Modern Algebra I Spring 2016
Review Sheet for the Final

Definition: Let $G_1$ and $G_2$ be groups. A function $f: G_1 \to G_2$ is a homomorphism if, for all $g, h \in G_1$, $f(gh) = f(g)f(h)$.

Examples: 1) $f$ an isomorphism, or more generally $f$ an isomorphism from $G_1$ to a subgroup of $G_2$. 2) $f(g) = 1$ for all $g \in G_1$. 3) $f: \mathbb{C} \to \mathbb{C}^*$ defined by $f(z) = e^z$. 4) $f: \mathbb{C}^* \to \mathbb{R}^*$ defined by $f(z) = |z|$. 5) $\varepsilon: S_n \to \{\pm 1\}$. 6) $\det: GL_n(\mathbb{R}) \to \mathbb{R}^*$. 7) $\pi_1: G_1 \times G_2 \to G_1$ defined by $\pi_1(g_1, g_2) = g_1$ (and similarly for $\pi_2: G_1 \times G_2 \to G_2$). 8) $\pi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\pi(k) = \lfloor k \rfloor = k + n\mathbb{Z}$. 9) For $G$ a (multiplicative) group and $g \in G$, the function $f: G \to G$ defined by $f(g) = g^n$. 10) For $G$ an abelian group and $n \in \mathbb{Z}$, the function $f: G \to G$ defined by $f(g) = g^n$.

Proposition: Let $f: G_1 \to G_2$ be a homomorphism. Then:

1. $f(1) = 1$.
2. For all $g \in G_1$, $f(g^{-1}) = f(g)^{-1}$.
3. If $H_1 \leq G_1$, then $f(H_1) \leq G_2$. In particular, the image $\text{Im } f = f(G_1)$ is a subgroup of $G_2$.
4. If $H_2 \leq G_2$, then $f^{-1}(H_2) \leq G_1$.

Proposition: Let $f: G_1 \to G_2$ and $g: G_2 \to G_3$ be homomorphisms. Then $g \circ f: G_1 \to G_3$ is a homomorphism.

Definition: Let $f: G_1 \to G_2$ be a homomorphism. Then the kernel of $f$, written $\text{Ker } f$, is the subgroup $f^{-1}(1) \leq G_1$.

In the above examples of homomorphisms, the kernel is as follows: 1) $\{1\}$; 2) $G_1$; 3) $\langle 2\pi i \rangle$; 4) $U(1) = \{z \in \mathbb{C} : |z| = 1\}$; 5) $A_n$; 6) $\text{SL}_n(\mathbb{R})$; 7) $H_2 = \{1\} \times G_2$; 8) $n\mathbb{Z}$; 9) $\{0\}$, if $g$ has infinite order, and $d\mathbb{Z}$, where $d$ is the order of $g$, in case $g$ has finite order; 10) the subgroup $\{g \in G : g^n = 1\}$ of $n$-torsion points (if, say, $n > 0$).

Proposition: Let $f: G_1 \to G_2$ be a homomorphism. Then $f$ is injective if and only if $\text{Ker } f = \{1\}$.

Cayley’s theorem: Let $G$ be a finite group. Then there exists an $n$ such that $G$ is isomorphic to a subgroup of $S_n$.

Cosets: let $G$ be a group and $H \leq G$. A left coset of $H$ in $G$ is a subset of $G$ of the form $gH = \{gh : h \in H\}$ for some $g \in G$. The set of all left cosets is denoted $G/H$. Right cosets $Hg$ are similarly defined. A left coset
of $G$ is an equivalence class for the equivalence relation $g_1 \equiv g_2 \pmod{H} \iff g_2^{-1}g_1 \in H$. Hence two left cosets for $H$ are either disjoint or equal, and every element of $G$ is in exactly one left coset. A similar result holds for right cosets, using the equivalence relation $g_1 \equiv_{r} g_2 \pmod{H} \iff g_1g_2^{-1} \in H$.

