^3H = \{e, a\} \cup \{r, d\} \cup \{r^2, c\} \cup \{r^3, b\}$.
- $H_2 = \langle b \rangle = \{1, b\},\ eH \cup rH \cup r^2H \cup r^3H$
- $H_3 = \langle c \rangle = \{1, c\},\ eH \cup rH \cup r^2H \cup r^3H$
- $H_4 = \langle d \rangle = \{1, d\},\ eH \cup rH \cup r^2H \cup r^3H$
- $H_5 = \langle r^2 \rangle = \{1, r^2\},\ eH \cup rH \cup aH \cup bH = \{e, r^2\} \cup \{r, r^3\} \cup \{a, c\} \cup \{b, d\}$
- $H_6 = \langle r \rangle = \{e, r, r^2, r^3\},\ eH \cup aH = \{e, r, r^2, r^3\} \cup \{a, b, c, d\}$
- $H_7 = \langle r^2, a \rangle = \{e, r^2, a, c = r^2a\},\ eH \cup bH = \{e, r^2, a, c\} \cup \{b, d, r^3, r\}$
- $H_8 = \langle r^2, b \rangle = \{e, r^2, b, d = br^2\},\ eH \cup aH$

#3b. We have $G = D_4 = \mathrm{Sym}(X)$, where X is a rigid square in the plane. For each subgroup $H_i \subset G$, we construct a decorated square X_i with $H_i = \mathrm{Sym}(X_i)$ as follows. First, draw a completely asymmetrical X_0, so that $\mathrm{Sym}(X_0) = \{e\}$. An element $h \in H$ takes X_0 to a different decorated square hX_0, and we let X_i be the union of all of these:

$$X_i = h_1 X_0 \cup \cdots \cup h_k X_0, \quad \text{where } H = \{h_1, \ldots, h_k\}.$$

A possible choice is: