Cavallaro, Jeffery
Math 221a
Homework #2

1.2.1

Let $\phi : G \to H$ be a homomorphism of groups.

a) Prove: $\phi(e_G) = e_H$

   Assume $a \in G$

   $\phi(ae_G) = \phi(a)$
   $\phi(ae_G) = \phi(a)\phi(e_G)$
   $\phi(a)\phi(e_G) = \phi(a)$

   $\phi(e_G a) = \phi(a)$
   $\phi(e_G a) = \phi(e_G)\phi(a)$
   $\phi(e_G)\phi(a) = \phi(a)$

   Thus $\phi(e_G)$ is a two-sided identity for H; however, the identity is unique,
   $\therefore \phi(e_G) = e_H$.

b) Prove: $\phi(a^{-1}) = \phi(a)^{-1}$

   Assume $a \in G$

   $\phi(aa^{-1}) = \phi(e_G) = e_H$
   $\phi(aa^{-1}) = \phi(a)\phi(a^{-1})$
   $\phi(a)\phi(a^{-1}) = e_H$

   $\phi(a^{-1}a) = \phi(e_G) = e_H$
   $\phi(a^{-1}a) = \phi(a^{-1})\phi(a)$
   $\phi(a^{-1})\phi(a) = e_H$

   Thus $\phi(a^{-1})$ is a two-sided identity for $\phi(a)$ in H; however, inverses are unique,
   $\therefore \phi(a^{-1}) = \phi(a)^{-1}$.

c) Let $G = H = \langle \mathbb{Z}_2, \cdot \rangle$ and define $\phi : G \to H$ by $\phi(x) = 0$. G and H are monoids with identity 1 (0 has no inverse). Also:

   $\phi(0x) = \phi(0) = 0 = 00 = \phi(0)\phi(x)$
   $\phi(x0) = \phi(0) = 0 = 00 = \phi(x)\phi(0)$
   $\phi(11) = \phi(1) = 0 = 00 = \phi(1)\phi(1)$

   and so ϕ is a homomorphism. However, $\phi(1) = 0 \neq 1$.

1.2.2

Let G be a group and define $\phi : G \to G$ by $\phi(x) = x^{-1}$.
Prove: G is abelian iff ϕ is an automorphism.

$\implies$ Assume G is abelian

Assume $\phi(x) = \phi(y)$
$x^{-1} = y^{-1}$
$x = y$
$\therefore \phi$ is an injection

Assume $y \in G$
$y^{-1} \in G$
Let $x = y^{-1}$
$\phi(x) = \phi(y^{-1}) = (y^{-1})^{-1} = y$
$\therefore \phi$ is a surjection and thus a bijection

Assume $x, y \in G$
$\phi(xy) = (xy)^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$
$\therefore \phi$ is a homomorphism and thus an isomorphism

$\therefore \phi$ is an automorphism

$\impliedby$ Assume ϕ is an automorphism

Assume $x, y \in G$
ϕ is a homomorphism
$\phi(xy) = \phi(x)\phi(y) = x^{-1}y^{-1} = (yx)^{-1} = \phi(yx)$
But ϕ is a bijection and thus one-to-one, so $xy = yx$
$\therefore G$ is abelian

1.2.5

Let G be a group and $S \subseteq G$ such that $S \neq \emptyset$. Define a relation $\sim$ on G by:

$$a \sim b \iff ab^{-1} \in S$$

Prove: $\sim$ is an equivalence relation $\iff S \leq G$.

$\implies$ Assume $\sim$ is an equivalence relation

S is non-empty by assumption
Assume $a \in S$
$ae^{-1} = ae = a \in S$
So $S = \bar{e}$

Assume $a, b \in S$
$a \sim e$ and $b \sim e$
$e \sim b$ (symmetry)
$a \sim b$ (transitivity)
$ab^{-1} \in S$
$\therefore$ by the yucky subgroup test, $S \leq G$.

