# SELECTED SOLUTIONS - MATH 330 - FALL 2012

ALEXANDER J STATHIS

Contents

## Chapter 2

**2.19.** Let $X = \{\text{rock}, \text{paper}, \text{scissors}\}$. Recall the game whose rules are: paper dominates rock, rock dominates scissors, and scissors dominates paper. Draw a subset of $X \times X$ showing that domination is a relation on $X$.

To be honest, I'm not really sure what it means to "draw a subset of $X \times X$ showing that domination is a relation on $X$." Accordingly, this may not be the intended solution.

| $*$ | $r$ | $p$ | $s$ |
|---|---|---|---|
| $r$ | | | • |
| $p$ | • | | |
| $s$ | | • | |

is a graph of $X \times X$ where the relation is given by the pairs indicated by the bullets. In words, the relation is given by $rRs$, $pRr$, and $sRp$.

**2.22.** Find $\operatorname{sgn}(\alpha)$ and $\alpha^{-1}$, where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

We begin by rewriting $\alpha$ as the cycle $(19)(28)(37)(46)$. Because $\alpha$ is written as four 2-cycles, we know that $\alpha$ is an even permutation and that $\operatorname{sgn}(\alpha) = 1$. We also notice that all the 2-cycles of $\alpha$ are disjoint, so that

$$\alpha^2 = (19)(28)(37)(46)(19)(28)(37)(46) = (19)(19)(28)(28)(37)(37)(46)(46) = (1),$$

and $\alpha = \alpha^{-1}$.

**2.25.**

(a) If $\alpha$ is an $r$-cycle, show that $\alpha^r = (1)$.

*Proof.* Suppose $\alpha$ is the $r$-cycle represented as $(a_0 a_1 a_2 \dots a_{r-1})$. We will show by induction $n$ that the image of $a_k$ under $\alpha^n$ is $a_d$ where $d = k + n \pmod r$.

For the base case when $n = 1$, the result is clear: $a_k$ is mapped to $a_{k+1}$ except in the case when $k = r - 1$. In this case, $k + 1 = r$ which is $0 \pmod r$.

The induction step is just as easy. Assume that the result is true for $n$. The image $\alpha^{n+1}(a_k)$ can be rewritten as $\alpha(\alpha^n(a_k))$. Applying our inductive hypothesis, we see that $\alpha^{n+1}(a_k)$ is going to be $\alpha(a_d)$ where $d \equiv k + n \pmod r$ and $0 \leq d < r$. In particular, we have that $d + 1 \equiv k + (n + 1) \pmod r$. Applying $\alpha$ to $a_d$ we find that the image of $a_d$ is $a_{d+1}$ if $d < r - 1$ and $a_0$ otherwise. Specifically, the image of $a_k$ under $\alpha^r$ is $a_l$ where $l \equiv d + 1 \equiv k + (n + 1) \pmod r$, as required.

Now we shall investigate $\alpha^r(a_k)$. By our lemma, we see that $\alpha^r(a_k) = a_d$ where $d = k + r \pmod r$. In particular, $d = k$, and $\alpha^r(a_k) = a_k$ for all $0 \leq k < r$. In other words, $\alpha^r = (1)$. □

(b) If $\alpha$ is an $r$-cycle, show that $r$ is the smallest positive integer $k$ such that $\alpha^k = (1)$.

*Proof.* Using the setup and the lemma we proved above, let $d < r$. We will show that $\alpha^d \neq (1)$. Specifically, notice that $\alpha^d(a_0) = a_d$, since $d < r$. Since the $a_i$ are all distinct, we have that $\alpha^d \neq r$. Hence, $r$ is the least positive integer with $\alpha^r = (1)$. □

**2.27.** Given $X = \{1, 2, \dots, n\}$, let us call a permutation $\tau$ of $X$ an *adjacency* if it is a transposition of the form $(i\, i+1)$ for $i < n$. If $i < j$, prove that $(i\, j)$ is a product of an odd number of adjacencies.

*Proof.* We prove a stronger result from which the required one should be evident. We will show that the transposition $(ij)$ can be written as the product of transpositions

$$((j-1)j)((j-2)(j-1)) \cdots ((i+1)(i+2))(i(i+1))((i+1)(i+2)) \cdots ((j-2)(j-1))((j-1)j),$$

and the proof proceeds by induction on the difference $j - i$. The base case $j - i = 1$ is clear since the transposition in that case is $(ij)$.

Assume that the result holds for all transpositions $(ab)$ with $b - a = k$ and suppose that $(ij)$ is a transposition such that $j - i = k + 1$. We notice that

$$(ij) = ((j-1)j)(i(j-1))((j-1)j),$$

and apply the inductive hypothesis to $(i(j-1))$ to finish the proof. □

**2.31.**

(a) Prove, for all $i$, that $\alpha \in S_n$ moves $i$ if and only if $\alpha^{-1}$ moves $i$.

*Proof.* Let $j$ be the image of $i$ under $\alpha$. Now assume that $\alpha^{-1}$ does not move $i$, so that $\alpha^{-1}(i) = i$. Composing the two

$$i = [\alpha \circ \alpha^{-1}](i) = \alpha(\alpha^{-1}(i)) = \alpha(i) = j,$$

so we see that $\alpha$ does not move $i$ either.

The other direction is analogous: in the proof above, choose $\alpha = \beta^{-1}$ for some $\beta \in S_n$ and notice that $(\beta^{-1})^{-1} = \beta$. □

(b) Prove that if $\alpha, \beta \in S_n$ are disjoint and if $\alpha\beta = (1)$, then $\alpha = (1)$ and $\beta = (1)$.

*Proof.* By the assumptions, we know that $\beta = \alpha^{-1}$. By part $(a)$, we know that if $\alpha$ moves some element $i$, then $\beta = \alpha^{-1}$ must also move $i$. In particular, if they are disjoint, neither must move any element, so both must be the identity. □

**2.36.** True or false with reasons.

(a) The function $e : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $e(m, n) = m^n$, is associative.
False. Try 2, 2, 3.

(b) Every group is abelian.
False. $S_3$.

(c) The set of all positive real numbers is a group under multiplication.
True. (Prove it!)

(d) The set of all positive real numbers is a group under addition.
False. For $a \in \mathbb{R}^+$, $-a \notin \mathbb{R}^+$.

(e) For all $a, b \in G$, where $G$ is a group, $aba^{-1}b^{-1} = 1$.
False, this would imply that $ab = ba$, or that the group is abelian.

(f) Every permutation of the vertices $v_1, v_2, v_3$ of an equilateral triangle $\pi_3$ is the restriction of a symmetry of $\pi_3$.
True.

*Proof.* The group of symmetries is a group of order six contained in the group of permutations on three letters. Since the permutation group on three letters has order six, it follows that they are equal, and that every such permutation can be obtained as a symmetry of $\pi_3$. □

(g) Every permutation of the vertices $v_1, v_2, v_3, v_4$ of a square $\pi_4$ is the restriction of a symmetry of $\pi_4$.
False. If we arrange the square as follows

$$\begin{array}{ccc} v_1 & \longrightarrow & v_2 \\ \uparrow & & \downarrow \\ v_4 & \longleftarrow & v_3 \end{array},$$

then with the rotation going in the direction of the arrows and the flip being about the vertical axis through the center of the square, then the permutation $v_1v_3v_2v_4$ cannot be obtained from rotations and flips.

(h) If $a, b \in G$, where $G$ is a group, then $(ab)^n = a^n b^n$ for all $n \in N$.
False, this would imply that the group is abelian.

(i) Every infinite group contains an element of infinite order.

False, but I'm not sure how to prove it given the information available to us currently. Otherwise, the infinite direct sum of copies of $\mathbb{Z}/2$ suffices.

(j) Complex conjugation permutes the roots of every polynomial having real coefficients.

True, if a polynomial has real coefficients, yet does not factor completely over $\mathbb{R}$, then its set of roots must contain pairs of complex conjugates, so the action of complex conjugation on the roots of a polynomial with real coefficients is well defined.

