Homework 2
Solutions

(1) (a) Let σ be the m-cycle $(a_1 a_2 \dots a_m)$ in S_n. Show that $|\sigma| = m$.
(b) Show that the order of an element in S_n is the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof:
(a) It is easy to see that $\sigma^i(a_k) = a_{k+i}$ where the indices are taken modulo m. Hence $\sigma^m = 1$ and since all a_k are distinct m is the smallest such integer. This implies $|\sigma| = m$.
(b) Let $\sigma \in S_n$ and let $c_1 \cdots c_k$ be the cycle decomposition of σ where c_i is a cycle of length m_i and all c_i are disjoint. Then the c_i commute and $\sigma^m = c_1^m \cdots c_k^m$. By part (a) $c_i^{m_i} = 1$ and hence $\sigma^m = 1$ if and only if m_i divides m for all i. Since σ is the least such m the conclusion follows.

(2) Let $\phi : G \to H$ be a homomorphism of groups, A a subgroup of G, and B a subgroup of H. Show that
(a) $\ker\phi$ and $\phi^{-1}(B) = \{a \in G \mid \phi(a) \in B\}$ are subgroups of G.
(b) $\phi(A)$ is a subgroup of H.

Proof:
(a) Recall that $\ker\phi = \{a \in G \mid \phi(a) = 1\}$. Let $a, b \in \ker\phi$. Then $\phi(ab) = \phi(a)\phi(b) = 1$ so that $ab \in \ker\phi$. Certainly $1 \in \ker\phi$. Finally, if $a \in \ker\phi$ then $\phi(a^{-1}) = \phi(a)^{-1} = 1$ so that $a^{-1} \in \ker\phi$. This proves that $\ker\phi$ is a subgroup of G. Since B is a subgroup of H, $1_H \in B$. And since $\phi(1_G) = 1_H \in B$ it follows that $1_G \in \phi^{-1}(B)$. Let $a, b \in \phi^{-1}(B)$. Then $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} \in B$ since $\phi(a), \phi(b) \in B$ and B is a subgroup of H. This shows that $\phi^{-1}(B)$ is a subgroup of G.
(b) Recall that $\phi(A) = \{b \in H \mid b = \phi(a) \text{ for some } a \in A\}$. Since A is a subgroup of G it follows that $1_G \in A$ and hence $1_H \in \phi(A)$. Suppose $g, h \in \phi(A)$. Then by definition there exist $a, b \in A$ such that $g = \phi(a)$ and $h = \phi(b)$. Hence $gh^{-1} = \phi(a)\phi(b)^{-1} = \phi(ab^{-1})$ since ϕ is a homomorphism.

Now $ab^{-1} \in A$ since A is a subgroup of G and therefore $gh^{-1} \in \phi(A)$ which proves that $\phi(A)$ is a subgroup of H.

(3) Dummit, Foote I.1.7 Exercise 18 (page 45)

Proof:

(1) Symmetry: We have $a \sim a$ since $a = 1 \cdot a$.

(2) Reflexivity: We need to show that $a \sim b$ implies $b \sim a$. If $a \sim b$ then there exists some $h \in H$ such that $a = h \cdot b$. Then $h^{-1} \cdot a = h^{-1}(h \cdot b) = (h^{-1}h) \cdot b = 1 \cdot b = b$.

(3) Transitivity: We need to show that $a \sim b$, $b \sim c$ implies $a \sim c$. By $a \sim b$ we have $a = h \cdot b$ for some h and by $b \sim c$ we have $b = g \cdot c$ for some g. Hence $a = h \cdot b = h(g \cdot c) = (hg) \cdot c$.

(4) Dummit, Foote I.1.7 Exercise 19 (page 45)

Proof: For $x \in G$ the orbit of x under H is $\mathcal{O} = \{hx \mid h \in H\}$. The claim is that the map $H \to \mathcal{O}$ which maps $h \mapsto hx$ is a bijection. For injectivity let $h, g \in H$ such that $hx = gx$. The cancellation law implies $h = g$. For surjectivity let $p \in \mathcal{O}$. Then by definition, there exists a $h \in H$ such that $p = hx$.

Now we want to prove Lagrange's theorem which says that if G is finite and $H \leq G$, then $|H|$ divides $|G|$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be the orbits of the action of H on G which partition G. That is, let x_i be a representative of $\mathcal{O}_i$ so that $\mathcal{O}_i = \{hx_i \mid h \in H\}$. Then $G = \cup_i \mathcal{O}_i$ is the disjoint union of the orbits. By the above arguments H is in bijection with each $\mathcal{O}_i$ which implies in particular that $|H| = |\mathcal{O}_i|$. Hence $|G| = |\mathcal{O}_1| + \cdots + |\mathcal{O}_k| = k|H|$.