Proposition: For all $g \in G$, there is a bijection from $H$ to $gH$. Hence, if $H$ is finite, for every $g \in G$, $#(gH) = #(H)$.

Corollary 1 (Lagrange): If $G$ is finite and $H \leq G$, then $#(G) = #(H) \cdot #(G/H)$.

In particular, $#(H)$ divides $#(G)$.

Definition: if $G$ is a group and $H \leq G$, the index $(G : H)$ of $H$ in $G$ is the integer $#(G/H)$, if $G/H$ is finite; otherwise $H$ is of infinite index in $G$. If $G$ is finite, then $(G : H) = #(G)/#(H)$. The index satisfies: if $K \leq H \leq G$, then $(G : K) = (G : H)(H : K)$.

Corollary 2: If $G$ is a finite group, then the order of every element of $G$ divides the order of $G$.

Corollary 3: If $G$ is a finite group of prime order, then $G$ is cyclic.

Corollary 4 (Fermat’s little theorem): If $p$ is a prime and $a \in \mathbb{Z}$ is such that $p$ does not divide $a$, then $a^{p-1} \equiv 1 \pmod{p}$. Hence for all $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

Corollary 5 (Euler’s generalization of Fermat’s little theorem): More generally, for $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, if $\gcd(a,n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi$ is the Euler $\varphi$-function.

Coset multiplication: we try to turn the set $G/H$ of left cosets into a group using multiplication of representatives. In other words, we try to define $(g_1H)(g_2H) = (g_1g_2)H$. To see that this is well-defined, we must show that it is independent of the choice of representative. In other words, we must check that, for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$, $(g_1h_1g_2h_2)H = (g_1g_2)H$, or equivalently that there exists an $h_3 \in H$ such that $g_1h_1g_2h_2 = g_1g_2h_3$.

Proposition: Coset multiplication for $G/H$ is well-defined if and only if, for all $g \in G$ and $h \in H$, there exists an $h' \in H$ such that $hg = gh'$. Equivalently, coset multiplication for $G/H$ is well-defined if and only if, for all $g \in G$ and $h \in H$, $g^{-1}hg \in H$.

Let $g^{-1}Hg = \{g^{-1}hg : h \in H\}$.

Proposition: Let $G$ be a group and let $H \leq G$. Then the following are equivalent:

1. For all $g \in G$ and $h \in H$, there exists an $h' \in H$ such that $hg = gh'$. 
2. For all $g \in G$, $Hg \subseteq gH$.

3. For all $g \in G$, $g^{-1}Hg \subseteq H$.

4. For all $g \in G$, $g^{-1}Hg = H$.

5. For all $g \in G$, $gH = Hg$, i.e. every left coset of $G$ is also a right coset.

Definition: $H$ is a normal subgroup of $G$ (written $H \triangleleft G$) if coset multiplication for $G/H$ is well-defined, i.e. if any and hence all of the equivalent conditions of the preceding proposition are satisfied. (Usually, the easiest to check in practice to show that, for all $g \in G$ and $h \in H$, $g^{-1}hg \in H$.)

Corollary: If $H$ has index two in $G$, then $H \triangleleft G$.

Proposition: If $H \triangleleft G$, then $G/H$ is a group under coset multiplication. It is called the quotient of $G$ by $H$ and a group of the form $G/H$ is called a quotient group. In this case, the function $\pi : G \to G/H$ defined by $\pi(g) = gH$ is a homomorphism, the quotient homomorphism, and Ker $\pi = H$.

Facts about normal subgroups:

1. If $H \triangleleft G$ and $K \triangleleft G$, then $H \cap K \triangleleft G$.

2. If $H \triangleleft G$ and $K \leq G$, then $H \cap K \triangleleft K$.

3. If $H \leq K$ and $H \triangleleft G$, then $H \triangleleft K$. But there are examples of subgroups $H \leq K \leq G$ such that $H \triangleleft K$ and $K \triangleleft G$, but $H$ is not a normal subgroup of $G$.

4. If $H \triangleleft G$ and $K \leq G$, then the set $HK = \{hk : h \in H, k \in K\}$ is a subgroup of $G$ and $H \triangleleft HK$, $K \leq HK$.