**2.37.** If $a_1, \ldots, a_n$ are (not necessarily distinct) elements in a group $G$, prove that

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^1 a_{n-1}^{-1} \cdots a_1^{-1}.$$

*Proof.* The proof proceeds by induction on $n$. For the case when $n = 1$, the result is clear. In the case when $n = 2$, we let $a, b \in G$. It follows that $ab(ab)^{-1} = 1$, so that we may multiply first by $a^{-1}$ on the left and then finally by $b^{-1}$ on the left again to obtain $(ab)^{-1} = b^{-1}a^{-1}$.

Assume the statement is true for $k < n$ and suppose $n \geq 3$. Let $a_1, \ldots, a_n$ be elements of $G$. We first note that the product $a_1 \cdots a_n$ may be written as the product $(a_1 \cdots a_{n-1})a_n$. In particular, we have that we may apply the inductive hypothesis for $k = 2$ to this product to obtain

$$(a_1 \cdots a_n)^{-1} = ((a_1 \cdots a_{n-1})a_n)^{-1} = a_n^{-1}(a_1 \cdots a_{n-1})^{-1}.$$

We may then apply the inductive hypothesis for $k = n - 1$ to $(a_1 \cdots a_{n-1})^{-1}$ to find that

$$a_n^{-1}(a_1 \cdots a_{n-1})^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1},$$

as desired. □

**2.39.**

(a) How many elements of order 2 are there in $S_5$ and $S_6$?

We will solve the more general problem below, but you should work these things out in cases of small order first to gain an intuition.

(b) How many elements of order 2 are there in $S_n$?

*Proof.* We have that an element of order two in $S_n$ must be the product of disjoint transpositions, and therefore must be of the cycle type

$$(a_1 a_2)(a_3 a_4) \cdots (a_{j-1} a_j)(a_{j+1}) \cdots (a_n).$$

The maximum number of disjoint two cycles that such an element of $S_n$ can contain is $\lfloor \frac{n}{2} \rfloor$ where $\lfloor * \rfloor$ is the floor function. Assume that $m$ is the number of disjoin two cycles in a given cycle type. The number of elements remaining is $n - 2m$ which can be arranged in any order to achieve the same element in $S_n$. Similarly, each two cycle may be written in two distinct ways, and all the two cycles may be arranged in $m!$ ways to achiave the same element of $S_n$. Therefore, there are

$$\frac{n!}{2m \cdot m! \cdot (n-2m)!}$$

such cycles of this type. Taking the sum from $m = 1$ to $m = \lfloor \frac{n}{2} \rfloor$ gives

$$\sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{2m \cdot m! \cdot (n-2m)!}$$

elements of order two. □

**2.40.** Let $G$ be a group and $y \in G$ have order $m$. If $m = dt$ for some $d \geq 1$, prove that $y^t$ has order $d$.

*Proof.* First,

$$1 = y^m = y^{dt} = (y^t)^d,$$

so that $\#(y^t) \leq d$. Assume that there is some natural number $e$ for which $(y^t)^e = 1$ with $e < d$. In this case, the product $te < td = m$ since $e < d$, but

$$1 = (y^t)^e = y^{te}$$

which contradicts that $y$ has order $m$. Hence, there is no such $e$ and $d$ is the order of $y^t$. □

**2.41.** Let $G$ be a group and let $a \in G$ have order $dk$, where $d, k > 1$. Prove that if there is $x \in G$ with $x^d = a$, then the order of $x$ is $d^2k$. Conclude that the order of $x$ is larger than the order of $a$.

*Proof.* Let $x \in G$ be such an element, so that $x^{d^2k} = (x^d)^{dk} = a^{dk} = 1$. Suppose there is some integer $e \leq d^2k$ such that the order of $x$ is $e$. It follows that $a^e = (x^d)^e = (x^e)^d = 1$ and therefore $dk \mid e$. Let $e = bdk$ for some natural number $b$, then $1 = x^e = x^{bdk} = (x^d)^{bk} = a^{bk}$ implies that $dk \mid bk$ and therefore that $d \mid b$. Hence, $e = cd^2k$ for some natural number $c$. But $e \leq d^2k$, so $c = 1$ and $e = d^2k$. □

**2.42.** Let $G = GL(2, \mathbb{Q})$, and let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Show that $A^4 = I = B^6$, but that $(AB)^n \neq I$ for all $n > 0$. Conclude that $AB$ can have infinite order even though both factors $A$ and $B$ have finite order (this cannot happen in a finite group).

*Proof.* For the first part, just compute it:

$$A^4 = (A^2)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = I,$$

and

$$B^6 = (B^2)^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = I.$$

To see that $AB^n \neq I$ for any $n > 0$, we prove the stronger result that

$$AB^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

by induction on $n$. The base case is trivial since

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

For the induction step, assume that the result holds for $n$, then

$$AB^{n+1} = AB^n \cdot AB = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(n+1) \\ 0 & 1 \end{pmatrix}$$

by the inductive hypothesis.

We conclude the last part due to the counter example we just computed. □

**2.43.**

(a) Prove, by induction on $k \geq 1$, that

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}.$$

*Proof.* The base case when $k = 1$ is obvious. Now suppose that the hypothesis holds for arbitrary $k$, and notice that

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{k+1} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k \cdot \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} \cdot \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

by the inductive hypothesis. Now perform the multiplication to achieve the matrix

$$\begin{pmatrix} \cos k\theta\cos\theta - \sin k\theta\sin\theta & -\sin\theta\cos k\theta - \sin k\theta\cos\theta \\ \cos k\theta\sin\theta + \sin k\theta\cos\theta & -\sin k\theta\sin\theta + \cos k\theta\cos\theta \end{pmatrix},$$

and apply the angle sum and difference identities to obtain the result. □

(b) Find all the element of finite order in $SO(2, \mathbb{R})$, the special orthogonal group.

*Proof.* We know that $SO(2, \mathbb{R})$ is all matrices representing rotation about the origin by some angle $\theta$. By what we did above, we see that only rotations such that $k\theta = 2\pi l$ for some $l \in \mathbb{Z}$ will have finite order, and therefore rotations by angles $2\pi q$ for $q \in \mathbb{Q}$ will have finite order. □

**2.44.** If $G$ is a group in which $x^2 = 1$ for every $x \in G$, prove that $G$ must be abelian.

*Proof.* Let $a, b \in G$. We must show that $a$ and $b$ commute. Notice that the requirement that $x^2 = 1$ for all $x \in G$ is equivalent to saying that $x$ is its own inverse for all $x \in G$. Hence,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1} = ba,$$

so the two commute. Since our choice of $a, b \in G$ was arbitrary, we are done. □

**2.46.** If $G$ is a group with an even number of elements, prove that the number of elements in $G$ of order 2 is odd. In particular, $G$ must contain an element of order 2.

*Proof.* We define a relation '!' on $G$ such that $a!b$ if $b = a^{-1}$ or if $b = a$. In this way, '!' is an equivalence relation: $a!a$ by definition, $a!b$ implies that $a = b$ or $b = a^{-1}$ so that in either case $b!a$, and $a!b$ with $b!c$ gives that $a = b$ or $b = a^{-1}$ and $b = c$ or $c = b^{-1}$ so that in any case $a!c$. We have then that $G$ is represented as the disjoint union of equivalence classes as dictated by '!'.

Each equivalence class has either one or two elements. Let $k$ be the number of equivalence classes with two elements, let $2n = \#G$, and let $m$ be the number of equivalence classes with a single element. We know that $m \geq 1$ since the identity is its own inverse. It follows that

$$m = 2n - 2k = 2(n - k)$$

is even, so $m - 1$ is odd and there are an odd number of elements of order two. □

**2.48.** The *stochastic group* $\Sigma(2,\mathbb{R})$ consists of all those matrices in $GL(2,\mathbb{R})$ whose column sums are 1; that is, $\Sigma(2,\mathbb{R})$ consists of all the nonsingular matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ with $a+b=1=c+d$.

Prove that the product of two stochastic matrices is again stochastic, and that the inverse of a stochastic matrix is stochastic.