(5) Let G and H be groups. Define the direct product of G and H to be the set $G \times H$ with binary operation

$$(a, b)(a', b') = (aa', bb') \qquad \text{where } a, a' \in G \text{ and } b, b' \in H.$$

(a) Show that $G \times H$ is a group.

(b) Let $\langle a \rangle$ and $\langle b \rangle$ be finite cyclic groups of orders m and n, respectively, which are relatively prime. Prove that $\langle a \rangle \times \langle b \rangle$ is cyclic.

(c) What about the converse?

Proof:

(a) $(1, 1)$ is the identity in $G \times H$, and (a^{-1}, b^{-1}) is the inverse of the element (a, b). Associativity follows from the associativity of G and H.

(b) We claim that $\langle a \rangle \times \langle b \rangle = \langle (a, b) \rangle$. Let μ denote the least common multiple of m and n. Note that $(a, b)^\mu = (1, 1)$ so that $|(a, b)| \leq \mu$. However, if $(a, b)^k = (1, 1)$, then $m|k$ and $n|k$ and hence $\mu|k$ so that $k \geq \mu$. It follows that

$|(a,b)| = \mu = mn$ since $(m,n) = 1$. Clearly $|\langle a\rangle \times \langle b\rangle| = mn$ so that (a,b) is a generator.

(c) The converse is true. Suppose that $|a| = m$ and $|b| = n$ and $(m,n) = d > 1$. Then $\langle a\rangle \times \langle b\rangle$ has the non-cyclic subgroup $G = \langle a^{m/d}\rangle \times \langle b^{n/d}\rangle \equiv (\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/d\mathbb{Z})$, so $\langle a\rangle \times \langle b\rangle$ is not cyclic.

(6) Dummit, Foote I.2.2 Exercise 10 (page 54)

Proof: If $H \leq G$ and $|H| = 2$ then $H = \{1, a\}$ where $1 \neq a$. Recall that

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$
$$C_G(H) = \{g \in G \mid ghg^{-1} = h\}$$

Certainly, $g1g^{-1} = 1$. Hence $gHg^{-1} = H$ implies that $gag^{-1} = a$. This proves that $N_G(H) = C_G(H)$. If $N_G(H) = G$ then by the previous arguments also $C_G(H) = G$ so that $1, a$ commute with all elements in G. Hence they are in the center of G.

(7) Dummit, Foote I.2.3 Exercise 26 (page 62)

Proof:

(a) First of all, it is clear that σ_a is a homomorphism since $\sigma_a(x^\alpha x^\beta) = \sigma_a(x^{\alpha+\beta}) = x^{a(\alpha+\beta)} = x^{a\alpha}x^{b\beta} = \sigma_a(x^\alpha)\sigma_a(x^\beta)$. If $(a,n) = 1$ then we can write $\alpha a + \beta n = 1$ for some integers α, β so that $\alpha a = -\beta n + 1$. Hence $\sigma_a(x^\alpha) = x$ since $x^n = 1$. Since σ_a is a homomorphism and x generates Z_n this implies that σ_a is surjective, and since the order of Z_n is finite this also implies that σ_a is an automorphism. Conversely assume that $(a,n) \neq 1$ and let $d = (a,n) > 1$. Then $a = kd$ and $n = \ell d$ for some k and ℓ. Then $\sigma_a(x^\ell) = x^{a\ell} = x^{kn} = 1$. Since $1 \leq \ell < n$ it follows that $x^\ell \neq 1$ and hence $\ker\sigma_a \neq \{1\}$. Hence by a theorem proved in class σ_a is not a monomorphism, and hence no automorphism.

(b) Since σ_a is a homomorphism and x generates Z_n, $\sigma_a = \sigma_b$ if and only if $\sigma_a(x) = \sigma_b(x)$. Since $1, x, x^2, \ldots, x^{n-1}$ are distinct elements of Z_n this in turn is equivalent to $a \equiv b \bmod n$.

(c) Since x generates Z_n each automorphism of Z_n is specified by saying which element x is mapped to. All elements in Z_n are of the form x^a. Hence every automorphism of Z_n must be σ_a for some a.

(d) Again, since x generates Z_n and σ_a is a homomorphism, it suffices to show $\sigma_a \circ \sigma_b = \sigma_{ab}$ applied to x. We have $\sigma_a \circ \sigma_b(x) = \sigma_a(x^b) = (\sigma_a(x))^b = (x^a)^b = x^{ab} = \sigma_{ab}(x)$.

By problem (2a) on homework 1, the elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ are those $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ such that $(a, n) = 1$. By parts (a)-(c) we have $Z_n = \{\sigma_a \mid (a, n) = 1\}$. Hence $\sigma_a \circ \sigma_b = \sigma_{ab}$ implies that $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n)$ given by $\bar{a} \mapsto \sigma_a$ is an isomorphism.