Math 453

Fall 2011

Answers to Selected Problems

Page 21

7. Show that if a and b are positive integers then $ab = \text{lcm}(a, b) \cdot \gcd(a, b)$.

Proof. We assume that we have proved the fundamental theorem of arithmetic, namely that we can write both a and b as products of primes in a unique way. Let $p_1, p_2, \ldots, p_k$ be all the primes that appear as factors of **either** a **or** b. Then, allowing some exponents to be 0, we can write

$$a = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k},$$

and

$$b = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k},$$

for some non-negative integers n_i and m_i. For each i, let $\ell_i = \max(n_i, m_i)$ and $r_i = \min(n_i, m_i)$. Note then, that for each i, we have $p_i^{r_i} | a$ and $p_i^{r_i} | b$. Moreover, by our choice of r_i, we see that either $p_i^{r_i+1} \not| a$ or $p_i^{r_i+1} \not| b$. Thus $p_i^{r_i}$ is the highest power of p_i dividing both a and b, and therefore is the highest power of p_i dividing $\gcd(a, b)$ (see problem 12). Thus, by the fundamental theorem of arithmetic,

$$gcd(a, b) = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}.$$

On the other hand, note that if

$$c = p_1^{\ell_1} p_2^{\ell_2} \ldots p_k^{\ell_k},$$

then, by our choice of ℓ_i, we see that $a|c$ and $b|c$. Moreover, if s is any common multiple of a and b, then for each i we must have $p_i^{\ell_i} | s$, and thus $c|s$. Thus (problem

12) $c = \text{lcm}(a, b)$. Now, for each i, we see that $r_i + \ell_i = n_i + m_i$, and thus

$$\gcd(a, b) \cdot \text{lcm}(a, b) = p_1^{r_1+\ell_1} p_2^{r_2+\ell_2} \dots p_k^{r_k+\ell_k} =$$
$$p_1^{n_1+m_1} p_2^{m_2+n_2} \dots p_k^{n_k+m_k} = ab.$$

□

8. Suppose that a and b are integers dividing c. Show that if a and b are relatively prime, then ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

Proof. Since $a|c$ and $b|c$ we can write

$$c = ak = bn,$$

for some integers n and k. Since $\gcd(a, b) = 1$, we can choose integers s and t with $as + bt = 1$. Now

$$c = (as + bt)c = acs + bct = a(bn)s + b(ak)t = ab(ns + kt),$$

which shows that $ab|c$.

To see that the statement need not be true if a and b are both relatively prime, we take $a = 6$, $b = 4$ and $c = 12$. Then $gcd(a, b) = 2$, $a|c$ and $b|c$, but $ab \not| c$. □

14. Show $5n + 3$ and $7n + 4$ are relatively prime, for all n.

Solution: Recall, $\gcd(a, b)$ is the smallest positive integer linear combination of a and b. That is, the smallest positive integer d so that $d = as + bt$, for some $s, t \in \mathbb{Z}$. So, $\gcd(a, b) = 1$ if and only if we can find $s, t \in \mathbb{Z}$ for which $as + bt = 1$. Now, in our case, we see $a = 5n + 3$ and $b = 7n + 4$, we can take $s = 7$ and $t = -5$, i.e., $7(5n+3)+(-5)(7n+4) = 35n+20-35n-20 = 1$. So, we conclude $\gcd(5n+3, 7n+4) = 1$.□

20. Let $p_1, p_2, \dots, p_n$ be distinct primes. Show that $p_1 p_2 \dots p_n + 1$ is divisible by none of these primes.

Proof. Recall that $n|a$ if and only if $a = 0 \bmod n$. Since each p_i is prime, $p_i > 1$. Let $a = p_1 \dots p_n + 1$. Then each $p_i|(a-1)$, so $a = 1 \bmod p_i$, and since $p_i > 1$, we see that $a \neq 0 \bmod p_i$, and this shows that $p_i \nmid a$. □

21. Show that there are infinitely many primes.

Proof. We argue by contradiction. Suppose to the contrary that there are only finitely many primes. In particular, suppose that $p_1, \dots, p_n$ constitute all the primes. Let $a = p_1 p_2 \dots p_n + 1$. By problem 20 $p_i \nmid a$ for each $1 \leq i \leq n$. Thus, a must be a prime different from $p_1, \dots, p_n$. This contradicts our assumption that $p_1, \dots, p_n$ were all the primes. Consequently, there are infinitely many primes. □

30. Prove the Fibonacci numbers, f_n satisfy $f_n < 2^n$.

Proof. We prove this by the second principle of mathematical induction. Since $f_1 = 1$, we have $f_1 = 1 < 2^1$, so the claim holds for $n = 1$. Also, the claim holds for $n = 2$, since $f_2 = 1 < 2^2 = 4$. Now, suppose $n \geq 2$ and the claim holds for $1 \leq k \leq n$, i.e., suppose $f_k < 2^k$, for $k = 1, 2, \dots, n$. Then $f_{n+1} = f_{n-1} + f_n < 2^{n-1} + 2^n < 2^n + 2^n = 2^{n+1}$. Therefore, if the claim holds for $1, 2, \dots, n$, then the claim holds for $n + 1$. So, by the second principle of mathematical induction, $f_n < 2^n$, for all $n > 1$. □

Page 35

9. Associate the number $+1$ with a rotation and the number -1 with a reflection. Describe an analogy between multiplying these two numbers and multiplying elements of D_n.