*Proof.* We first show that the subset of stochastic matrices is closed. Let

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \text{ and } \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

be stochastic matrices so that $a+b=c+d=x+z=y+w=1$. Their product is

$$\begin{pmatrix} ax+cz & ay+cw \\ bx+dz & by+dw \end{pmatrix}$$

with

$$(ax+cz)+(bx+dz) = x(a+b)+z(c+d) = x+z = 1$$

and

$$(ay+cw)+(by+dw) = y(a+b)+w(c+d) = y+w = 1.$$

Hence, the product of any two stochastic matrices is stochastic.

Using the $a, c, b, d$ matrix above, its inverse is

$$\frac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

whose left column sums to

$$\frac{d-b}{ad-bc}.$$

However, since $c+d=1$, we have that $d=1-c$ and $ad-bc = a(1-c)-bc = a-c(a+b) = a-c$ while $a+b-(c+d)=0$ so $a-c=d-b$ and the fraction above is equal to one. The right column is analogous, so that we have that the stochastic matrices are closed under inverses and are therefore a subgroup of $GL(2,\mathbb{R})$. □

**2.49.** Show that the symmetry group $\Sigma(C)$ of a circle $C$ is infinite.

*Proof.* We need only exhibit an infinite number of isometries of the plane $\mathbb{R}^2$ such that their restriction to the circle is an automorphism. To do this, we make the simple observation that rotations around the origin are isometries of the plane which are automorphisms of the circle, and two rotations by the angles $\sigma$ and $\theta$ are equal only when $\sigma = \theta + 2k\pi$ for $k \in \mathbb{Z}$. In particular, any angle $0 \leq \theta < 2\pi$ incduces a unique automorphism of the circle, which completes the proof. □

**2.50.** Prove that every element in a dihedral group $D_{2n}$ has a unique factorization of the form $a^i b^j$, where $0 \leq i < n$ and $j = 0$ or 1.

*Proof.* This problem is frustrating without the language of free groups and presentations, but we are able to do it anyways.

We let $a, b$ be as in the definition of the dihedral group, so that it only remains to show that any sequence $a^{i_1}b^{j_1}a^{i_2}b^{j_2}\cdots a^{i_k}b^{j_k}$ can be rewritten as required with $i_l, j_l$ as nonnegative integers and $0 \leq i_l < n$ and $0 \leq j_l < 2$ for each $1 \leq l \leq k$. Notice that any element of the dihedral group as we've defined it can be written uniquely this way, possibly with $i_1 = 0$ or $j_k = 0$ and with no other $i_l, j_l$ equal to zero. To show this, we induct on $k$, and the base case is trivial.

For the inductive step, assume that the result holds for $k$, and we will show the $k+1$ case. Let $a^{i_1}b^{j_1}a^{i_2}b^{i_2}\cdots a^{i_k}b^{i_k}$ be such a sequence. We apply our inductive hypothesis to the $k_1$ part to achieve a representation for our sequence as

$$a^m b^p a^{i_k} b^{j_k}$$

with $0 \leq m < n$ and $p = 0$ or $p = 1$. If $p \leq j_k$, then we are done, as we simply apply the relation $bab = a^{-1}$ the lesser of $p$ or $i_k$ times and then the relation $a^n = 1$ to achieve the required representation. In the other case, let $x = \min\{i_k, j_k\}$ we're left with the product

$$a^m b^{p-x} a^{i_k - x}.$$

If $x = i_k$, we're again done, so assume that $i_k - j_k > 0$. We can derive the relation $aba = b$ from $bab = a^{-1}$ and apply this the required number of times to achieve the desired result. □

**2.51.** Let $e_1 = (1,0)$ and $e_2 = (0,1)$, If $\varphi$ is an isometry of the plane fixing $O$, let $\varphi(e_1) = (a,b)$, $\varphi(e_2) = (c,d)$, and let $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Prove that $\det(A) = \pm 1$.

*Proof.* We need to show that $ad - bc = \pm 1$. This is equivalent to showing that $(ad-bc)^2 = 1$, so we will show this instead. Since $\varphi$ is an isometry, it preserves distance and therefore length of vectors. It follows that

$$a^2 + b^2 = c^2 + d^2 = 1$$

and that

$$(a-c)^2 + (b-d)^2 = (1-0)^2 + (0-1)^2 = 2.$$

Using the latter, we find that

$$a^2 + b^2 + c^2 + d^2 = 2(ac + bd) + 2,$$

but $a^2 + b^2 = c^2 + d^2 = 1$. Hence,

$$ac + bd = 0,$$

and more importantly, its square is zero. Multiplying the two equations from the first equality and rearranging the terms gives

$$1 = (a^2 + b^2)(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2,$$

so $(ad - bc)^2 = 1$ as required. □

**2.52.** True or false with reasons. Here, $G$ is always a group.

(i) If $H$ is a subgroup of $K$ and $K$ is a subgroup of $G$, then $H$ is a subgroup of $G$.

True. Prove it.

(ii) $G$ is a subgroup of itself.

True, but this is a tautology, and therefore has no content.

(iii) The empty set $\emptyset$ is a subgroup of $G$.

False, the identity is not in $H$. This also has no content.

(iv) If $G$ is a finite group and $m$ is a divisor of $\#G$, then $G$ contains an element of order $m$.

False! This is obviously not true, as we have exhibited noncyclic groups of finite order.

(v) Every subgroup of $S_n$ has order dividing $n!$.

True, this is the statement of Lagrange's theorem applied to $S_n$.

(vi) If $H$ is a subgroup of $G$, then the intersection of two (left) cosets of $H$ is a (left) coset of $H$.

False, cosets of $H$ partition $G$, so their intersection is empty.

(vii) The intersection of two cyclic subgroups of $G$ is a cyclic subgroup.

The intersection of two subgroups is a subgroup of each. Subgroups of cyclic groups are cyclic, so this is true.

(viii) If $X$ is a finite subset of $G$, then $\langle X\rangle$ is a finite subgroup.

False. The set $\{1\}$ containing only the element $1 \in \mathbb{Z}$ is a finite subgroup, but generates all of $\mathbb{Z}$.

(ix) If $X$ is an infinite set, then

$$F = \{\sigma \in S_X : \sigma \text{ moves only finitely many elements of } X\}$$

is a subgroup of $S_X$.

*Proof.* This is true. The composition of two such elements moves only a finite number of elements of $X$, and the inverse of such an element $\sigma$ moves on the elements moved by $\sigma$. Thus $F$ is closed under products and inverses, and the identity is clearly in $F$. This proves $F$ is a subgroup. □

(x) Every proper subgroup of $S_3$ is cyclic.

*Proof.* True, every proper subgroup of $S_3$ has order $1, 2$, or $3$ by Lagranges theorem, which all must be cyclic. □

(xi) Every proper subgroup of $S_4$ is cyclic.

False. $S_3$ is a subgroup of $S_4$ in a natural way, and is not cyclic.

**2.55.** Give an example of two subgroups $H$ and $K$ of a group $G$ whose union $H \cup K$ is not a subgroup of $G$.

*Proof.* We appeal to our favorite counter example, $S_3$. In particular, take the subgroup generated by the cycle (12) and the subgroup generated by the cycle (123). The former has order two, while the latter has order three, and their intersection is just the identity (see the following problem for a proof, or just compute it!). Their union is a set of order four, which cannot be a subgroup of $S_3$ by Lagrange's theorem. □

**2.57.** If $H$ and $K$ are subgroups of a group $G$ and if $\#H$ and $\#K$ are relatively prime, prove that $H \cap K = \{1\}$.

*Proof.* The intersection $H \cap K$ of two subgroups $H, K$ of $G$ is a subgroup of $H$, $K$, and $G$ (if this is not clear you should prove it yourself). By Lagrange's theorem, we have that the order of $H \cap K$ must divide the order of $H$ and divide the order of $K$. But $\#H, \#K$ are coprime, so the only positive integer dividing both is one. Hence, $\#(H \cap K) = 1$, and therefore $\#(H \cap K) = \{1\}$. □

**2.58.** Prove that every infinite group contains infinitely many subgroups.

*Proof.* If there exists an element $g \in G$ of infinite order, then we're done, since the subgroup generated by $g^k$ for each $k \in \mathbb{N}$ is never equal to the subgroup generated by $g^l$ for $l \neq k$.