$\Longleftarrow$ Assume $S \leq G$

R: Assume $a \in G$

$a^{-1} \in G$
$e \in S$
$aa^{-1} = e \in S$
$\therefore a \sim a$

S: Assume $a \sim b$

$ab^{-1} \in S$
$(ba^{-1})^{-1} \in S$
But S is a group, so $ba^{-1} \in S$
$\therefore b \sim a$

T: Assume $a \sim b$ and $b \sim c$

$ab^{-1} \in S$ and $bc^{-1} \in S$
But S is a group, so by closure, $(ab^{-1})(bc^{-1}) \in S$
$(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = aec^{-1} = ac^{-1} \in S$
$\therefore a \sim c$

$\therefore \sim$ is an equivalence relation.

1.2.6

Let G be a group and let S be a non-empty, finite, subset of G.
Prove: $S \leq G \iff S$ is closed under the induced operation of G.

$\Longrightarrow$ Assume $S \leq G$

S is a group under the induced operation of G
$\therefore S$ is closed under that operation.

$\Longleftarrow$ Assume S is closed under the induced operation of G

S is a finite, non-empty subset of G and closed by assumption
G is associative, and so S is associative
Thus, S is a semigroup
Assume $a, b, c \in S$
Assume $ac = bc$
$a, b, c \in G$
$c^{-1} \in G$
Thus, $a = b$, so right cancellation works
Likewise, assume $ca = cb$
Thus, $a = b$, so left cancellation works
So by HW 1.1.15, S is a group
$\therefore S \leq G$

1.2.9

Let $\phi : G \to H$ be a homomorphism of groups and let $A \leq G$ and $B \leq H$.

a) Prove:

1) $\ker \phi \leq G$

   $\ker \phi = \{a \in G \mid \phi(a) = e_H\}$

   Assume $a, b \in \ker \phi$
   $a, b \in G$
   $ab \in G$
   $\phi(ab) = \phi(a)\phi(b) = e_H e_H = e_H$
   So $ab \in \ker \phi$
   $\therefore \ker \phi$ is closed

   $\ker \phi \subseteq G$
   G is associative
   $\therefore \ker \phi$ is associative

   $\phi(e_G) = e_H$
   $\therefore e_G \in \ker \phi$

   Assume $a \in \ker \phi$
   $a \in G$ and $a^{-1} \in G$
   $\phi(a^{-1}) = \phi(a)^{-1} = e_H^{-1} = e_H$
   $\therefore a^{-1} \in \ker \phi$

   $\therefore \ker \phi \leq G$

2) $\phi^{-1}[B] \leq G$

   $\phi^{-1}[B] = \{a \in G \mid \phi(a) \in B\}$

   $B \leq H$, so $e_H \in B$
   $\phi(e_G) = e_H \in B$
   $\therefore e_G \in \phi^{-1}[B]$ and $\phi^{-1}[B] \neq \emptyset$

   Assume $a, b \in \phi^{-1}[B]$
   $\phi(a) \in B$ and $\phi(b) \in B$ and thus $\phi(a)\phi(b) \in B$
   $a, b \in G$ and thus $ab \in G$
   $\phi(ab) = \phi(a)\phi(b) \in B$
   So $ab \in \phi^{-1}[B]$
   $\therefore \phi^{-1}[B]$ is closed

   $\phi^{-1}[B] \subseteq G$
   G is associative
   $\therefore \phi^{-1}[B]$ is associative

Assume $a \in \phi^{-1}[B]$
$\phi(a) \in B$
But B is a group, so $\phi(a)^{-1} \in B$
$\phi(a)^{-1} = \phi(a^{-1}) \in B$
$\therefore a^{-1} \in \phi^{-1}[B]$

$\therefore \phi^{-1}[B] \leq G$

b) Prove: $\phi[A] \leq H$

$\phi[A] = \{\phi(a) \mid a \in A\}$

$A \leq G$, so $e_G \in A$
$\phi(e_G) = e_H$
$\therefore e_H \in \phi[A]$ and $\phi[A] \neq \emptyset$