Solution: Note that a rotation composed with a rotation is a reflection, a reflection composed with a reflection is a rotation, and composing a reflection and rotation in any order is a reflection. On the other hand multiplying $+1$ and $+1$ yields $+1$, as does multiplying -1 and -1, while multiplying -1 and $+1$ is -1. So, multiplying rotations and reflections can be associated with multiplying ± 1 in this way. □

21. What group theoretic property do the upper case letters $F, G, J, K, , P, Q$ and R have that is not shared by the other 20 upper case letters?

Solution: You might note, these six letters have no symmetries (either rotational or reflectional), while all others have at least one non-trivial symmetry.□

Page 52

14. Suppose that G is a group with the property that whenever $ab = ca$ we have $b = c$. Show that G is abelian.

Proof. Let a and b be elements of G. Take $c = aba^{-1}$. Then $ca = aba^{-1}a = ab$. Since $ca = ab$, the hypothesis implies $c = b$, that is $aba^{-1} = b$. Now multiplying on the right by a, we get $ab = ba$ □

19. Let a and b be elements of a group, and let $n \in \mathbb{Z}$. Show that $(a^{-1}ba)^n = a^{-1}b^n a$.

Proof. Note that if $n = 1$, then we have $(a^{-1}ba)^1 = a^{-1}b^1a, ,$ i.e. the statement holds trivially for $n = 1$. Note that for $n = 2$, $(a^{-1}ba)^2 = (a^{-1}ba)(a^{-1}ba) = a^{-1}b(aa^{-1})ba = a^{-1}b^2a$. Thus the claim holds for $n = 2$. Suppose the claim holds for n. That is, assume that $(a^{-1}ba)^n = a^{-1}b^n a$. Note that $(a^{-1}ba)^{n+1} = (a^{-1}ba)^n(a^{-1}ba)$. Now, by assumption, $(a^{-1}ba)^n = a^{-1}b^n a$. Thus,

$$(a^{-1}ba)^{n+1} = (a^{-1}b^n a)(a^{-1}ba) = a^{-1}b^n(aa^{-1})ba = a^{-1}b^n eba = a^{-1}b^{n+1}a.$$

Thus, by induction, the claim holds for $n \geq 1$.

For $n = 0$, we have $a^{-1}b^0a = a^{-1}ea = e = (a^{-1}ba)^0$. Suppose $n < 0$. Then $-n > 0$, so $(a^{-1}ba)^{-n} = a^{-1}b^{-n}a$. Now,

$$(a^{-1}ba)^n = \left(\left(a^{-1}ba\right)^{-n}\right)^{-1} = (a^{-1}b^{-n}a)^{-1}.$$

Now show that $(a^{-1}b^{-n}a)^{-1} = a^{-1}b^n a$, and you're done. □

26. Show that if $(ab)^2 = a^2b^2$, in a group G, then $ab = ba$.

Proof. Since $(ab)^2 = a^2b^2$, we have $abab = aabb$. Then using the right and left cancellation laws, we have $ba = ab$, which is the claim. □

Page 64

4. Prove that in any group, an element and its inverse have the same order.

Proof. Suppose a is of infinite order. If, for some $n > 0$, $(a^{-1})^n = e$, then $a^n = a^n e = a^n(a^{-1})^n = (aa^{-1})^n = e$, which contradicts our assumption on the order of a. Thus, a^{-1} is also of infinite order.

Now suppose $|a| = m$, and $|a^{-1}| = n$. If $m > n$, then we have $a^{m-n} = e$, with $m > m - n > 0$, which contradicts our assumption that $|a| = m$. Thus, $m \leq n$. Similarly, if $n > m$, then $(a^{-1})^{n-m} = e$, with $n > n - m > 0$, which contradicts our assumption that $|a^{-1}| = n$. Thus, $n \leq m$, so $n = m$. □

22. Complete the partial Cayley table given below:

·	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			
6	6	5	7	8		1		
7	7	8	5	6			1	
8	8	7	6	5				1

Solution: In order that the table be a group, the group laws must be satisfied. Thus, we can use associativity of the group multiplication to help us complete the table. Also, each element among $\{1, 2, \ldots, 8\}$ must appear exactly once in each row and column. Note, since $5 = 2 \cdot 6$, we have $5 \cdot 6 = (2 \cdot 6) \cdot 6 = 2 \cdot 6^2 = 2 \cdot 1 = 2$. Similarly, $6 \cdot 5 = (2 \cdot 5) \cdot 5 = 2 \cdot 5^2 = 2 \cdot 1 = 2$. Note, $5 \cdot 8 = 5 \cdot (5 \cdot 3) = 5^2 \cdot 3 = 1 \cdot 3 = 3$.

