Debra Griffin
Math 210A
HW #3, 2.4 p. 72 #29, 31-35, 37
Hand in #35

2.29 Let H be a subgroup of a group G.
(i) Prove that right cosets Ha and Hb are equal if and only if $ab^{-1} \in H$.

Proof:
$\Rightarrow$: Assume Ha and Hb are equal.
Then $\forall\ h \in H, \exists\ h' \in H$ such that $ha = h'b$.
$\therefore \quad \Leftrightarrow \quad hab^{-1} = h'bb^{-1}$.
$\Leftrightarrow \quad h^{-1}hab^{-1} = h^{-1}h'$.
$\Leftrightarrow \quad ab^{-1} = h^{-1}h' \in H$.

$\Leftarrow$: Assume $ab^{-1} \in H$.

We will first show $Ha \subseteq Hb$. Let $ha \in Ha$.

Then $ab^{-1} \in H \Rightarrow hab^{-1} \in H \Rightarrow hab^{-1}b \in Hb \Rightarrow ha \in Hb$.

$\therefore\ Ha \subseteq Hb$.

To show $Hb \subseteq Ha$, we let $hb \in Hb$. Then $ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H \Rightarrow hba^{-1} \in H$

$\Rightarrow hba^{-1}a = hb \in Ha$.

$\therefore\ Hb \subseteq Ha$.

$\therefore\ Ha = Hb$.

(ii) Prove that the relation $a \equiv b$ if $ab^{-1} \in H$ is an equivalence relation on G whose equivalence classes are the right cosets of H.

Proof:
Let $a, b \in G$.

We first show reflexivity. Since $1 = aa^{-1} \in H$, then $a \equiv a$. $\therefore$ "$\equiv$" is reflexive.

To show symmetry, we note that $ab^{-1} \in H$ gives us that $(ab^{-1})^{-1} = ba^{-1} \in H$ also.

$\therefore a \equiv b \Leftrightarrow b \equiv a$. $\therefore$ "$\equiv$" is symmetric.

And to show transitivity, we assume $a \equiv b$ and $b \equiv c$ and note that $ab^{-1} \in H$ and $bc^{-1} \in H$

gives us $ab^{-1} \bullet bc^{-1} = ac^{-1} \in H$ by closure. $\therefore$ "$\equiv$" is transitive.

Let the equivalence class of a be X.

Then $X = \{g \in G \mid g \equiv b\} = \{g \in G \mid gb^{-1} \in H\} = \{g \in G \mid g \in Hb\} = Hb$.

By part (i) $Hb = Ha$, and these are the right cosets of H.

2.31 (i) Give an example of two subgroups H and K of a group G whose union, $H \cup K$ is not a subgroup of G.
Hint: Let G be the four-group $\boldsymbol{V}$.

Proof:
Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2, j^2, k^2 = 1$, $ij = k$, $jk = i$, and $ki = j$.

Let $H = \{\pm 1, \pm i\}$ and $K = \{\pm 1, \pm j\}$.

It is clear that H and K are subgroups of G.

But $H \cup K = \{\pm 1, \pm i, \pm j\}$ does not have closure as $ij = k \notin H \cup K$.

(ii) Prove that the union, $H \cup K$, of two subgroups is itself a subgroup iff either H is a subset of K or K is a subset of H.

Proof:
Let G be a group, $H \leq G$, and $K \leq G$.

$\Rightarrow$: Assume $H \cup K \leq G$.

Let $h \in H$ and $k \in K$. Then $hk \in H$ or $hk \in K$.

Suppose $hk \in K$. Then $hkk^{-1} = h \in K$. $\therefore$ $H \subseteq K$.

Similarly, if $hk \in H$, then $h^{-1}hk = k \in H$. $\therefore$ $K \subseteq H$.

$\therefore$ $H \subseteq K$ or $K \subseteq H$, as desired.

$\Leftarrow$: If $H \subseteq K$, then $H \cup K = K \leq G$.

If $K \subseteq H$, then $H \cup K = H \leq G$.

$\therefore$ $H \cup K \leq G$.

2.32 Let G be a finite group with subgroups H and K. If $H \leq K$, prove that $[G:H] = [G:K][K:H]$.

Proof:
Let $n = [G:H]$, $m = [G:K]$, and $t = [K:H]$.

Then $n|H| = |G| = m|K|$.

Since $|K| = t|H|$, then $n|H| = mt|H|$, hence $n = mt$.

$\therefore$ $[G:H] = [G:K][K:H]$.

2.33 If H and K are subgroups of a group G and if $|H|$ and $|K|$ are relatively prime, prove that $H \cap K = \{1\}$.
Hint: If $x \in H \cap K$, then $x^{|H|} = x^{|K|}$.

Proof:
Let $a \in H \cap K$ with $\circ(a) = d$. Then $a^d = 1$.

Since $a \in H$ and $a \in K$, then $d \mid |H|$ and $d \mid |K|$.

But $|H|$ and $|K|$ are relatively prime, so d must be 1.