Now assume that $G$ has no elements of infinite order, and assume that $G$ has only finitely many cyclic subgroups $\langle a_i\rangle$ for $1 \leq i \leq n$ with $\langle a_i\rangle \nsubseteq \langle a_j\rangle$ for $i \neq j$. Each element of $G$ generates a cyclic subgroup, however, and is therefore in some $\langle a_i\rangle$: if it weren't then it would generate a new cyclic subgroup, contradicting our assumption. It follows that

$$G = \bigcup_i \langle a_i\rangle,$$

but each $\langle a_i\rangle$ is finite, so $G$ is finite.

Thus, if $G$ is infinite, $G$ must have infinitely many cyclic subgroups $\langle a_i\rangle$ such that $\langle a_i\rangle \nsubseteq \langle a_j\rangle$ for $i \neq j$ or $G$ must have an element of infinite order. Hence $G$ has infinitely many subgroups. □

**2.59.** Let $G$ be a group of order 4. Prove that $G$ is cyclic or $x^2 = 1$ for every $x \in G$. Conclude, using Exercise 2.44 on page 147, that $G$ must be abelian.

*Proof.* Assume $G$ is not cyclic, and let $x \in G$ be any element but the identity. Since $G$ is not cyclic, $\#x \neq 4$. Furthermore, Lagrange's theorem tells us that $\#x \mid \#G = 4$, so $\#x = 2$ (since it is nonidentity). Exercise 2.44 proves $G$ must be abelian. □

**2.67.**

(a) Prove that the composite of two homomorphisms is itself a homomorphism.

*Proof.* Let $A, B, C$ be groups, $\varphi : A \to B$, $\psi : B \to C$ be group morphisms, and $x, y \in A$. It follows that

$$[\psi \circ \varphi](xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = [\psi \circ \varphi](x) \cdot [\psi \circ \varphi](y),$$

so the composition $\psi \circ \varphi$ is a homomorphism of groups. □

(b) Prove that the inverse of an isomorphism is an isomorphism.

*Proof.* We should already know that the inverse of a bijection is a bijection, so we need only show that the inverse of an isomorphism is a homomorphism of groups.

Let $A, B$ be a groups, $\varphi : A \to B$ be an isomorphism, and $x, y \in B$. Also assume by surjectivity that there exists $\bar{x}, \bar{y} \in A$ such that $\varphi(\bar{x}) = x$ and $\varphi(\bar{y}) = y$. Notice that applying $\varphi^{-1}$ to both sides of the previous two equalities gives that $\varphi^{-1}(x) = \bar{x}$ while $\varphi^{-1}(y) = \bar{y}$ while $xy = \varphi(\bar{x})\varphi(\bar{y}) = \varphi(\bar{x}\bar{y})$. Now,

$$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(\bar{x}\bar{y}) = \bar{x}\bar{y} = \varphi^{-1}(x)\varphi^{-1}(y).$$

This shows that $\varphi^{-1}$ is a homomorphism and therefore an isomorphism. Also, it is important to note that we made heavy use of the fact that $\varphi$ was both surjective and injective. □

(c) Prove that isomorphism is an equivalence relation on any family of groups.

*Proof.* We will show that '$\cong$' is an equivalence relation by way of showing that it is reflexive, symmetric, and transitive. Fortunately, we did most of the work in the previous parts.

The identity is an automorphism of any group $G$, so '$\cong$' is clearly reflexive.

Assume that $A \cong B$ so that there exists a group isomorphism $\varphi : A \to B$. We showed in part $(b)$ that $\varphi^{-1} : B \to A$ is an isomorphism of groups also, so $B \cong A$.

Assume that $\varphi : A \to B$ and $\psi : B \to C$ are group isomorphisms. By part $(a)$, $\psi \circ \varphi : A \to C$ is a homomorphism of groups. The composition of two bijections is a bijection, so that $\psi \circ \varphi$ is a bijective homomorphism of groups. Hence, it is an isomorphism of groups, and $A \cong C$. □

(d) Prove that two groups that are isomorphic to a third group are isomorphic to each other.

*Proof.* Assume that $A \cong B$ and $C \cong B$ for groups $A, B, C$. Since '$\cong$' is an equivalence relation by the above, symmetry gives us that $C \cong B$ implies $B \cong C$, and transitivity gives us that $A \cong C$. □

**2.70.**

(a) Show that every group $G$ with $\#G < 6$ is abelian.

*Proof.* The group of order 1 is simply the group $\{1\}$, which is abelian. By Lagrange's theorem, any nonidentity element of any group of order two, three, or five must have order two, three, or five (respectively). Hence, such a group is cyclic. Cyclic groups are abelian (if this isn't clear, you should prove it!). For groups of order four, we appeal to Exercise 2.59 in the text. □

(b) Find two nonisomorphic groups of order 6.

*Proof.* This is easy. The groups $\mathbb{Z}/6\mathbb{Z}$ (or the cyclic group of order six) and $S_3$ are nonisomorphic by the simple observation that the center of a group is invariant under isomorphism. Specifically, $\mathbb{Z}/6\mathbb{Z}$ is its center, while the center of $S_3$ is trivial. □

**2.75.** If $G$ is a group and $a, b \in G$, prove that $ab$ and $ba$ have the same order.

*Proof.* Suppose that $(ab)^n = 1$, then $a^{-1}(ab)^n a = a^{-1}a = 1$ also, and

$$1 = a^{-1}(ab)^n a = a^{-1}a(ba)^{n-1}(ba) = (ba)^n.$$

We may now conclude that $ab$ and $ba$ have the same order. □

**2.76.**

(a) If $f : G \to H$ is a homomorphism and $x \in G$ has order $k$, prove that $f(x) \in H$ has order $m$, where $m \mid k$.

*Proof.* Assume that $x \in G$ of order $k$, then

$$f(1) = f(x^k) = f(x)^k$$

but $f(1) = 1$, so $f(x)$ has finite order which divides $k$. □

(b) If $f : G \to H$ is a homomorphism and if $(\#G, \#H) = 1$, prove that $f(x) = 1$ for all $x \in G$.

*Proof.* Let $x \in G$ and note that the order of $x$ must divide $\#G$ while the order of $f(x)$ must divide $\#H$. But the order of $f(x)$ must also divide the order of $x$, and therefore must divide $\#G$. Hence, $\#(f(x)) = 1$, and $f(x)$ is the trivial morphism. □

**2.78.** Let $G$ be the additive group of all polynomials in $x$ with coefficients in $\mathbb{Z}$, and let $H$ be the multiplicative group of all positive rationals. Prove that $G \cong H$.

*Proof.* Let $f(x) \in \mathbb{Z}[x]$ be the polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and let $p_i$ be the $i^{\text{th}}$ prime (ordered by size, if you wish). The map

$$\varphi : G \to H$$

such that the image $\varphi(f(x)) = p_0^{a_0} p_1^{a_1} \cdots p_n^{a_n}$ is a homomorphism of groups. Indeed, it is bijective: given $q \in Q$, we just write down the polynomial with coefficients given by the exponents of the prime decomposition, and the kernel is obviously trivial.

As a clever side note, we could have used heavier machinery: these are both free $\mathbb{Z}$-modules with a countable basis and are therefore isomorphic as $\mathbb{Z}$-modules (which is stronger than being isomorphic as abelian groups) by the classification theorem of modules over a PID. □

**2.92.** An *automorphism* of a group $G$ is an isomorphism $G \to G$.

(a) Prove that $\mathrm{Aut}(G)$, the set of all automorphisms of a group $G$, is a group under composition.

*Proof.* In problem 2.67 we showed that the inverse of an isomorphism is an isomorphism and that the composition of two isomorphisms is an isomorphism. It follows easily that $\mathrm{Aut}(G)$ is closed under composition and inverses. The identity map $id_G : G \to G$ such that $id_G(x) = x$ for all $x \in G$ serves as the identity element. The associativity of composition of homomorphisms follows from the associativity of composition of maps between sets. □

(b) Prove that $\gamma : G \to \mathrm{Aut}(G)$, defined by $g \mapsto \gamma_g$ (conjugation by $g$), is a homomorphism.