Now, 4 is the only element which hasn't appeared n the "5" row, so we must have $5 \cdot 7 = 4$. (Or we could note $5 \cdot 7 = 5 \cdot (5 \cdot 4) = 5^2 \cdot 4 = 1 \cdot 4 = 4$.) Thus, the table, so far looks as follows:

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1	2	4	3
6	6	5	7	8	5	1		
7	7	8	5	6			1	
8	8	7	6	5				1

Now, note, since $5 \cdot 7 = 4$, we cannot have $6 \cdot 7 = 4$ (again each element appears once in each row and column – or we could note if $5 \cot 7 = 6 \cdot 7$, then, since $7^2 = 1$, we have $5 \cdot 7^2 = 6 \cdot 7^2$, or $5 = 6$, which is a contradiciton.) Thus, $6 \cdot 7 = 3$ and $6 \cdot 8 = 4$. Now looking at the last two columns, we see the only choices are $7 \cdot 8 = 2$, and $8 \cdot 7 = 2$. Thus, the table now looks like,

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1	2	4	3
6	6	5	7	8	5	1	3	4
7	7	8	5	6			1	2
8	8	7	6	5			2	1

= Now, to fill in the last four squares, we note $7 \cdot 5 = 7 \cdot (7 \cdot 3) = 7^2 \cdot 3 = 1 \cdot 3 = 3$. Now, we see $7 \cdot 6 = 4$. So, finally , we must have $8 \cdot 5 = 4$, and $8 \cdot 6 = 3$. So, the table must be:

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1	2	4	3
6	6	5	7	8	5	1	3	4
7	7	8	5	6	3	4	1	2
8	8	7	6	5	4	3	2	1

□

Page 81

7. Find an example of a noncyclic group, all of whose proper subgroups are cyclic.

Solution: Let G be an abelian group of order 4, with elements $\{e, a, b, ab|\ \ |a| = |b| = 2\}$. Then the proper subgroups of G are: $H_1 = \{e, a\} =< a >$, $H_2 = \{e, b\} =< b >$, and $H_3 = \{e, ab\} =< ab >$. Note that, since the product of any two of a, b or ab is the third, that a subgroup with any two of a, b, and ab is equal to G. Thus, all the proper subgroups of G are cyclic. On the other hand, G is not cyclic, since we see that $< a >$, $< b >$, and $< ab >$ are all proper subgroups of G.□

11. Let G be a group and $a \in G$. Prove $\langle a \rangle = \langle a^{-1} \rangle$.

Solution: Recall $\langle a \rangle = \{a^n \mid a \in \mathbb{Z}\}$. Since $a^{-1} = a^n$, for $n = -1$, we see $a^{-1} \in \langle a \rangle$, and thus, $\langle a^{-1} \rangle \subseteq \langle a \rangle$. But on the other hand $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$, so $\langle a \rangle \subseteq \langle a^{-1} \rangle$. Thus, $\langle a^{-1} \rangle = \langle a \rangle$.□

18. If a cyclic group has an element of infinite order, how many elements of finite order does it have?

Solution Since $|e| = 1$, there is at least one element of G of finite order. Let $G =< a >$. Since G has an element of infinite order, a is of infinite order. Suppose a^j is an element of finite order, for some $j \neq 0$. Then $(a^j)^n = e$, and therefore, $a^{jn} = e$. By the Corollary to Theorem 4.1, the order of a divides jn. Thus $|a| = \ell$ for some $\ell < \infty$. But, if $|a| = \ell$, then $G =< a >= \{e, a, a^2, \ldots, a^{\ell-1}\}$ is a finite group. This contradicts our assumption that G has an element of infinite order. Therefore, a^j is of infinite order for every $j \neq 0$, and therefore e is the only element of G of finite order.□

31. Let G be a finite group. Show there is a fixed positive integer n so that $a^n = e$ for all $a \in G$.

Proof: Let $G = \{e, a_1, \ldots, a_k\}$. For each $1 \leq i \leq k$, let $m_i = |a_i|$. Then $a_i^{m_i} = e$. Now let $n = \text{lcm}(m_1, m_2, \ldots, m_k)$. Then $m_i | n$ for each i and hence $a_i^n = e$. Since $e^n = e$, we see $a^n = e$ for all $n \in G$.□

Page 113

6. Show that A_8 contains an element of order 15.

Proof: Recall that a 3–cycle $(abc) = (ab)(ac)$ is even, and a 5–cycle $(abcxy) = (ab)(ac)(ax)(ay)$ is even. So $(123) \in A_8$ and $(45678) \in A_8$. Therefore, $\alpha = (123)(45678) \in A_8$. Since (123) and (45678) are disjoint, Ruffini's theorem says that $|\alpha| = 15$.□

30. What cycle is $(a_1\ a_2 \ldots a_n)^{-1}$?

Solution: Recall that $\alpha = (a_1\ a_2 \ldots a_n)$ is a one to one and onto function, from a a set A to itself. If $\alpha(a) = b$, then $\alpha^{-1}(b) = a$. Since $\alpha(a_1) = a_2$, we have $\alpha^{-1}(a_2) = a_1$. For $2 \leq j \leq n-1$, we have $\alpha(a_j) = a_{j+1}$, so $\alpha^{-1}(a_{j+1}) = a_j$. Note that $\alpha(a_n) = a_1$, so $\alpha^{-1}(a_1) = a_n$. Finally, α fixes all indices except for $a_1, \ldots, a_n$. Thus

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

31. Let G be a group of permutations on a set X. Let $a \in X$, and define $\text{stab}(a) = \{\alpha \in G | \alpha(a) = a\}$. We call $\text{stab}(a)$ the stabilizer of a in G. Prove that $\text{stab}(a)$ is a subgroup of G.