Assume $a, b \in \phi[A]$
$\exists\, x, y \in A, \phi(x) = a$ and $\phi(y) = b$
$xy \in A$
$\phi(xy) \in \phi[A]$
$\phi(xy) = \phi(x)\phi(y) = ab \in \phi[A]$
$\therefore \phi[A]$ is closed

$\phi[A] \subseteq H$
H is associative
$\therefore \phi[A]$ is associative

Assume $a \in \phi[A]$
$\exists\, x \in A, \phi(x) = a$
$x^{-1} \in A$
$\phi(x^{-1}) \in \phi[A]$
$\phi(x^{-1}) = \phi(x)^{-1} = a^{-1}$
$\therefore a^{-1} \in \phi[A]$

$\therefore \phi[A] \leq H$

1.2.10

Recall:

$\mathbb{Z}_2 = \{0, 1\}$

$\bigoplus$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

$\implies$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\implies K_4$

So, the possible subgroups are:

$\{e\}$
$\{e, a\}$
$\{e, b\}$
$\{e, c\}$
$\{e, a, b, c\}$

In order to be isomorphic to $\mathbb{Z}_4$, K_4 must be cyclic. However, K_4 has only trivial (order 1) and proper (order 2) cyclic subgroups, and so $K_4 \not\cong \mathbb{Z}_4$.

1.2.11

Let G be group. Prove: $Z(G)$ is an abelian subgroup of G.

$Z(G) = \{a \in G \mid \forall\, x \in G, ax = xa\}$

$e \in G$
$\forall\, x \in G, ex = xe$
$\therefore e \in Z(G)$ and $Z(G) \neq \emptyset$

Assume $a, b \in Z(G)$
$a, b \in G$ and so $ab \in G$
Assume $x \in G$
$(ab)x = axb = x(ab)$
$ab \in Z(G)$
$\therefore Z(G)$ is closed

$Z(G) \subseteq G$
G is associative
$\therefore Z(G)$ is associative

Assume $a \in Z(G)$
$a \in G$ and $a^{-1} \in G$
Assume $x \in G$
$a^{-1}x = (x^{-1}a)^{-1} = (ax^{-1})^{-1} = xa^{-1}$
$\therefore a^{-1} \in Z(G)$

$\therefore Z(G) \leq G$

Assume $a, b \in Z(G)$
$a, b \in G$
By definition, $ab = ba$

$\therefore Z(G)$ is abelian.

1.2.13

Let $\phi : G \to H$ be a homomorphism of groups and $G = \langle a \rangle$.
Prove: ϕ is completely determined by $\phi(a)$

Lemma

Let $\phi : G \to H$ be a homomorphism of groups:

$$\forall\, a \in G, \forall\, n \in \mathbb{Z}, \phi(a^n) = \phi(a)^n$$

Proof

Assume $a \in G$
Assume $n \in \mathbb{Z}$

Case 1: $n > 0$

Proof by induction on n

Base: $n = 1$

$$\phi(a^1) = \phi(a) = \phi(a)^1$$

Assume $\phi(a^n) = \phi(a)^n$

Consider $\phi(a^{n+1})$

$$\phi(a^{n+1}) = \phi(a^n a) = \phi(a^n)\phi(a) = \phi(a)^n\phi(a) = \phi(a)^{n+1}$$

Case 2: $n = 0$

$$\phi(a^0) = \phi(e_G) = e_H = \phi(a)^0$$

Case 3: $n < 0$

Let $m = -n > 0$
$\phi(a^n) = \phi(a^{-m}) = \phi((a^{-1})^m) = \phi(a^{-1})^m = (\phi(a)^{-1})^m = \phi(a)^{-m} = \phi(a)^n$

Now, assume $b \in H$
$\exists\, a^n \in G, \phi(a^n) = \phi(a)^n = b$
$\therefore \phi$ is completely determined by $\phi(a)$

1.2.15

Let G be a group and $\mathrm{Aut}\, G$ be the set of all automorphisms of G.

a) Prove: $\mathrm{Aut}\, G$ is a group under composition.