*Proof.* Let $g, h, x$ be elements of $G$. We will denote the operation in $\mathrm{Aut}(G)$ explicitely by $\circ$, while the operation is $G$ will be denoted as normal to reduce confusion. The product of $\gamma(g)$ and $\gamma(h)$ is

$$[\gamma(g) \circ \gamma(h)](x) = \gamma_g(\gamma_h(x)) = \gamma_g(hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = \gamma(gh)$$

so $\gamma$ is a homomorphism of groups. □

(c) Prove that $\ker \gamma = Z(G)$.

*Proof.* Assume that $g$ is in the kernel of $\gamma$. Then $\gamma(g) = id_G$, so that $gxg^{-1} = x$ for all $x \in X$, and hence $gx = xg$ for all $x \in X$. Therefore, $g \in Z(G)$, the center of $G$, and $Z(G) \subseteq \ker \gamma$.

For the other containment, assume that $g \in Z(G)$. Then $gxg^{-1} = x$ for all $x \in G$, and $[\gamma(g)](x) = gxg^{-1} = x$ for all $x \in G$. Hence, $\gamma(g) = id_G$, and $Z(G) \subseteq \ker \gamma$. □

(d) Prove that $\mathrm{im}\, \gamma \triangleleft \mathrm{Aut}(G)$.

*Proof.* It suffices to show that if $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, then $\alpha\gamma(g)\alpha^{-1} = \gamma(h)$ for some $h \in G$. But for all $x \in G$,

$$[\alpha \circ \gamma(g) \circ \alpha^{-1}](x) = [\alpha \circ \gamma(g)](\alpha^{-1}(x)) = \alpha(g\alpha^{-1}(x)g^{-1}) = \alpha(g)x\alpha(g^{-1}) = \alpha(g)x\alpha(g)^{-1}$$

and hence $\alpha\gamma(g)\alpha^{-1} = \gamma(\alpha(g))$. □

**2.93.** If $G$ is a group, prove that $\mathrm{Aut}(G) = \{1\}$ if and only if $\#G \leq 2$.

*Proof.* Suppose first that $\#\mathrm{Aut}(G) = \{1\}$. By what we have seen in the above problem, $G/Z(G) \cong \mathrm{im}\, \gamma \subseteq \mathrm{Aut}(G)$, so that $G$ must be abelian. Furthermore, if $G$ is an abelian group containing an element with order $\neq 2$, then the homomorphism sending every element to its inverse is a nontrivial automorphism, so every element of $G$ must have order 2. If $\#G > 2$, then there exists two such elements, and the homomorphism permuting these two and fixing everything else is a nontrivial automorphism. Hence, $\#G \leq 2$.

The other direction is obvious. □

**2.95.** True or false, with reasons.

(1) If $[a] = [b]$ in $\mathbb{I}_m$, then $a = b$ in $\mathbb{Z}$.

False. $[0] = [2]$ in $\mathbb{I}_2$.

(2) There is a homomorphism $\mathbb{I}_m \to \mathbb{Z}$ defined by $[a] \to a$.

False. This homomorphism is not well defined.

(3) If $a = b$ in $\mathbb{Z}$, then $[a] = [b]$ in $\mathbb{I}_m$.

True. If two elements are equal, then they have the same remainder after division by $m$.

(4) If $G$ is a group and $K \triangleleft G$, then there is a homomorphism $G \to G/K$ having kernel $K$.

True.

*Proof.* The projection map $\pi : G \to G/K$ sending $a \in G$ to the coset $aK$ is a surjective homomorphism. Thus, the first isomorphism theorem tells us that $G/\ker \pi \cong G/K$, so $\ker \pi = K$. □

(5) If $G$ is a group and $K \triangleleft G$, then every homomorphism $G \to G/K$ has kernel $K$.

False. The zero map from $G \to G/K$ has kernel equal to $G$.

(6) Every quotient group of an abelian group is abelian.

True.

*Proof.* The homomorphic image of an abelian group is abelian (if this isn't clear to you, you should prove it), and a quotient of an abelian group is the image of the surjective projective map. □

(7) If $G$ and $H$ are abelian groups, then $G \times H$ is an abelian group.

True.

*Proof.* Let $(g_1, h_1), (g_2, h_2) \in G \times H$, then

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) = (g_2, h_2) \cdot (g_1, h_1),$$

since $G, H$ are abelian. □

(8) If $G$ and $H$ are cyclic groups, then $G \times H$ is a cyclic group.

False. This is true if and only if $(\#G, \#H) = 1$. In particular, see Example 2.125 in the text.

(9) If every subgroup of a group $G$ is a normal subgroup, then $G$ is abelian.

False. The quaternion group is such a group, see Example 2.98.

(10) If $G$ is a group, then $\{1\} \lhd G$ and $G/\{1\} \cong G$.

True. The projection map in this case is an isomorphism.

**2.96.** Prove that $U(\mathbb{I}_9) \cong \mathbb{I}_6$ and $U(\mathbb{I}_{15}) \cong \mathbb{I}_4 \times \mathbb{I}_2$.

*Proof.* For the first one, note that $\phi(9) = 3^2 - 3^{2-1} = 9 - 3 = 6$ is the number of elements of $U(\mathbb{I}_9)$. It suffices then to show that it is generated by a single element, and is therefore isomorphic to $\mathbb{I}_6$. The unit in $U(\mathbb{I}_9)$ is 1, so we will use 2 as a generator. To see that it generates, simply compute its powers modulo nine that divide six: $2^2 = 4 \neq 1$, $2^3 = 8 \neq 1$, so $2^6$ is the order of 2 in $U(\mathbb{I}_9)$.

While it goes unstated, the proof of Corollary 2.131 almost proves what we need: if $g(U(\mathbb{I}_{mn})) = U(\mathbb{I}_m) \times U(\mathbb{I}_n)$ and $U(\mathbb{I}_{mn}) \cong U(\mathbb{I}_m) \times U(\mathbb{I}_n)$ since $g$ is an injection. Hence $U(\mathbb{I}_{3\cdot 5}) \cong U(\mathbb{I}_5) \cdot U(\mathbb{I}_3)$. But $U(\mathbb{I}_3) \cong \mathbb{I}_2$ and $U(\mathbb{I}_5) \cong \mathbb{I}_4$, so we're done. □

**2.98.** If $G$ is a group and $G/Z(G)$ is cyclic, where $Z(G)$ denotes the center of $G$, prove that $G$ is abelian; that is, $G = Z(G)$. Conclude that if $G$ is not abelian, then $G/Z(G)$ is never cyclic.

*Proof.* We will denote $Z(G)$ by just $Z$. Assume $G/Z$ is cyclic with generator $xZ$, and let $a, b \in G$. The cosets of $Z$ are all of the form $x^i Z$ and partition $G$, so every element of $G$ may be written as the element of some coset. In particular, we may write $a = x^n z_a$ and $b = x^m z_b$ for nonnegative integers $m, n$ and $z_a, z_b \in Z$. But then,

$$ab = x^n z_a x^m z_b = x^n x^m z_a z_b = x^m x^n z_b z_a = x^m z_b x^n z_a = ba,$$

since $x$ commutes with itself and $z_a, z_b$ commute with everything in $G$ (they are elements of the center!).

The conclusion is just the contrapositive of our statement. □

**2.103.** Let $A$ and $B$ be groups, let $A' \lhd A$ and $B' \lhd B$ be normal subgroups, and let $\alpha : A \to B$ be a homomorphism with $\alpha(A') \leq B'$.

(1) Prove that there is a (well-defined) homomorphism $\alpha_* : A/A' \to B/B'$ given by $\alpha_* : aA' \mapsto \alpha(a)B'$.

*Proof.* First we show that this map is well defined. To do this, choose $g$ and $h$ to be representatives of the same coset in $A/A'$. In particular, $gh^{-1} = a \in A'$, so $\alpha(gh^{-1}) = b \in B'$. But then

$$\alpha^*(gh^{-1}A') = \alpha(gh^{-1})B' = B',$$

and it follows that

$$\alpha_*(gA') = \alpha(g)B' = \alpha(h)B' = \alpha_*(hA'),$$

as required. This is clearly a homomorphism because $\alpha$ is. □

(2) Prove that if $\alpha$ is surjective, then $\alpha_*$ is surjective.