Proof: We will use the two step subgroup test. First note that stab(a) is non-empty. If ε is the identity permutation on X, then, by definition, $\varepsilon(x) = x$ for all $x \in X$. In particular, $\varepsilon(a) = a$, and hence, $\varepsilon \in \text{stab}(a)$. Therefore, stab($a$) is non-empty. Now we need to show that if $\alpha, \beta \in \text{stab}(a)$, then $\alpha\beta$ and $\alpha^{-1} \in \text{stab}(a)$. First note that $\alpha\beta(a) = \alpha(\beta(a))$. Since $\beta \in \text{stab}(a)$, we know that $\beta(a) = a$. Therefore, $\alpha\beta(a) = \alpha(a) = a$, since $\alpha \in \text{stab}(a)$. Consequently, stab($a$) is closed under the group operation in G. Next suppose $\alpha(a) = a$. Then, by multiplying by α^{-1} on each side, i.e., applying the function α^{-1} to each side, we see that $\alpha^{-1}(\alpha(a)) = \alpha^{-1}(a)$, and thus, $\alpha^{-1}\alpha(a) = \varepsilon(a) = a = \alpha^{-1}(a)$. We conclude that if $\alpha \in \text{stab}(a)$, then $\alpha^{-1} \in \text{stab}(a)$. This completes the proof.□

Page 133

6. Prove that the relation isomorphism is transitive.

Proof: We need to show that if $G \cong H$ and $H \cong K$, then $G \cong K$. Let $\varphi : G \longrightarrow H$ and $\psi : H \longrightarrow K$ be isomorphisms. By Theorem 0.3, $\psi\varphi : G \longrightarrow K$ is both one-to-one and onto. Suppose $x, y \in G$. Then $\psi\varphi(xy) = \psi(\varphi(xy))$, and since φ is an isomorphism we have $\psi\varphi(xy) = \psi(\varphi(x)\varphi(y))$. Note that $\varphi(x)$ and $\varphi(y)$ are elements of H, and ψ is an isomorphism. Thus, $\psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = \psi\varphi(x)\psi\varphi(y)$. Therefore, $\psi\varphi$ is an isomorphism, and $G \cong K$. This establishes the claim.□

7. Prove that S_4 is not isomorphic to D_{12}.

Proof Note that both groups are of order 24. In S_4, the values for the order of an element are 1, 2, 3, or 4. However, the element R_{30} of D_{12} has order 12. Thus, by property 5 of Theorem 6.1, D_{12} cannot be isomorphic to S_4.□

17. Let $r \in U(n)$. Prove that the mapping $\alpha : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ defined by $\alpha(s) = sr$ for all $s \in \mathbb{Z}_n$ is an automorphism of $\mathbb{Z}_n$.

Proof: We need to to show that α is one-to-one, onto, and preserves the group operation in $\mathbb{Z}_n$. We begin by showing that α is onto. That is, we intend to show that, for each $y \in \mathbb{Z}_n$, there is an $s \in \mathbb{Z}_n$ with $\alpha(s) = y$. Since $r \in U(n)$, we know

that $gcd(n, r) = 1$, and therefore the equation $xr = 1(\text{mod } n)$ is solvable. So, for some $x \in \mathbb{Z}_n,\ \alpha(x) = 1$. Let $s = yx$. Then $\alpha(s) = sr = (yx)r = y(xr) = y(\ \text{mod } n)$. Thus, we know that α is onto. Since α is an onto function from $\mathbb{Z}_n$ to itself, α is one-to-one. (A direct proof that α is one-to-one is as follows: If $\alpha(s) = \alpha(t)$, then $sr = tr\ (\text{mod } n)$. Thus, $n|r(s-t)$, and, since $gcd(n, r) = 1$, $n|(s-t)$. Thus, $s = t$.)

We finally need to show that α preserves the group operation. Let $s, t \in \mathbb{Z}_n$. Then $\alpha(s+t) = (s+t)r = sr + tr = s\alpha + t\alpha\ (\text{mod } n)$. Thus, α is an isomorphism. □

35. Suppose g and h induce the same inner automorphism of a group G. Prove $h^{-1}g \in Z(G)$.

Proof: Let φ_g and φ_h be the inner automorphisms induced by g and h, respectively. Then, for any $x \in G$, we have $\varphi_g(x) = \varphi_h(x)$, which says $gxg^{-1} = hxh^{-1}$, for every $x \in G$. Multiplying on the left by h^{-1} and the right by g we have $h^{-1}gx = xh^{-1}g$. Thus, $h^{-1}g$ commutes with every $x \in G$. Therefore, by definition, $h^{-1}g \in Z(G)$.□.

Page 149

6. Let n be an integer greater than 1. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$. Find all the left cosets of H in $\mathbb{Z}$. How many of them are there?

Solution: Suppose $a + H = b + H$. Then $b - a \in H$, which is equivalent to $n|(b-a)$. Thus $a + H = b + H$ if and only if $a = b \bmod n$. Thus the left cosets of H in $\mathbb{Z}$ are $0 + H, 1 + H, \dots, (n-1) + H$, and hence there are n of them.□

17. Compute $5^{15} \bmod 7$ and $7^{13} \bmod 11$.

Solution: Since 7 is prime, $U(7)$ is cyclic, of order 6, and this $5^6 = 1 \bmod 7$. Thus $5^{12} = 1 \bmod 7$, and therefore $5^{15} \equiv 5^3 \equiv 5^2 \cdot 5 \equiv 4 \cdot 5 \equiv 6 \bmod 7$. Similarly, $U(11)$ is cyclic of order 10, so $7^{10} \equiv 1 \bmod 11$. Thus, $7^{13} \equiv 7^3 \equiv 7^2 \cdot 7 \equiv 5 \cdot 7 \equiv 2 \bmod 11$.□

Note: An alternative proof is to use Fermat's Little Theorem, which says $x^p \equiv x \bmod p$.

26. Suppose that G is a group with more than one element, and G has no proper, nontrivial subgroup. Prove that $|G|$ is prime.