Note that the identify function $i_G \in \mathrm{Aut}\, G$ so $\mathrm{Aut}\, G \neq \emptyset$.

Assume $\sigma, \tau \in \operatorname{Aut}(G)$
σ and τ are bijections, so $\sigma\tau$ is also a bijection
σ and τ are homomorphisms
Assume $x, y \in G$
$xy \in G$
$(\sigma\tau)(xy) = \sigma[\tau(xy)] = \sigma[\tau(x)\tau(y)] = \sigma[\tau(x)]\sigma[\tau(y)] = [(\sigma\tau)(x)][(\sigma\tau)(y)]$
So $\sigma\tau$ is also a homomorphism, and thus an isomorphism, and thus an automorphism
$\therefore \operatorname{Aut} G$ is closed

Composition is associative

Assume $\sigma \in \operatorname{Aut} G$
σ is a bijection, and so σ^{-1} exists such that $\sigma\sigma^{-1} = \sigma^{-1}\sigma = i_G$
$\therefore \operatorname{Aut} G$ has inverses

$\therefore \operatorname{Aut} G$ is a group

b) Prove:

1) $\operatorname{Aut} \mathbb{Z} \simeq \mathbb{Z}_2$

Since $\mathbb{Z}$ has two generators: ± 1, the possible automorphisms are defined by: $\phi_1(1) = 1$ (identity) and $\phi_{-1}(1) = -1$:

$\phi_1(n) = n$
$\phi_{-1}(n) = -n$
$(\phi_{-1}\phi_{-1})(n) = -(-n) = n = \phi_1(n)$

$\circ$	ϕ_1	ϕ_{-1}
ϕ_1	ϕ_1	ϕ_{-1}
ϕ_{-1}	ϕ_{-1}	ϕ_1

$\simeq$

+	0	1
0	0	1
1	1	0

$= \mathbb{Z}_2$

2) $\operatorname{Aut} \mathbb{Z}_6 \simeq \mathbb{Z}_2$

Since $\mathbb{Z}_6$ has two generators: $1, 5$, the possible automorphisms are defined by: $\phi_1(1) = 1$ (identity) and $\phi_5(1) = 5$:

$\phi_1(n) = n$
$\phi_5(n) = 5n$
$(\phi_5\phi_5)(n) = 5(5n) = n = \phi_1(n)$

$\circ$	ϕ_1	ϕ_5
ϕ_1	ϕ_1	ϕ_5
ϕ_5	ϕ_5	ϕ_1

$\simeq$

+	0	1
0	0	1
1	1	0

$= \mathbb{Z}_2$

3) $\operatorname{Aut} Z_8 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Since $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \simeq K_4$, it is sufficient to show that $\operatorname{Aut} Z_8 \simeq K_4$.

Since $\mathbb{Z}_8$ has four generators: $1, 3, 5, 7$, the possible automorphisms are defined by: $\phi_1(1) = 1$ (identity), $\phi_3(1) = 3$, $\phi_5(1) = 5$, and $\phi_7(1) = 7$:

$\phi_1(n) = n$
$\phi_3(n) = 3n$
$\phi_5(n) = 5n$
$\phi_7(n) = 7n$

So $\operatorname{Aut} \mathbb{Z}_8$ is a group of order 4, and thus must be isomorphic to either $\mathbb{Z}_4$ or K_4. But:

$(\phi_1\phi_1)(n) = n = \phi_1(n)$
$(\phi_3\phi_3)(n) = 3(3n) = n = \phi 1(n)$
$(\phi_5\phi_5)(n) = 5(5n) = n = \phi 1(n)$
$(\phi_7\phi_7)(n) = 7(7n) = n = \phi 1(n)$

So each element in the group is its own inverse, indicating that $\operatorname{Aut} \mathbb{Z}_8 \simeq K_4$.

