# MAT 312/AMS 351: Applied Algebra
## Solutions to Problem Set 5 (14pts)

**4.3 3; 2pts** *Let $G$ be a group and $e$ be its identity element. Suppose that $a^2=e$ for every $a\in G$. Show that $G$ is abelian.*

Let $a,b\in G$. By assumption and associativity,

$$e=(ab)^2=(ab)(ab)=a(ba)b.$$

Multiplying by $a$ on the left and by $b$ on the right, we obtain

$$ab=aeb=aa(ba)bb=e(ba)e=ba.$$

Thus, $ab=ba$ for all $a,b\in G$, i.e. $G$ is abelian.

**4.3 4; 4pts** *Let $(G,\cdot)$ be a group and $c\in G$. Show that $(G,*)$, where*

$$*\colon G\times G\longrightarrow G,\qquad a*b=a\cdot c^{-1}\cdot b,$$

*is also a group.*

We denote the identity element for $\cdot$ by $e$. and the inverse of $a$ with respect to $\cdot$ by $a^{-1}$. We need to check that $*$ takes values in $G$ (closure), is associative, has an identity element $e_*$, and every element $a$ has an inverse $a_*^{-1}$ with respect to $*$. The first is immediate because $a\cdot c^{-1}\cdot b$ is a product of three elements in $(G,\cdot)$ and thus lies in $G$. If $a,b,d\in G$, then

$$(a*b)*d=(a\cdot c^{-1}\cdot b)\cdot c^{-1}\cdot d=a\cdot c^{-1}\cdot(b\cdot c^{-1}\cdot d)=a*(b*d)$$

by the associativity of $\cdot$. Since

$$a*c=a\cdot c^{-1}\cdot c=a=c\cdot c^{-1}\cdot a=c*a$$

for every $a\in G$, $e_*=c$ is the identity element for $(G,*)$. If $a\in G$,

$$\begin{aligned}a*(ca^{-1}c)&=ac^{-1}(ca^{-1}c)=a(c^{-1}c)a^{-1}c=aa^{-1}c=c=e_*,\\(ca^{-1}c)*a&=(ca^{-1}c)c^{-1}a=ca^{-1}(cc^{-1})a=ca^{-1}a=c=e_*.\end{aligned}$$

Thus, $a_*^{-1}=ca^{-1}c$ is an inverse of $a$ with respect to $*$.

**4.3 6; 2pts** *The group $D_4$ of rigid symmetries of a square contains only one of the $4!=24$ elements of the group $S_4$ of the permutations of its four vertices. Give a quick reason for this.*

Label the vertices of the square by $1,2,3,4$ in a circular order (thus 13 is a diagonal and 24 is the other diagram). In the group $S_4$, a permutation $\pi$ can send 1 to 4 possible places (1,2,3, or 4). With $\pi(1)$ fixed, $\pi(3)$ can take **3** possible values (any of 1,2,3, or 4). Given $\pi(1)$ and $\pi(3)$, $\pi(2)$ can take either of the two remaining values, leaving one possible value for $\pi(4)$. In the group $D_4$, a rigid symmetry $\sigma$ can send 1 to 4 possible places (1,2,3, or 4) as well. However, with $\sigma(1)$ fixed, $\sigma(3)$ can take only **1** possible value (the one diagonally opposite to $\sigma(1)$, either $\sigma(1)+2$ or $\sigma(1)-2$), because $\sigma$ sends the diagonal 13 either back to itself or to the other diagonal 24. Given $\sigma(1)$ and $\sigma(3)$, $\sigma(2)$ can take either of the two remaining values as before, leaving one possible value for $\sigma(4)$. Thus, there are 1/3 of the choices for a rigid symmetry $\sigma$ of a square as for an arbitrary permutation $\pi$ of its vertices.

## Problem B (6pts)

*Let $G$ be a group and $e$ be its identity element.*

*(a) Suppose $G=\{e,a\}$ consists of exactly two distinct elements. Show that $a^2=e$.*

*(b) Suppose $G=\{e,a,b\}$ consists of exactly three distinct elements. Show that $a^2=b$ and $a^3=e$.*

*(c) Suppose $|G|=4$. Show that either there exists $a\in G$ such that $G=\{1,a,a^2,a^3\}$ with $a^4=e$ or there exist distinct $a,b\in G$ such that $G=\{1,a,b,ab\}$ with $a^2,b^2=e$ and $ab=ba$.*

*Note: By (a) and (b), all groups of orders 2 and 3 are isomorphic to $(\mathbb{Z}_2,+)$ and $(\mathbb{Z}_3,+)$, respectively. By (c), every group of order 4 is isomorphic either to $(\mathbb{Z}_4,+)$ or $(\mathbb{Z}_2,+)\times(\mathbb{Z}_2,+)$. In particular, all of these groups are abelian. The smallest non-abelian group, $S_3$, has 6 elements.*

**(a; 1pt)** Since $a\neq e$, $a^2\neq a$ and thus $a^2=e$.

**(b; 2pts)** Since $a,b\neq e$, $ab\neq b,a$ and thus $ab=e$. Since $a\neq e,b$, $a^2\neq a,ab$ and thus $a^2=b$ and $a^3=e$.

**(c; 3pts)** Since $a,b\neq e$, $ab\neq b,a$. Thus, $ab=e$ or $ab=c$. If $ab=e$, then $ac=b$ (because $ac\neq a,c,ab$), $a^2=c$ (because $a^2\neq a,ab,ac$), $a^3=b$, and $a^4=e$. If $ac=e$ or $bc=e$, we similarly find that $G$ is cyclic of order 4. The remaining possibility is that $ab,ba=c$, $ac,ca=b$, $bc,cb=a$. Combining these equations, we obtain $a^2,b^2,c^2=e$.