MTH 561/661 **Fall 2018**
Exam 1 — Fri Sept 21 **Drew Armstrong**

Problem 1. Definition of Subgroup. Let $(G, *, \varepsilon)$ be a group and let $H \subseteq G$ be any subset. We say that H is a *subgroup* if the following three conditions hold:

(S1) For all $a, b \in H$ we have $a * b \in H$.
(S2) We have $\varepsilon \in H$.
(S3) For all $a \in H$ we have $a^{-1} \in H$.

(a) If H is a subgroup, prove that for all $a, b \in H$ we have $a * b^{-1} \in H$.

If $a, b \in H$ then (S3) implies $b^{-1} \in H$ and then (S1) implies $a * b^{-1} \in H$.

(b) **(Bonus)** Assume that for all $a, b \in H$ we have $a*b^{-1} \in H$. Prove that H is a subgroup.

We will prove (S2), (S3), (S1), in that order:

(S2) If $a \in H$ then $\varepsilon = a * a^{-1} \in H$.
(S3) If $b \in H$ then from (S2) we have $b^{-1} = \varepsilon * b^{-1} \in H$.
(S1) If $a, b \in H$ then from (S3) we have $b^{-1} \in H$ and hence $a * b = a * (b^{-1})^{-1} \in H$.

(c) If $H, K \subseteq G$ are subgroups prove that $H \cap K$ is a subgroup. [Hint: Use (a) and (b).]

Suppose that $a, b \in H \cap K$, which implies $a, b \in H$ and $a, b \in K$. Then part (a) says that $a * b^{-1} \in H$ and $a * b^{-1} \in K$, hence $a * b^{-1} \in H \cap K$. We conclude from part (b) that $H \cap K$ is a subgroup.

Problem 2. Cyclic Groups. Let $(G, *, \varepsilon)$ be a group and let $g \in G$ be any element. Consider the cyclic subgroup $\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \subseteq G$.

(a) If $\langle g \rangle$ is a **finite** set, prove that there exists an integer $n \geq 1$ such that $g^n = \varepsilon$.

If $\langle g \rangle$ is finite then there exist integers $k < \ell$ such that $g^k = g^\ell$. Now define $n = \ell - k$ and observe that

$$\begin{aligned} g^\ell &= g^k \\ g^\ell * g^{-k} &= g^k * g^{-k} \\ g^{\ell-k} &= \varepsilon. \end{aligned}$$

(b) If $g^n = \varepsilon$ for some $n \geq 1$, prove that $\langle g \rangle = \{\varepsilon, g, g^2, \ldots, g^{n-1}\}$.

Consider any element $g^k \in \langle g \rangle$ and divide k by n to obtain $k = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < k$. Now observe that

$$g^k = g^{qn+r} = (g^n)^q * g^r = \varepsilon^q * g^r = g^r \in \{\varepsilon, g, g^2, \ldots, g^{n-1}\}.$$

(c) If m is the **smallest** positive integer such that $g^m = \varepsilon$, prove that the m elements

$$g^0, g^1, g^2, \ldots, g^{m-1}$$

are distinct, and hence $\#\langle g \rangle = m$.

Suppose for contradiction that we have $g^k = g^\ell$ for some integers $0 \leq k < \ell \leq m-1$, so that $1 \leq \ell - k < m$. Then from part (a) we have $g^{\ell-k} = \varepsilon$, which contradicts the minimality of m.

Problem 3. Homomorphism and Isomorphism. Let $(G, *, \delta)$ and $(H, \bullet, \varepsilon)$ be groups and let $f : G \to H$ be any function satisfying

$$f(a * b) = f(a) \bullet f(b) \text{ for all } a, b \in G.$$

(a) Prove that $f(\delta) = \varepsilon$.

$$\begin{aligned} \delta * \delta &= \delta \\ f(\delta) \bullet f(\delta) &= f(\delta) \\ f(\delta) \bullet f(\delta) \bullet f(\delta)^{-1} &= f(\delta) \bullet f(\delta)^{-1} \\ f(\delta) &= \varepsilon. \end{aligned}$$

(b) For all $a \in G$ prove that $f(a^{-1}) = f(a)^{-1}$.

$$\begin{aligned} a * a^{-1} &= \delta \\ f(a * a^{-1}) &= f(\delta) \\ f(a) \bullet f(a^{-1}) &= \varepsilon && \text{from (a)} \\ f(a)^{-1} \bullet f(a) \bullet f(a^{-1}) &= f(a)^{-1} \bullet \varepsilon \\ f(a^{-1}) &= f(a)^{-1}. \end{aligned}$$

(c) Assuming that the inverse function $f^{-1} : H \to G$ exists, prove that

$$f^{-1}(a \bullet b) = f^{-1}(a) * f^{-1}(b) \text{ for all } a, b \in H.$$

Observe that

$$f(f^{-1}(a) * f^{-1}(b)) = f(f^{-1}(a)) \bullet f(f^{-1}(b)) = a \bullet b.$$

Then apply f^{-1} to both sides.

Problem 4. Orthogonal Matrices. Consider the set of 2×2 orthogonal matrices:

$$O_2(\mathbb{R}) = \{A \in \mathrm{Mat}_2(\mathbb{R}) : A^T A = I\}.$$

(a) Given A and B in $O_2(\mathbb{R})$ prove that AB^{-1} is in $O_2(\mathbb{R})$.

Assume that $A^T A = I$ and $B^T B = I$, hence $(B^{-1})^T = B$. Then we have

$$(AB^{-1})^T (AB^{-1}) = (B^{-1})^T A^T A B^{-1} = BIB^{-1} = I.$$

(b) Let $\langle -, - \rangle : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ be the standard dot product and let $A \in \mathrm{Mat}_2(\mathbb{R})$. If $\langle A\mathbf{x}, A\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$, prove that $A \in O_2(\mathbb{R})$.

Let $\mathbf{e}_i$ and $\mathbf{e}_j$ be the i-th and j-th standard basis vectors. Then the i, j-entry of the matrix $A^T A$ is

$$\mathbf{e}_i^T (A^T A)\mathbf{e}_j = (A\mathbf{e}_i)^T (A\mathbf{e}_j) = \langle A\mathbf{e}_i, A\mathbf{e}_j \rangle = \langle \mathbf{e}_i, \mathbf{e}_j \rangle = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

In other words, $A^T A = I$.

(c) Prove that every matrix $A \in O_2(\mathbb{R})$ has the form

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{or} \qquad A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

The equation $A^T A = I$ says that the two columns of A are perpendicular unit vectors. Since the first column is a unit vector it must equal $(\cos\theta, \sin\theta)$ for some angle θ. Then since the second column is a perpendicular unit vector, it must be $(-\sin\theta, \cos\theta)$ or $(\sin\theta, -\cos\theta)$.