Proof: Let $a \in G$, with $a \neq e$. Then $< a >$ is a nontrivial subgroup of G. Thus, by our hypothesis, $G =< a >$. If $|a|$ is infinite, then $G \simeq \mathbb{Z}$ (see Example 2 of Chapter 6). Then $< a^2 >$ is a proper, nontrivial subgroup of G, which contradicts our assumption. Thus, $|a|$ must be finite. Now, G is a finite cyclic group. If d divides $|G|$, then, by the Fundamental Theorem of Cyclic Groups, there is a cyclic subgroup of G of order d. Since G and $\{e\}$ are the only subgroups of G, we see that $|G|$ can have no proper divisors, i.e., $|G|$ must be prime.□

36. Let G be a group of order p^n, where p is prime. Prove the center of G cannot have order p^{n-1}.

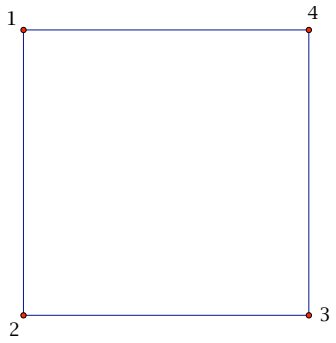
Proof: Let $Z = Z(G)$ be the center of G, and suppose $|Z| = p^{n-1}$. Then $Z \neq G$, so G is nonabelian. Suppose $x \notin Z$. We claim none of $x, x^2, \ldots, x^{p-1}$ are elements of Z. Suppose not. Then $x^k \in Z$, for some $2 \leq k \leq p-1$. Now, $|Z| = p^{n-1}$, so $(x^k)^{p^{n-1}} = e$. But then $x^{p^{n-1}k} = e$, so $|x|$ divides $p^{n-1}k$. Since $|x|$ divides $|G| = p^n$, we see k must be a power of p, which contradicts our assumption. Thus, $x^k \notin Z$ for $k = 1, 2, \ldots, p-1$. Now, I claim $x^k Z \neq x^j Z$, for $1 \leq k < j \leq p-1$. For if not, $x^{j-k} \in Z$, which contradicts what we just showed. Since $|G : Z| = |G|/|Z| = p$, there are p distinct cosets of Z in G. Thus $Z, xZ, \ldots, x^{p-1}Z$ are the distinct cosets of Z in G. Therefore, every $y \in G$ can be written in the form $x^j z$ for some $0 \leq j \leq p-1$, and some $z \in Z$. Now if $y_1, y_2 \in G$, then $y_1 = x_j z_1$, and $y_2 = x^k z_2$, we have $y_1 y_2 = y_2 y_2$, (since $z_i \in Z$ and powers of x commute with each other). Then G is abelian, contradicting our assumption. Thus, $|Z| \neq p^{n-1}$.□

Note: There is a much easier proof using the G/Z theorem in Chapter 9.

Page 494

1. Determine the number of ways in which the four corners of a square can be colored with two colors.

Solution: Number the corners of the square $1, 2, 3, 4$ in the counterclockwise direction, as in the picture.



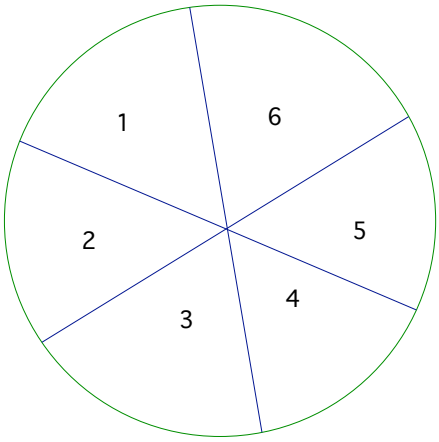
There are $2^4 = 16$ ways to arrange the colors of the corners. In order to determine the number of non-equivalent, we use Burnside's Lemma. The symmetries of the square are given by D_4. Notice that R_0 fixes all 16 arrangements. R_{90} and R_{270} only fix arrangements with all four colors the same color. Since the orbits under R_{180} are $\{1, 3\}$ and $\{2, 4\}$, the colorings fixed by R_{180} are the ones with vertices 1 and 3 are the same color, and vertices 2 and 4 are the same color. Thus, R_{180} fixes 4 colorings. The orbits under H are $\{1, 2\}$ and $\{3, 4\}$, so H (and similarly V) fixes 4 arrangements. Note the diagonal reflection D has orbits $\{1\}, \{3\}$ and $\{2, 4\}$, so fixes $2^3 = 8$ arrangements. Similarly D' fixes 8 arrangements. Thus, by Burnside's Lemma there are

$$\frac{1}{|D_4|} \sum_{\phi \in D_4} |\operatorname{fix}(\phi)| = \frac{1}{8} (16 + 2 \cdot 2 + 4 + 2 \cdot 4 + 2 \cdot 8) = \frac{1}{8}(48) = 6$$

non-equivalent colorings.

11. Suppose we cut a cake into 6 identical pieces. How many ways can we color the cake with n colors if each piece gets one color.

Proof: Number the slices of the cake 1 through 6 as in the picture.