Proposition: If $f : G_1 \to G_2$ is a homomorphism, then Ker $f$ is a normal subgroup of $G_1$.

More generally, if $f : G_1 \to G_2$ is a homomorphism and $H_2$ is a normal subgroup of $G_2$, then $f^{-1}(H_2)$ is a normal subgroup of $G_1$. If $f$ is surjective and if $H_1$ is a normal subgroup of $G_1$, then $f(H_1)$ is a normal subgroup of $G_2$.

Theorem (First Isomorphism Theorem, or Fundamental Homomorphism Theorem): Let $f : G_1 \to G_2$ be a homomorphism and let $K = \text{Ker } f$. Then there exists a unique isomorphism $\tilde{f} : G_1/K \to \text{Im } f$ such that $\tilde{f}(gK) = f(g)$ for all $g \in G_1$. Hence $f = i \circ \tilde{f} \circ \pi$, where $i : \text{Im } f \to G_2$ is the inclusion and $\pi : G_1 \to G_1/K$ is the quotient homomorphism: $\pi(g) = gK$ for all $g \in$
In other words, every homomorphism can be “factored” into a quotient homomorphism, followed by an isomorphism, followed by an inclusion of a subgroup.

The situation is expressed by the following “commutative diagram:”

\[
\begin{array}{ccc}
G_1 & \xrightarrow{f} & G_2 \\
\downarrow \pi & & \uparrow i \\
G_1/K & \xrightarrow{f} & \text{Im } f.
\end{array}
\]

Examples: 1) \(G\) a group, \(g \in G\), and \(f: \mathbb{Z} \to G\) defined by \(f(k) = g^k\): then \(\text{Im } f = \langle g \rangle \cong \mathbb{Z}\) if \(g\) is of infinite order and \(\text{Im } f = \langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}\) if \(g\) has order \(n\). 2) \(G_1\) and \(G_2\) two groups, with normal subgroups \(H_1 \triangleleft G_1\) and \(H_2 \triangleleft G_2\). Then \(f: G_1 \times G_2 \to (G_1/H_1) \times (G_2/H_2)\) defined by

\[f(g_1, g_2) = (g_1 H_1, g_2 H_2)\]

is a homomorphism with kernel \(H_1 \times H_2\), so that \((G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)\). 3) \(GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*\). 4) The homomorphism \(f: \mathbb{R} \to \mathbb{C}^*\) defined by \(f(t) = e^{2\pi it}\) has image \(U(1)\) and kernel \(\mathbb{Z}\). Thus \(\mathbb{R}/\mathbb{Z} \cong U(1)\), and \(\mathbb{Q}/\mathbb{Z} \cong \mu_\infty\), the torsion subgroup of \(U(1)\).

Third Isomorphism Theorem: Let \(G\) be a group, \(H, K\) two subgroups of \(G\) with \(H \leq K\), and suppose that \(H \triangleleft G\) and \(K \triangleleft G\). Then the image \(\pi(K) = K/H\) is a normal subgroup of \(G/H\), and

\[(G/H)/(K/H) \cong G/K.\]

Definition: A group \(G\) is simple if \(G \neq \{1\}\) and the only normal subgroups of \(G\) are either \(\{1\}\) or \(G\).

Example: If \(p\) is a prime, then \(\mathbb{Z}/p\mathbb{Z}\) is simple. Every abelian finite simple group is isomorphic to \(\mathbb{Z}/p\mathbb{Z}\) for some prime \(p\).

Theorem: The group \(A_n\) is simple for \(n \geq 5\).

Corollary (HW): If \(n \geq 5\) and \(H\) is a normal subgroup of \(S_n\), then \(H\) is either \(S_n\), \(A_n\), or \(\{1\}\).