*Proof.* Let $bB'$ be a coset in $B/B'$. Since $\alpha$ is surjective, there exists $a \in A$ such that $\alpha(a) = b$. Hence,

$$\alpha_*(aA') = \alpha(a)B' = bB',$$

and $\alpha_*$ is surjective. □

(3) Give an example in which $\alpha$ is injective and $\alpha_*$ is not injective.

*Proof.* Let $G$ be a group of order greater than or equal to two, and take $A = B = G$ with $A' = \{0\}$, $B' = G$, and $\alpha = id_G$. The map $\alpha$ is clearly an injective homomorphism and $\alpha(\{0\}) \subset G$, but $\alpha_*$ is the zero map, and is therefore not injective. □

**2.107.** Prove the converse of Lemma 2.112: if $K$ is a subgroup of a group $G$, and if every left coset $aK$ is equal to a right coset $Kb$, then $K$ is normal in $G$.

*Proof.* Assume the hypothesis, and let $b \in G$. Then $Kb = aK$ for some $a \in G$, so there exists some $k \in K$ such that $a = kb$. But then $ab^{-1} = k \in K$, so $aK = bK$, and therefore $bK = Kb$. Since our choice of $b$ was arbitrary it follows that $bK = Kb$ for all $b \in G$, and therefore $K$ is normal. □

**2.108.** Let $G$ be a group and regard $G \times G$ as the direct product of $G$ with itself. If the multiplication $\mu : G \times G \to G$ is a group homomorphism, prove that $G$ must be abelian.

*Proof.* If $a, b \in G$, then $(a, 1)$ and $(1, b)$ are elements of $G \times G$, and

$$(a, 1) \cdot (1, b) = (a, b) = (1, b) \cdot (1, a).$$

Assume that multiplication $\mu : G \times G \to G$ is a group homomorphism. It follows that

$$\mu(a, 1) \cdot \mu(1, b) = \mu((a, 1) \cdot (1, b)) = \mu((1, b) \cdot (a, 1)) = \mu(1, b) \cdot \mu(a, 1).$$

But, $\mu(a, 1) = a$ and $\mu(1, b) = b$, so

$$ab = \mu(a, 1) \cdot \mu(1, b) = \mu(1, b) \cdot \mu(a, 1) = ba.$$

Therefore, $G$ is abelian. □

**2.109.** Generalize Theorem 2.128 as follows. Let $G$ be a finite (additive) abelian group or order $mn$, where $(m, n) = 1$. Define

$$G_m = \{g \in G : \#g \mid m\} \text{ and } G_n = \{h \in G : \#h \mid n\}.$$

(a) Prove that $G_m$ and $G_n$ are subgroups with $G_m \cap G_n = \{0\}$.

*Proof.* It suffices to show that $G_m$ is a subgroup, as the argument for $G_n$ is analogous. It is clear that the identity is in $G_m$, and that $G_m$ is closed under inverses, so we need only show closure under the group operation. Assume that $g_1 \in G_m$ and $g_2 \in G_m$ such that $\#g_1 = k \mid m$ and $\#g_2 = l \mid m$. We need that the sum $g_1 + g_2$ has order dividing $m$. But it is easy to see that the order of $g_1 + g_2$ is the least common multiple of $l$ and $k$, and the least common multiple of two numbers divides every multiple of the two, so it divides $m$.

For the disjoint part, notice that if $g \in G_m \cap G_n$, then $\#g \mid (m, n) = 1$, so $g = \{0\}$. □

(b) Prove that $G = G_m + G_n = \{g + h : g \in G_m \text{ and } h \in G_n\}$.

*Proof.* We need to show that every element $x \in G$ can be written as the sum of something in $G_m$ and something in $G_n$. We know that $(m, n) = 1$, so there exist integers $a, b$ such that $am + bn = 1$. In particular,

$$x = \sum^{am+bn} x = \sum^{am} x + \sum^{bn} x.$$

But

$$\sum^{n} \left[ \sum^{am} x \right] = \sum^{amn} x = \sum^{a} \sum^{nm} x = \sum^{a} 0 = 0,$$

and similarly,

$$\sum^{m} \left[ \sum^{bn} x \right] = \sum^{bmn} x = \sum^{b} \sum^{nm} x = \sum^{b} 0 = 0.$$

Hence, $\sum^{am} x$ has order dividing $n$ and $\sum^{bn} x$ has order dividing $m$, so $x$ can be expressed as the sum of something in $G_m$ and something in $G_n$, as required. □

(c) Prove that $G \cong G_m \times G_n$.

*Proof.* This follows immediately from the previous two parts. □

**2.110.**

(a) Generalize Theorem 2.128 by proving that if prime factorization of an integer $m$ is $m = p_1^{e_1} \cdots p_n^{e_n}$, then

$$\mathbb{I}_m \cong \mathbb{I}_{p_1^{e_1}} \times \cdots \times \mathbb{I}_{p_n^{e_n}}.$$

*Proof.* The proof proceeds by induction on the number of prime factors in the prime factorization. The base case is proved in Theorem 2.128. Assume then that $m = p_1^{e_1} \cdots p_k^{e_k}$, and that the result holds true for $k - 1$. If $m' = p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}$, then

$$\mathbb{I}_m \cong \mathbb{I}_{m'} \times \mathbb{I}_{p_k^{e_k}}$$

by Theorem 2.128, so that by the inductive hypothesis,

$$\mathbb{I}_{m'} \times \mathbb{I}_{p_k^{k+1}} \cong \mathbb{I}_{p_1^{e_1}} \times \cdots \times \mathbb{I}_{p_{k-1}^{e_{k-1}}} \times \mathbb{I}_{p_k^{e_k}},$$

as was necessary to show. □

(b) Generalize Corollary 2.131 by proving that if the prime factorization of an integer $m$ is $m = p_1^{e_1} \cdots p_n^{e_n}$, then

$$U(\mathbb{I}_m) \cong U(\mathbb{I}_{p_1^{e_1}}) \times \cdots \times U(\mathbb{I}_{p_n^{e_n}}).$$

*Proof.* This proof is analogous to the above by replacing 2.128 with 2.131 and taking unit groups. □

**2.113.** If $G$ is a group and $x, y \in G$, define their *commutator* to be $xyx^{-1}y^{-1}$, and define the *commutator subgroup* $G'$ to be the subgroup generated by all the commutators (the product of two commutators need not be a commutator).

(a) Prove that $G'$ is normal in $G$.

*Proof.* We begin by showing that the conjugate of a commutator is a commutator. Notice that this is not enough – we will need to do more to prove the required result! Assume that $x, y \in G$, write $\overline{xy} = xyx^{-1}y^{-1}$ for their commutator. If $g \in G$, then

$$g\overline{xy}g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1},$$

so that the conjugate $g\overline{xy}g^{-1}$ is the commutator $\overline{(gxg^{-1})(gyg^{-1})}$. Now, if $x_i, y_i \in G$ for $1 \leq i \leq n$, then

$$g\left(\prod_1^n \overline{x_i y_i}\right) g^{-1} = g\overline{x_1 y_1}\left(\prod_2^n g^{-1} g\overline{x_i y_i}\right) g^{-1} = \prod_1^n g\overline{x_i y_i} g^{-1}.$$

But every conjugate of a commutator is a commutator, so that the conjugate of a product of commutators is a product of commutators, and is therefore in $G'$. It follows that $G'$ is normal in $G$. □

(b) Prove that $G/G'$ is abelian.

*Proof.* Let $aG'$ and $bG'$ be elements of $G/G'$. Since $(ab)(ba)^{-1} = aba^{-1}b^{-1} \in G'$, it follows that $ab$ is congruent to $ba$ modulo $G'$. Hence, $abG' = baG'$, so $G/G'$ is abelian. □

(c) If $\varphi : G \to A$ is a homomorphism where $A$ is an abelian group, prove that $G' \leq \ker\varphi$. Conversely, if $G' \leq \ker\varphi$, prove that $\operatorname{im}\varphi$ is abelian.