There are n^6 arrangements of the colors of slices on the cake. The symmetry group of our cake is $G = \{R_0, R_{60}, R_{120}, R_{180}, R_{240}, R_{300}\}$, the subgroup of rotations in D_6. (We do not allow reflections, since we wouldn't want to turn the cake upside down.) Look at the orbits of each type of element. element. R_0 fixes every element, and hence fixes all n^6 colorings. For a rotation of order 6 there is one orbit $\{1, 2, 3, 4, 5, 6\}$. So these two elements fix n colorings. The two rotations of order 3 have two orbits $\{1, 3, 5\}$ and $\{2, 4, 6\}$. Thus, these elements fix n^2 elements. Finally, the element R_{180} has three orbits: $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$. Thus this element fixes n^3 elements. Applying Burnside's Lemma we a have the number of colorings of the cake is

$$\frac{1}{|G|}\sum_{\phi\in G}|\operatorname{fix}(\phi)| = \frac{1}{6}\left(n^6 + 2n + 2n^2 + n^3\right).$$

Page 167

7. Prove that $G_1 \oplus G_2$ is isomorphic to $G_2 \oplus G_1$.

Proof. Let $\psi : G_1 \oplus G_2 \longrightarrow G_2 \oplus G_1$ be given by $\psi(g_1, g_2) = (g_2, g_1)$, for each $(g_1, g_2) \in G_1 \oplus G_2$. Note that if $\psi(g_1, g_2) = \psi(h_1, h_2)$, then $(g_2, g_1) = (h_2, h_1)$, so $g_1 = h_1$, and $g_2 = h_2$. In other words, if $\psi(g_1, g_2) = \psi(h_1, h_2)$, then $(g_1, g_2) = (h_1, h_2)$, and thus ψ is one-to-one. Now suppose that $(g_2, g_1) \in G_2 \oplus G_1$. Then $(g_2, g_1) = \psi(g_1, g_2)$, i.e., ψ

is onto. If (g_1, g_2), and (h_1, h_2) are in $G_1 \oplus G_2$, then

$$\psi((g_1, g_2)(h_1, h_2)) = \psi(g_1h_1, g_2h_2) = (g_2h_2, g_1h_1)$$
$$= (g_2, g_1)(h_2, h_1) = \psi(g_1, g_2)\psi(h_1, h_2).$$

Thus, ψ is an isomorphism, so $G_1 \oplus G_2 \cong G_2 \oplus G_1$. □

26. Find a subgroup of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ which is not of the form $H \oplus K$, with H a subgroup of $\mathbb{Z}_4$ and K a subgroup of $\mathbb{Z}_2$.

Solution: Let $a = (1, 1)$. Then $|a| = 4$, and $< a >= \{(0, 0), (1, 1), (2, 0), (3, 1)\}$ is not of the form $H \oplus K$. For $< a >$ has an element of order 4, which means H would have to be all of $\mathbb{Z}_4$, but then, as the second coordinates are not all 0, we would also have to have $K = \mathbb{Z}_2$, which would imply $< a >= \mathbb{Z}_4 \oplus \mathbb{Z}_2$, but this isn't the case. □

39 If a finite abelian group has exactly 24 elements of order 6, how many cyclic subgroups of order 6 does it have?

Solution: Suppose G is our finite abelian group, with 24 elements of order 6. Suppose $H \leq G$ is a cyclic subgroup of order 6. Then $H =< a >$, and $|a| = 6$. Furthermore, H contains exactly $\varphi(6) = 2$ elements of order 6, namely a and a^5. Since every element of order 6 generates a cyclic subgroup of order 6, we see that there are $24/2 = 12$ cyclic subgroups of order 6 in G.□

Page 193

4. Let $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, d \neq 0, b \in \mathbb{R} \right\}$. Is H a normal subgroup of $GL(2, \mathbb{R})$?

Solution: No. Recall that H is normal in G if $aHa^{-1} = H$, for all $a \in G$. Let $h = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in H$. Let $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $A^{-1} = A$, and

$$AhA^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \notin H.$$

Thus, H is not normal in $GL(2, \mathbb{R})$.□

38. Suppose that H is a normal subgroup of G and let $a \in G$. If aH is of order 3 in G/H, and $|H| = 10$, what are the possibilities for $|a|$.

Solution: Since aH is of order 3, we see that $a^3H = H$, which is equivalent to $a^3 \in H$. By Corollary 1 to Lagrange's Theorem, we see that $|a^3| = 1, 2, 5$, or 10. Thus, $|a| = 3, 6, 15$, or 30. □

46. If G is a group and $[G : Z(G)] = 4$, prove $G/Z(G) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Proof. Since $[G : Z(G)] = 4$, we know $|G/Z(G)| = 4$, so either $G/Z(G) \cong \mathbb{Z}_4$, or $G/Z(G) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. But if $G/Z(G) \cong \mathbb{Z}_4$, then, by the G/Z–Theorem, G is abelian, so $|G/Z(G)| = 1$, which is not true. Thus, we must have $G/Z(G) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. □

62. Suppose G has a subgroup of order n. Show the intersection of all subgroups of order n is a normal subgroup of G.

Proof. Let $|H| = n$. Note that if $a \in H$, then aHa^{-1} s a subgroup of order n. (To see this note that if $h_1, h_2 \in H$, then $(ah_1a^{-1})(ah_2a^{-1})^{-1} = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$, so the claim holds by the one step subgroup test.) Now, let K be the intersection of all subgroups of order n. By assumption, K is non-empty, since $e \in K$. If $k \in K$, and $a \in G$, then we need to show $aka^{-1} \in K$. If H is any subgroup of order n, then, by definition, $k \in H$. But above we showed $a^{-1}Ha$ is a subgroup of order n (we replace a with a^{-1} here) so, since $k \in K$, we have $k \in a^{-1}Ka$. □

Page 211

8. Let G be a group of permutations. For each $\sigma \in G$, define

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is an even permutation,} \\ -1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Prove that sgn is a homomorphism from G to $\{\pm 1\}$. What is the kernel? Why does this allow you to conclude A_n is a normal subgroup of of S_n of index 2.