Definition: Let \(G\) be a group and \(X\) a set. Then an action of \(G\) on \(X\) is a function \(F: G \times X \to X\), where we write \(F(g, x) = g \cdot x\), satisfying:

1. For all \(g_1, g_2 \in G\) and \(x \in X\), \(g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x\).
2. For all \(x \in X\), \(1 \cdot x = x\).
When the action $F$ is understood, we say that $X$ is a $G$-set.

Examples:

1. The trivial action: $g \cdot x = x$ for all $g \in G$ and $x \in X$.

2. $S_n$ acts on $\{1, \ldots, n\}$ via $\sigma \cdot k = \sigma(k)$ (here we use the definition of multiplication in $S_n$ as function composition). More generally, if $X$ is any set, $S_X$ acts on $X$, and on $\mathcal{P}(X)$, and on all subsets of $X$ of a fixed cardinality.

3. $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$, via matrix multiplication, and $\mathbb{R}^*$ acts on $\mathbb{R}^n$ by scalar multiplication. Also $O_n$ and $SO_n$ act on $\mathbb{R}^n$, and on $S^{n-1}$, the unit sphere in $\mathbb{R}^n$.

4. $D_n$ acts on the set of vertices of a regular $n$-gon, as well as on the set of edges. Similarly for the symmetry groups of the five regular solids, which are subgroups of $SO_3$.

5. $G$ acts on itself by left multiplication: $g \cdot x = gx$. More generally, if $H \leq G$, then $G$ acts on the set of left cosets $G/H$ via: $g \cdot (xH) = (gx)H$.

6. $G$ acts on itself by conjugation $i_g$: $i_g(x) = gxg^{-1}$.

If $X$ is a $G$-set and $f: G' \to G$ is a homomorphism, then $X$ becomes a $G'$-set via $g \cdot x = f(g) \cdot x$. In particular, if $H \leq G$, then a $G$-set $X$ is also an $H$-set by just looking at $h \cdot x$ for $h \in H$.

Generalization of the proof of Cayley’s Theorem: Given a homomorphism $\rho: G \to S_X$, then $X$ becomes a $G$-set. Conversely, if $F: G \times X \to X$ is an action, then let $\ell_g: X \to X$ be defined by $\ell_g(x) = F(g,x) = g \cdot x$. (For $X = G$ with the action of left multiplication, this is the definition from the proof of Cayley’s Theorem.) Thus $\ell_1 = \text{Id}_X$ and $\ell_g \circ \ell_h(x) = g \cdot (h \cdot x) = (gh) \cdot x = \ell_{gh}(x)$. In particular $\ell_g \circ \ell_{g^{-1}} = \ell_{g^{-1}} \circ \ell_g = \ell_1 = \text{Id}_X$, so that $\ell_{g^{-1}} = \ell_g^{-1}$ and $\ell_g$ is a bijection for all $g \in G$. In particular we see that

$$y = g \cdot x \iff x = g^{-1} \cdot y.$$  

Moreover, $\rho: G \to S_X$ defined by $\rho(g) = \ell_g$ is a homomorphism from $G$ to $S_X$. Finally, the two constructions just described (passing from a homomorphism $G \to S_X$ to an action of $G$ on $X$, and passing from an action of $G$ on $X$ to a homomorphism $G \to S_X$) are inverse constructions. Thus, the concept of a $G$-set $X$ is equivalent to the concept of a homomorphism $G \to S_X$. 

5
Definition: If $X$ is a $G$-set, then a $G$-subset $Y$ of $X$ is a subset $Y \subseteq X$ such that, for all $g \in G$ and $y \in Y$, $g \cdot y \in Y$. A $G$-subset is itself a $G$-set.

Definition: If $X_1$ and $X_2$ are $G$-sets, an isomorphism $f$ from $X_1$ to $X_2$ (of $G$-sets) is a bijection $f: X_1 \to X_2$ such that $f(g \cdot x) = g \cdot f(x)$ for all $g \in G$ and $x \in X$. In this case we say that $X_1$ and $X_2$ are isomorphic (as $G$-sets) and write this as $X_1 \cong_G X_2$. If $f: X_1 \to X_2$ is an isomorphism of $G$-sets, then so is $f^{-1}$; likewise the composition of two isomorphisms of $G$-sets is again an isomorphism of $G$-sets.