*Proof.* It suffices to show that the image of every commutator in $A$ is the identity. Let $\overline{xy}$ be the commutator of two elements $x, y \in G$, then

$$\varphi(\overline{xy}) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}.$$

But $A$ is abelian, so these elements all commute and cancel. Thus $G' \subseteq \ker\varphi$.

Conversely, assume that $G' \subseteq \ker\varphi$, so that $\varphi$ factors through a unique homomorphism $\tilde{\varphi} : G/G' \to A$, i.e., $\varphi = \tilde{\varphi}\circ\pi$. But then $\operatorname{im}\varphi$ is the homomorphic image of an abelian group, and is therefore abelian. □

(d) If $G' \leq H \leq G$, prove that $H$ is normal in $G$.

*Proof.* Subgroups of $G/G'$ correspond to subgroups of $G$ containing $G'$. Even more so, normal subgroups of $G/G'$ correspond to normal subgroups of $G$ containing $G'$. But every subgroup of $G/G'$ is normal since $G/G'$ is abelian, so any subgroup containing $G'$ is normal also. □

**2.133.** Prove that if a simple group $G$ has a subgroup of index $n$, then $G$ is isomorphic to a subgroup of $S_n$.

*Proof.* Let $H$ be a subgroup of $G$ with index $n$. There is an action of $G$ on $G/H$ by left multiplication. There is a map $\varphi : G \to S_n$ sending each element of $G$ to the permutation it induces on the cosets of $H$. In fact, $\varphi$ is a homomorphism, which follows easily from the action axioms. Also, any element not in $H$ induces a nontrivial permutation, so $\varphi$ is not the zero map.

The kernel of $\varphi$ is a normal subgroup of $G$, so it is either $G$ or trivial. We have already seen that this is not the zero map, so it must be trivial. Therefore, $\varphi$ is injective, and $G$ is isomorphic to its image, a subgroup of $S_n$. □

**2.134.** Let $G$ be a group with $\#G = mp$, where $p$ is a prime and $1 < m < p$. Prove that $G$ is not simple.

*Proof.* $G$ has an element $g$ of order $p$ by Sylow's first theorem (this is proved as result in chapter 2, but left unnamed). Consider $G$ acting by left multiplication on $G/\langle g\rangle$, the set of right cosets of $\langle g\rangle$, which has order $m$. This induces a homomorphism $\varphi : G \to S_m$ since each element of $G$ permutes the cosets of $\langle g\rangle$. The kernel of $G$ is a normal subgroup of $G$, so it suffices to show that $\varphi$ is not injective (it is obviously not the zero map, as there are elements outside of $\langle g\rangle$).

Assume $\ker\varphi = \{1\}$, then $G \mid m!$, but $p \nmid m!$ since $m < p$: every prime factor of anything less than or equal to $m$ is less than $p$. Therefore $\ker\varphi \neq \{1\}$, so we have exhibited a nontrivial normal subgroup of $G$. Hence, $G$ is not simple. □

## Chapter 3

**3.1.** True or false with reasons.

(a) The subset $\{r + s\pi : r, s \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$.

*Proof.* False, the issue is with closure: $\pi \cdot \pi = \pi^2$, but $\pi^2$ is not in the above set. □

(b) Every subring of a domain is a domain.

*Proof.* True. The product on the subring $S \subseteq R$ is the restriction of the product on $R \times R$ to $S \times S$. □

(c) The zero ring is a subring of $\mathbb{Z}$.

*Proof.* False. Rings should have multiplicative identities. I'm not sure what the book says, but it's wrong if it says otherwise. □

(d) There are infinitely many positive integers $m$ for which $\mathbb{I}_m$ is a domain.

*Proof.* True, any prime $p$ fulfills this requirement. There are infinitely many primes (if you don't know why this is true, you should figure it out!). □

(e) If $S$ is a subring of a commutative ring $R$, then $U(S)$ is a subgroup of $U(R)$.

*Proof.* True, it suffices to show that $U(S)$ is closed under the product, but $S$ is a subring and the result follows immediately. □

(f) If $S$ is a subring of a commutative ring $R$, then $U(S) = U(R) \cap S$.

*Proof.* False, take $R = \mathbb{R}$ and $S = \mathbb{Z}$. □

(g) If $R$ is an infinite commutative ring, then $U(R)$ is infinite.

*Proof.* False, $\mathbb{Z}$ is infinite, while $\mathbb{Z}^* \cong \mathbb{Z}/2$ (as groups). □

(h) If $X$ is an infinite set, then the family of all finite subsets of $X$ forms a subring of the Boolean ring $B(X)$.

*Proof.* False, the product is intersection, and the multiplicative identity is the space itself which is not a finite subset. □

**3.2.** Prove that a commutative ring $R$ has a unique one 1; that is, if $e \in R$ satisfies $er = r$ for all $r \in R$, then $e = 1$.

*Proof.* This is the same proof from that of groups: $e = e \cdot 1 = 1$. □

**3.5.** Assume that $S$ is a subset of a ring $R$ such that

(i) $1 \in S$;
(ii) if $a, b \in S$, then $a + b \in S$;
(iii) if $a, b \in S$, then $ab \in S$.

Give an example of a commutative ring $R$ containing such a subset $S$ which is not a subring of $R$.

Take $R = \mathbb{Z}$ and $S$ to be the set of positive integers. $0 \notin S$, so $S$ is not a subring.

**3.6.** Find multiplicative inverses of nonzero elements in $\mathbb{I}_{11}$.

*Proof.* Every element but 0 has a multiplicative inverse since 11 is prime. Also, every element but 1 generates the group of units of $\mathbb{Z}/11\mathbb{Z}$ which has order 10, so that its inverse is itself to the ninth power modulo 11. □

**3.13.** Prove that the only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself.

*Proof.* $\mathbb{Z}$ is a cyclic group under addition with generator 1. In particular, if $1 \in S \subseteq \mathbb{Z}$ and $S$ is closed under sums and inverses, then $S = \mathbb{Z}$, but every subring of $\mathbb{Z}$ is closed under sums and inverses and contains 1. □

**3.17.** True or false with reasons.

(i) Every field is a domain.

*Proof.* True, units are never zero divisors. □

(ii) There is a finite field with more than $10^{100}$ elements.

*Proof.* True, there is a finite field with $11^{100}$ elements. □

(iii) If $R$ is a domain, then there is a unique field containing $R$.

*Proof.* False, $R = \mathbb{Z}$ is contained in both $\mathbb{Q}$ and $\mathbb{R}$. □

(iv) Every commutative ring is a subring of some field.

*Proof.* False, fields do not have zero divisors, but some commutative rings do. □

(v) The subset $R = \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$.

*Proof.* True, prove it by hand. □

(vi) The prime field of $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ is $\mathbb{Q}$.

*Proof.* True, it is clear that $\mathbb{Q}$ is a subfield of the prime field, as $\mathbb{Q}$ is a subfield of $\mathbb{Q}[i]$. However, $\mathbb{Q}$ contains no proper subfields (it is the field of fractions of $\mathbb{Z}$ which every subring of $\mathbb{Q}[i]$ contains). □

(vii) If $R = \mathbb{Q}[\sqrt{2}]$, then $Frac(R) = \mathbb{R}$.

*Proof.* False, $\sqrt{3}$ is not an element of $Frac(R)$. □

**3.19.** Define $\mathbb{F}_4$ to be the set of all $2 \times 2$ matrices

$$\mathbb{F}_4 = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{F}_2 \right\}.$$

(a) Prove that $\mathbb{F}_4$ is a commutative ring whose operations are matrix addition and matrix multiplication.

*Proof.* It suffices to show that $\mathbb{F}_4$ is closed under sums and additive inverses, and that it is closed under products since it is a subset of $M_2(\mathbb{F}_2)$, the set of $2 \times 2$ matrices with coefficients in $\mathbb{F}_2$. This is clear by direct computation. □

(b) Prove that $\mathbb{F}_4$ is a field having exactly four elements.

*Proof.* The entries of any matrix in $\mathbb{F}_4$ have two degrees of freedom, and there are 2 choices for each, hence there are four such matrices. To see that any nonzero ones are invertible, we simply compute the determinant

$$\det \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} = a(a+b) - b^2 = a^2 - b^2 + ab$$

with the requirement that either $a$ or $b$ is nonzero. In any of the three cases, the determinant is nonzero and the matrix is invertible. □

(c) Show that $\mathbb{I}_4$ is not a field.