Proof. Suppose $\sigma, \tau \in G$. If $\sigma\tau$ is even, then $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau)$, and we see that $1 = \operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. If $\sigma\tau$ is odd, then $\operatorname{sgn}(\sigma) = -\operatorname{sgn}(\tau)$, and so $-1 = \operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. Thus, for all σ, τ we have $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$, so sgn is a homomorphism.

Note that $\ker \operatorname{sgn} = \{\sigma \in G | \operatorname{sgn}(\sigma) = 1\} = \{\sigma \in G | \sigma \text{ is even}\}$. Thus, if $G \subset S_n$, we have $\ker \operatorname{sgn} = G \cap A_n$. Now suppose $G = S_n$. Then $\ker \operatorname{sgn} = A_n$, and $\operatorname{sgn}(S_n) = \{\pm 1\}$. Since A_n is the kernel of a homomorphism, it is a normal subgroup. Moreover, we have $S_n/A_n \simeq \{\pm 1\}$ is of order 2, so $|S_n : A_n| = 2$. □

9. Prove that the mapping from $G \oplus H$ to G given by $(g, h) \mapsto g$ is a homomorphism. What is the kernel?

Proof. We denote the map by p, i.e., $p((g, h)) = g$. (For geometric motivation, take $G = H = \mathbb{R}$, so p is the projection of a point (x, y) onto the x–axis.) Let $(g_1, h_1), (g_2, h_2) \in G \oplus H$. Then

$$p((g_1, h_1)(g_2, h_2)) = p((g_1 g_2, h_1 h_2)) = g_1 g_2 = p((g_1, h_1))p((g_2, h_2)),$$

so p is a homomorphism. Let e_G be the identity of G. Note that $\ker p = \{(g, h) | p((g, h)) = e_G\} = \{(e_G, h) | h \in H\}$. □

21. Suppose that φ is a homomorphism from $\mathbb{Z}_{30}$ onto a group of order 5. Determine the kernel of φ.

Solution: Since φ is onto, we have $|\varphi(\mathbb{Z}_{30})| = 5$. We also know that $|\mathbb{Z}_{30}| = 30$. By the First Isomorphism Theorem, we know that $\mathbb{Z}_{30}/\ker\varphi \simeq \varphi(\mathbb{Z}_{30})$, and thus $|\mathbb{Z}_{30}/\ker\varphi| = 5$. By Lagrange's Theorem, $|\ker\varphi| = 6$, and by the Fundamental Theorem of Cyclic Groups, $\mathbb{Z}_{30}$ has a unique subgroup of order 6. Thus, $\ker\varphi$ must be this subgroup, i.e., $\ker\varphi =< 5 >= \{0, 5, 10, 15, 20, 25\}$. □

30. Suppose that $\varphi : G \longrightarrow \mathbb{Z}_6 \oplus \mathbb{Z}_2$, is onto and $|\ker\varphi| = 5$. Explain why G must have normal subgroups of orders $5, 10, 15, 10, 30$, and 60.

Explanation: Recall that if $K \subset Z_6 \oplus \mathbb{Z}_2$ is a subgroup, then $K \triangleleft \mathbb{Z}_6 \oplus \mathbb{Z}_2$ (since $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ is abelian). Since φ is onto, $\varphi^{-1}(K) = \{g \in G | \varphi(g) \in K\}$ is normal in G (Theorem 10.2) Since $\ker \varphi$ is of order 5, part 6 of Theorem 10.1 implies that $|\varphi^{-1}(K)| = 5|K|$. Since the possible orders for K are $1, 2, 3, 4, 6$, and 12, we see that G has normal subgroups of order $5, 10, 15, 20, 30$, and 60. □

Page 226

9. Suppose G is an abelian group of order 120, and G has exactly three elements of order 2. Determine the isomorphism class of G.

Solution: The prime factorization of 120 is $2^3 \cdot 3 \cdot 5$. By the Fundamental Theorem of Finite Abelian Groups, G is isomorphic to one of the following three groups:

$$G_1 = \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

$$G_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

$$G_3 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5.$$

Note that since $gcd(8, 3, 5) = 1$, we have $G_1 \simeq \mathbb{Z}_{120}$. By Theorem 4.4, $\mathbb{Z}_{120}$ has $\varphi(2) = 1$ element of order 2. Therefore, $G \not\simeq G_1$. Suppose that $x = (a_1, a_2, a_3, a_4, a_5)$ is an element of order 2 in G_3. Then $2 = |x|$ implies $a_4 = 0 (\text{mod } 3)$ and $a_5 = 0 (\text{mod } 5)$. Therefore, $x = (a_1, a_2, a_3, 0, 0)$. Now we have 8 choices for $x = (a_1, a_2, a_3, 0, 0)$, and only one of them, $(0, 0, 0, 0, 0)$, is not of order 2. Therefore, G_3 has 7 elements of order 2, so $G \not\simeq G_3$. Thus, we must have $G \simeq G_2$. (Check though!) □

10. Find all abelian groups (up to isomorphism) of order 360.

Solution: Since $360 = 2^3 3^2 5$, we see, from the Fundamental Theorem of finite abelian groups, that the list of isomorphism classes is as follows:

$$\mathbb{Z}_{360} \simeq \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$$

$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5. \quad \square$$

12. Suppose the order of some finite abelian group is divisible by 10. Show that G has a cyclic subgroup of order 10.

Proof. Since 10 divides the order of G, and G is abelian, we know that G contains a subgroup of order 10. (See the Corollary to the Fundamental Theorem of Finite Abelian Groups.) Let H be such a subgroup. Since G is abelian, H is abelian. Since H has order $10 = 2 \cdot 5$, we see that $H \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_{10}$. $\square$

29. Let G be an abelian group of order 16. Suppose that there are elements a and b in G such that $|a| = |b| = 4$, but $a^2 \neq b^2$. Determine the isomorphism class of G.