Definition: If $X$ is a $G$-set and $x \in X$, the orbit of $X$ (under $G$) is the set $G \cdot x = \{g \cdot x : g \in G\}$. Thus $G \cdot x \subseteq X$. Clearly $G \cdot x$ is a $G$-subset of $X$ and is the smallest $G$-subset of $X$ containing $x$. The orbit of $x$ is the equivalence class containing $x$ for the equivalence relation $x \sim_G y \iff$ there exists a $g \in G$ such that $g \cdot x = y$. Thus, two orbits are either disjoint or equal. If $G \cdot x = X$ for one (or equivalently all) $x \in X$, we say that $G$ acts transitively on $X$.

Example: if $\sigma \in S_n$, then we have previously defined the orbits $O_\sigma(i)$ of $\sigma$. The link with the current definition is as follows: the orbits of $\sigma$ in the previous sense are the orbits of the cyclic subgroup $\langle \sigma \rangle$ acting on $\{1, \ldots, n\}$ as a subgroup of $S_n$.

Definition: If $X$ is a $G$-set and $x \in X$, the isotropy subgroup $G_x$ is the set $\{g \in G : g \cdot x = x\}$. It is a subgroup of $G$.

Definition: If $X$ is a $G$-set, then the fixed set $X^G$ is the set $\{x \in X : g \cdot x = x \text{ for all } g \in G\}$. It is the largest $G$-subset of $X$ for which the $G$-action is trivial. Clearly $x \in X^G \iff G_x = G \iff G \cdot x = \{x\} \iff$ the orbit $G \cdot x$ contains exactly one element.

Example: If $G$ acts on itself by conjugation, then the fixed set $G^G$ is the center $Z(G)$, the orbit of $x \in G$ is the conjugacy class $C(x) = \{gxg^{-1} : g \in G\}$, and the isotropy group of $x$ is the centralizer of $x$, namely the subgroup $Z_G(x) = \{g \in G : gxg^{-1} = x\}$.

Proposition: If $X$ is a $G$-set, $x \in X$, and $y = g \cdot x \in G \cdot x$, then $G_y = gG_xg^{-1}$. In other words, the isotropy groups of $x$ and $y$ are conjugate by $g$.

Theorem: If $X$ is a $G$-set and $x \in X$, then there is an isomorphism of $G$-sets from $G \cdot x$ to $G/G_x$, where $G$ acts on the set of left cosets of $G_x$ in the usual way (by left multiplication of cosets).

Corollary: If $G$ is finite, $X$ is a $G$-set, and $x \in X$, then

$$\#(G) = \#(G_x) \cdot \#(G \cdot x),$$
or equivalently
\[ \#(G \cdot x) = (G : G_x). \]

Hence the number of elements of an orbit of \( G \) in \( X \) divides the order of \( G \).

For example, if \( G \) is a finite group and \( x \in G \), then
\[ \#(C(x)) = (G : Z_G(x)). \]

Suppose \( X \) is a finite \( G \)-set with the different orbits listed (for some \( x_1, \ldots, x_k \in X \)) as \( O_1 = G \cdot x_1, \ldots, O_k = G \cdot x_k \). Then
\[ \#(X) = \sum_{i=1}^{k} \#(G \cdot x_i) = \sum_{i=1}^{k} \#(O_i). \]

We rewrite this by grouping together the one-element orbits into \( X^G \), as
\[ \#(X) = \#(X^G) + \sum_{\#(G \cdot x_i) > 1} \#(G \cdot x_i) = \#(X^G) + \sum_{\#(O_i) > 1} \#(O_i), \]
where the second sum is over the orbits which have more than one element (note that \( \#(O) \) divides \( \#(G) \) if \( G \) is finite). Thus:

Corollary: If \( \#(G) = p^r \), where \( p \) is a prime, and if \( X \) is a finite \( G \)-set, then
\[ \#(X) \equiv \#(X^G) \pmod{p}. \]

For a general finite group \( G \), regarding \( G \) as acting on itself by conjugation, we get the class equation
\[ \#(G) = \#(Z(G)) + \sum \#(C(x_i)), \]
where the sum is over the distinct conjugacy classes \( C(x_i) \) which have more than one element (i.e. for which \( x_i \notin Z(G) \)).