$\therefore$ $\circ(a) = 1$ and the only element with order 1 is the identity. Hence $a = 1$.

2.34 Prove that every subgroup S of a cyclic group $G = \langle a \rangle$ is itself cyclic.
Hint: If $S \neq 1$, choose k to be the smallest positive integer with $a^k \in S$.

Proof:
Let S be a subgroup of G. If $S = \{e\}$, then $S = \langle e \rangle$ and we are done.

Assume $S \neq \{e\}$, then S contains a nonidentity element of G, say a^i with $i \neq 0$.

Thus $a^{-i} \in S$ also. One of i or $-i$ is positive, so S contains positive powers of a. Let k be the smallest positive integer such that $a^k \in S$. If x is an arbitrary element in S, then $x = a^m$ for some m. By the Division Algorithm, $m = kq + r$ with $0 \leq r < k$. Thus $r = m - kq$ and $a^r = a^{m-kq} = a^m a^{-kq} = a^m (a^k)^{-q}$. Both a^m and a^k are in S. $\therefore$ $a^r \in S$ by closure. Since a^k is the smallest positive power of a in S and since $r < k$, we must have $r = 0$. $\therefore$ $m = kq$ and $x = a^m = a^{kq} = (a^k)^q \in \langle a^k \rangle$. Hence $S = \langle a^k \rangle$.

2.35 Prove that a cyclic group G of order n has a unique subgroup of order d for every d dividing n.
Hint: If $G = \langle a \rangle$ and $n = dk$, consider $\langle a^k \rangle$.

Proof:
Let G be a cyclic group $\langle a \rangle$ of order n and suppose $d \mid n$.

Then $n = dk$ for some integer $k \geq 1$.

Since G contains every integral power of a, then $a^k \in G$.

And since $\circ(a) = |\langle a \rangle| = n$, then we can apply the gcd theorem to find the order of a^k.

$$\circ(a^k) = \frac{n}{\gcd(n,k)} = \frac{dk}{\gcd(dk,k)} = d \text{ . } \therefore \text{ } d = \circ(a^k) = |\langle a^k \rangle|.$$

And we know $\langle a^k \rangle \subseteq \langle a \rangle$ as $\forall\ t \in \mathbb{Z}$, $(a^k)^t = a^{kt}$ where $kt \in \mathbb{Z}$.

To show $\langle a^k \rangle \leq \langle a \rangle$ we first note that $\langle a^k \rangle \neq \varnothing$ as $a^k \in \langle a^k \rangle$.

Let $a^{ki}, a^{kj} \in \langle a^k \rangle$.

Since $a^{ki} \bullet (a^{kj})^{-1} = a^{k(i-j)}$, then $a^{k(i-j)} \in \langle a^k \rangle$, hence $\langle a^k \rangle \leq \langle a \rangle$.

We now will show the uniqueness of $\langle a^k \rangle$.

Suppose $\langle x \rangle$ is a subgroup of $\langle a \rangle$ and $|\langle x \rangle| = d$ ($dk = n$, as defined above).

Then for some integer m, $x = a^m$.

Let $x^t \in \langle x \rangle$. Then $x^t = a^{mt}$. And $a^{mtd} = 1$ as $\circ(a^m) = d$.

Thus, as $\circ(a) = n$ we have

$$n \mid md$$
$$\Rightarrow md = nr \text{ for some } r \in \mathbb{N}$$
$$\Rightarrow m = kr.$$

$\therefore$ We can write $x^t = a^{mt} = a^{krt} = (a^k)^{rt}$. $\therefore$ $x^t \in \langle a^k \rangle$, hence $\langle x \rangle \subseteq \langle a^k \rangle$.

And since $|\langle x \rangle| = |\langle a^k \rangle|$, then $\langle x \rangle = \langle a^k \rangle$.

2.37 If H is a subgroup of a group G, prove that the number of left cosets of H in G is equal to the number of right cosets of H in G.
Hint: The function ϕ: $aH \rightarrow Ha^{-1}$ is a bijection from the family of all left cosets of H to the family of all right cosets of H.

Proof:
Define ϕ: $\{aH\}_{a \in G} \rightarrow \{Hb\}_{b \in G}$ by $\phi(aH) = Ha^{-1}$. We will show this is a bijective function.

Let $x, y \in G$ where $x \neq y$. We have that

$\phi(xH) = \phi(yH) \Leftrightarrow Hx^{-1} = Hy^{-1} \Leftrightarrow y^{-1}x = y^{-1}(x^{-1})^{-1} \in H \Leftrightarrow xH = yH$.

$\therefore$ ϕ is well-defined and injective.

Let Hb be a right coset in G. Since G is a group, then there is a unique inverse of b in G.

And since $\phi((b^{-1})H) = H(b^{-1})^{-1} = Hb$, then ϕ is surjective.

$\therefore$ ϕ is a bijection from $\{aH\}_{a \in G}$ to $\{Hb\}_{b \in G}$.

$\therefore$ The number of left cosets of H in G is equal to the number of right cosets of H in G.