4) $\operatorname{Aut} Z_p \simeq \mathbb{Z}_{p-1}$, where p is prime

Since p is prime, all non-zero elements of $\mathbb{Z}_p$ are relatively prime with p, and so $\mathbb{Z}_p$ has $p-1$ generators. Each generator corresponds to an automorphism determined by $\sigma_k(1) = k$ where $1 \leq k \leq p-1$:

$\sigma_k(n) = kn$

So $\operatorname{Aut} Z_p$ is a group under composition of order $p-1$.

Let $\sigma_h, \sigma_k \in \operatorname{Aut} Z_p$
$(o_h o_k)(n) = h(kn) = (hk)n = \sigma_{hk}(n)$

Define $\phi : \operatorname{Aut} Z_p \to \left\langle \mathbb{Z}_p^*, \cdot \right\rangle$ by $\phi(\sigma_k) = k$
ϕ is clearly bijective
Assume $\sigma_h, \sigma_k \in \operatorname{Aut} Z_p$
$\phi(\sigma_h\sigma_k) = \phi(\sigma_{hk}) = hk = \phi(\sigma_h)\phi(\sigma_k)$
So p is a homomorphism and thus an isomorphism

So $\operatorname{Aut} Z_p \simeq \left\langle \mathbb{Z}_p^*, \cdot \right\rangle$; however, $\left\langle \mathbb{Z}_p^*, \cdot \right\rangle$ is cyclic of order $p-1$ and is thus isomorphic to $\mathbb{Z}_{p-1}$.

$\therefore \operatorname{Aut} Z_p \simeq \mathbb{Z}_{p-1}$

c) Describe $\operatorname{Aut} Z_n$

Let $\mathbb{Z}_n^\times = \{k \in \mathbb{N} \mid 1 \leq k < n \text{ and } (k, n) = 1\}$.

Claim: $\langle \mathbb{Z}_n^\times, \cdot \rangle$ is a group:

$(1, n) = 1$ and thus $1 \in \mathbb{Z}_n^\times$ and $\mathbb{Z}_n^\times \neq \emptyset$

Assume $h, k \in \mathbb{Z}_n^\times$
$(h, n) = 1$ and $(k, n) = 1$
ABC: $hk \notin \mathbb{Z}_n^\times$
$n \mid hk$
But $n \nmid h$, so $n \mid k$

Contradiction!
$\therefore hk \in \mathbb{Z}_n^\times$ and $\mathbb{Z}_n^\times$ is closed

Multiplication $\pmod n$ is associative

Assume $m \in \mathbb{Z}_n^\times$
$(m, n) = 1$
$\exists h, k \in \mathbb{Z}_n^\times, hm + kn = 1$
But $kn = 0$, so $hm = 1$
$h = m^{-1} \in \mathbb{Z}_n^\times$
(Hmm: we did this in class, but how do we know that $h, k \in \mathbb{Z}_n^\times$?)

$\therefore \langle \mathbb{Z}_n^\times, \cdot \rangle$ is a group

Now, consider $\operatorname{Aut} Z_n$. It will have $\phi(n)$ generators, where $\phi(n)$ is the Euler totient function. Each generator is defined by $o_k(1) = k$, where $1 \leq k < n$ and $(k, n) = 1$, and so the k are indeed the set $\mathbb{Z}_n^\times$, which is closed under multiplication.

$\sigma_k(n) = kn$

Assume $\sigma_h, \sigma_k \in \operatorname{Aut} Z_n$
$h, k \in \mathbb{Z}_n^\times$
$hk \in \mathbb{Z}_n^\times$
$(\sigma_h \sigma_k)(n) = h(kn) = (hk)n = \sigma_{hk}(n)$

Define $\phi : \operatorname{Aut} Z_n \to \mathbb{Z}_n^\times$ by $\phi(\sigma_k) = k$
ϕ is clearly bijective
$\phi(\sigma_h \sigma_k) = \phi(\sigma_{hk}) = hk = \phi(\sigma_h)\phi(\sigma_k)$
Thus ϕ is a homomorphism, and thus an isomorphism

$\therefore \operatorname{Aut} Z_n \simeq \langle \mathbb{Z}_n^\times, \cdot \rangle$