Corollary: Let \( p \) be a prime number. If \( \#(G) = p^r \) with \( r \geq 1 \), then \( Z(G) \neq \{1\} \). In particular, if \( \#(G) \neq p \), then \( G \) is not simple (and hence, by induction, solvable).

Corollary: Let \( p \) be a prime number. If \( \#(G) = p^2 \), then \( G \) is abelian.

Definition: Let \( p \) be a prime number. Let \( G \) be a finite group such that \( \#(G) = p^r m \) where \( r > 0 \) and \( p \) does not divide \( m \). A \( p \)-Sylow subgroup of \( G \) is a subgroup \( P \) such that \( \#(P) = p^r \), or equivalently \( (G : P) = m \).

Theorem (Sylow Theorem): Let \( G \) be a group of order \( n \), let \( p \) be a prime number such that \( p \mid n \), and write \( n = p^r m \) where \( p \) does not divide \( m \). Then:
1. There exists a $p$-Sylow subgroup of $G$.

2. If $P_1$ and $P_2$ are two $p$-Sylow subgroups of $G$, then $P_1$ and $P_2$ are conjugate, i.e. there exists a $g \in G$ such that $gP_1g^{-1} = P_2$.

3. If $H \leq G$ and $\#(H) = p^s$, then there exists a $p$-Sylow subgroup $P$ of $G$ such that $H \leq P$.

4. The number of $p$-Sylow subgroups of $G$ is congruent to 1 (mod $p$) and divides $\#(G)$.

Lemma (Cauchy’s Theorem for abelian groups): Let $G$ be a finite abelian group and let $p$ be a prime number such that $p$ divides $\#(G)$. Then $G$ contains an element of order $p$.

Lemma: Let $G$ be a group, and $H$ and $K$ two subgroups of $G$. Set $X = G/K$, with $G$ acting on $X$ by left multiplication of cosets.

1. Viewing $X$ as an $H$-set by restricting the action to $H$, we have
   $$X^H = \{gK : H \leq gKg^{-1}\}.$$  

2. If in addition $H = K$ and $H$ is finite,
   $$X^H = \{gH : H = gHg^{-1}\}.$$  

Definition: For a subgroup $H$ of a group $G$, the normalizer $N_G(H)$ of $H$ in $G$ is the set
   $$\{g \in G : gHg^{-1} = H\}.$$  

Then $N_G(H) \leq G$, $H \trianglelefteq N_G(H)$, and $H \trianglelefteq G \iff N_G(H) = G$. (2) of the lemma then says: if $X = G/H$, then $X^H = N_G(H)/H$.

Corollary (of (3) of the Sylow theorem): A group $G$ contains exactly one $p$-Sylow subgroup $\iff$ there exists a normal $p$-Sylow subgroup.

Corollary (of (4) of the Sylow theorem): Let $p$ and $q$ be distinct primes. Then a group of order $pq$ is not simple. In fact, if $p < q$, $P$ is a $p$-Sylow subgroup, and $Q$ is a $q$-Sylow subgroup, then $Q \lhd G$, $Q \cap P = \{1\}$, and $G = PQ$. Hence, if $q$ is not congruent to 1 mod $p$, then $P$ is also normal and $G \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Corollary: Let $P$ be a finite group of order $p^r$, where $p$ is a prime number. Then for each $i \leq r$, there exists a subgroup of $P$ of order $p^i$. Thus, if $G$ be a group of order $n = p^rm$, where $r > 0$ and $p$ does not divide $m$, then $G$ has a subgroup of order $p^i$ for $i \leq r$. The case $i = r$ is 1) of the Sylow Theorem and the case $i = 1$ is the general form of Cauchy’s Theorem.