*Proof.* 2 is a zero divisor in $\mathbb{I}_4$. □

**3.21.** Find all the units in the ring $\mathbb{Z}[i]$ of Gaussian integers.

*Proof.* We define the *norm function* $N : \mathbb{Z}[i] \to \mathbb{N}$ to be the multiplicative function

$$N(a+bi) = (a+bi)(a-bi) = a^2 + b^2.$$

You should verify this function is multiplicative, that is, that $N(z)N(w) = N(zw)$ for $z, w \in \mathbb{Z}[i]$. If $u \in \mathbb{Z}[i]$ is a unit, then its norm $N(u)$ divides $N(1) = 1$ since $N(u)N(u^{-1}) = N(1) = 1$. If $N(u) = a^2+b^2$ and divides 1, then it follows that $N(u) = \pm 1$ so that either $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. Indeed, any such choice of $a, b$ produces a number $a + bi$ which is a unit, and we have therefore exhibited them all. To be succinct,

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\},$$

the fourth roots of unity. □

**3.26.** Let $k$ be a field, and let $R$ be a subring

$$R = \{n \cdot 1 : n \in \mathbb{Z}\} \subseteq k.$$

(a) If $F$ is a subfield of $k$, prove that $R \subseteq F$.

*Proof.* Any subfield $F$ of $k$ is a subring so that it contains 1 and therefore contains any integer multiples of 1. Hence, $R \subseteq F$. □

(b) Prove that a subfield $F$ of $k$ is the prime field of $k$ if and only if it is the *smallest* subfield of $k$ containing $R$; that is, there is no subfield $F'$ with $R \subseteq F' \subset F$.

*Proof.* Every subfield contains $R$ by the above, so that it suffices to note that the prime field is the smallest subfield of $F$ by definition. □

(c) If $R$ is a subfield of $k$, prove that $R$ is the prime field of $k$.

*Proof.* This follows directly from the previous part: if $R$ is already a field and the prime field is the smallest field containing $R$, then the prime field is $R$. □

**3.30.** Show that if $R$ is a nonzero commutative ring, then $R[x]$ is never a field.

*Proof.* It suffices to exhibit an element that is not invertible. In particular, the element $x \in R[x]$ has no inverse: if $f(x)$ was an inverse for $x$, then $xf(x) = 1$. But then if

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

for nonzero $a_0$, then

$$xf(x) = a_0x^{n+1} + a_1x^n + \cdots + a_nx.$$

Thus, $\deg(xf(x)) = 1 + \deg(f(x)) = \deg(1) = 0$, a contradiction. □

**3.32.**

(a) Let $R$ be a domain. Prove that a polynomial in $f(x)$ is a unit in $R[x]$ if and only if $f(x)$ is a nonzero constant which is a unit in $R$.

*Proof.* If $R$ is a domain, then so is $R[x]$, so the degree of a product of two polynomials is the sum of the degrees of the factors. Therefore, $f(x)$ is a unit if and only if its degree is zero (and also its inverse is zero). But if it is degree zero and invertible, then it is a unit in $R$. □

(b) Show that $([2]x+[1])^2 = [1]$ in $\mathbb{I}_4[x]$. Conclude that the statement in part $(i)$ may be false for commutative rings that are not domains.

*Proof.*

$$(2x+1)(2x+1) = 4x^2 + 4x + 1,$$

and modulo 4 gives the required property. □

**3.33.** Show that if $f(x) = x^p - x \in \mathbb{F}_p[x]$, then its polynomial function $f^b : \mathbb{F}_p \to \mathbb{F}_p$ is identically zero.

*Proof.* This is Fermat's Little Theorem. □

**3.39.** If $R$ is a commutative ring, define $R[[x]]$ to be the set of all formal power series over $R$.

(a) Show that the formulas defining addition and multiplication on $R[x]$ make sense for $R[[x]]$, and prove that $R[[x]]$ is a commutative ring under these operations.

*Proof.* Just verify the formulas, this is tedious but worthwhile to do once on your own so that you memorize and understand them. □

(b) Prove that $R[x]$ is a subring of $R[[x]]$.

*Proof.* $R[x]$ is a ring and it embeds canonically in $R[[x]]$, therefore it is a subring. □

(c) Denote a formal power series $\sigma = (s_0, s_1, s_2, \ldots, s_n, \ldots)$ by

$$\sigma = s_0 + s_1 x + s_2 x^2 + \cdots .$$

Prove that if $\sigma = 1 + x + x^2 + \cdots$, then $\sigma = 1/(1-x)$ is in $R[[x]]$.

*Proof.* I think this is just asking us to prove that $(1-x)\sigma = 1$, which it is. Again, you should check this on your own using the formulas. It's not tedious, but it leads to a much deeper result: elements $f(x) \in R[[x]]$ are invertible if and only if their constant terms are invertible in $R$. □

**3.43.**

(a) Prove that the field with 4 elements and $\mathbb{I}_4$ are not isomorphic commutative rings.

*Proof.* $\mathbb{I}_4$ has a zerodivisor[1], therefore it is not a field. □

(b) Prove that any two fields having exactly four elements are isomorphic.

*Proof.* □

**3.58.** Find the gcd of $x^2 - x - 2$ and $x^3 - 7x + 6$ in $\mathbb{F}_5[x]$, and express it as a linear combination of them.

[1]A nonzero element $a \in R$ is a *zerodivizor* if there exists nonzero $b \in R$ such that $ab = 0$. Elements which are not zero divisors are called *nonzerodivisors*.

**3.60.** If $R$ is a domain and $f(x) \in R[x]$ has degree $n$, show that $f(x)$ has at most $n$ roots in $R$.

*Proof.* Let $k$ be the field of fractions of $R$. $k[x]$ is a Euclidean domain (we can perform division), so that $f(x)$ has at most $n$ roots in $k$. But $R$ embeds into $k$, so if $f(x)$ has at most $n$ roots in $k$, then it has at most $n$ roots in $R$. □

**3.64.** Let $k$ be a field, and let $f(x), g(x) \in k[x]$ be relatively prime. If $h(x) \in k[x]$, prove that $f(x) \mid h(x)$ and $g(x) \mid h(x)$ imply $f(x)g(x) \mid h(x)$.

*Proof.* $k[x]$ is a Euclidean domain (we can perform division), so that in particular it is a UFD. Factoring $f(x)$ and $g(x)$ into their prime factorizations gives that each prime factor divides $h(x)$, and their factorizations are disjoint: no factor dividing $g$ divides $f$ (and vice versa) by the gcd assumption. Hence each prime factor from both $f$ and $g$ divides $h$, so that the product of the prime factors does and therefore $fg$ does. □

**3.67.** Let $f(x) = (x - a_1) \cdots (x - a_n) \in R[x]$, where $R$ is a commutative ring. Show that $f(x)$ has no repeated roots (that is, all the $a_i$ are distinct) if and only if the $\gcd(f', f) = 1$, where $f'$ is the derivative of $f$.

*Proof.* Taking derivatives, the product rule gives that

$$f'(x) = \sum_{i=1}^{n} (x - a_1) \cdots \widehat{(x - a_i)} \cdots (x - a_n)$$

where the hat indicates that the factor is omitted. Indeed, we see that $f'(x)$ vanishes at $a_i$ if, and only if, $f(x)$ vanishes $a_i$ with multiplicity greater than two. □

**3.75.** If $k$ is a field, show that the ideal $(x, y)$ in $k[x, y]$ is not a principal ideal.

*Proof.* Assume that there was some element $a$ which generated the ideal $(x, y)$, i.e., $(x, y) = a$. Then $a$ would have to divide $x$ and $a$ would have to divide $y$. But $x$ and $y$ are both irreducible and $k[x, y]$ is a UFD, so that $a = \pm x$ and $a = \pm y$. Obviously, this cannot be since $\pm x \neq \pm y$. □

University of Illinois at Chicago, Dept. of Mathematics, Statistics, and Computer Science, Chicago IL 60607
*E-mail address*: astath2@uic.edu