Solution: We know that there are five non-isomorphic abelian groups of order 16 :

$$\mathbb{Z}_{16}$$

$$G_1 = \mathbb{Z}_8 \oplus \mathbb{Z}_2$$

$$G_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_4$$

$$G_3 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$G_4 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Since G has elements of order 4, we see that $G \not\simeq G_4$. Since $|a^2| = |b^2| = 2$, we see that G has at least two elements of order 2, so $G \not\simeq \mathbb{Z}_{16}$. Note that, if $(x, y, z) \in G_3$, and $|(x, y, z)| = 4$, then $x = 0$ or $3 \bmod 4$, and since $y, z \in \mathbb{Z}_2$, we see that $2y = 2z = 0 \bmod 2$. Now, $(x, y, z)^2 = (2, 0, 0)$, so the squares of all elements of order 4 in G_3 are equal. Thus, $G \not\simeq G_3$. Similarly, if (x, y) is of order 4 in G_1, then $x = 2$ or 6, and $(x, y)^2 = (2x \bmod 8, 2y \bmod 2) = (4, 0)$, and thus all the squares of the elements of order 4 in G_1 are equal. So, by the process of elimination, $G \simeq G_2$. Note that $a = (0, 1)$ and $b = (1, 0)$ are elements of G_2 with the desired property. □

pg. 242

8. Show that a ring is commutative if it has the property that $ab = ca$ implies $b = c$.

Proof. We need to show that if $x, y \in R$ then $xy = yx$. Let $a = x$ $b = yx$ and $c = xy$. Then $ab = x(yx) = (xy)x = ca$. Thus, by the hypothesis, $b = c$, or $xy = yx$. Thus, for $x, y \in R$ we have $xy = yx$. □

22. Let R be a commutative ring with unity, and let $U(R)$ denote the set of units in R. Prove that $U(R)$ is a subgroup under the ring multiplication in R.

Proof. Let 1 be the unity, i.e., the multiplicative identity of R. If $a, b, c \in U(R)$, then $(ab)c = a(bc)$, since this is a defining property of the ring R. We have to show $U(R)$ is closed. Suppose $a, b \in R$ and a^{-1}, b^{-1} are their inverses (see Theorem 12.2 – exercise 5). Now $(ab)(b^{-1}a^{-1} = a(bb^{-1})a^{-1} = a1a^{-1} = 1$, so ab is a unit. Thus, $U(R)$ is closed under multiplication. Also, 1 is an identity for this operation on $U(R)$. Finally, if $a \in U(R)$, then $aa^{-1} = 1$, so a^{-1} is also a unit, and thus, every element of $U(R)$ has an inverse in $U(R)$. Therefore, $U(R)$ s a group with the ring multiplication of R as its group operation. □

pg. 255

8. Describe all zero divisors and units of $\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$.

Solution: The zero element of $R = \mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$ is $(0, 0, 0)$. Note, each of $\mathbb{Z}$ and $\mathbb{Q}$ individually is an integral domain, so has no zero divisors. The multiplication in R is component-wise. So suppose $(a, b, c)(x, y, z) = (0, 0, 0)$, with

$$(a, b, c) \neq (0, 0, 0) \text{ and } (x, y, z) \neq (0, 0, 0). \tag{1}$$

Then $(ax, by, cz) = (0, 0, 0)$, so one of a or x is zero, as is one of b or y, and one of c or z. By (1) we see at least one of a, b, c and one of x, y, z must be zero. Conversely, suppose One component of $s = (a, b, c)$ is zero. Let r be the element of R with one non-zero component, namely the one corresponding to a zero component for (a, b, c), and take that component to be 1. Then $rs = (0, 0, 0$, with $r \neq 0$ and $s \neq 0$, so r is a zero divisor. Thus the zero divisors are the elements $(0, a, b), (a, 0, b)$, and $(a, b, 0)$, with $(a, b) \neq (0, 0)$.

Now, note the unity of R is $(1, 1, 1)$. Then (a, b, c) is a unit, if and only if each of $a, b, c \neq 0$. Since the units of $\mathbb{Z}$ are ± 1, andthe units of $\mathbb{Q}$ are all non-zero elements, then we see $U(R) = \{(\pm 1, x, \pm 1) | x \neq 0\}$. □

38. Construct a multiplication table for $\mathbb{Z}_2[i]$, the ring of Gaussian integers modulo 2. Is this ring a field? Is it an integral domain?

Solution:

$\cdot$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

Note that $1 + i$ has no multiplicative inverse, and thus $\mathbb{Z}_2[i]$ is not a field. Also, $(1 + i)(1 + i) = 0$, so, $\mathbb{Z}_2[i]$ is not an integral domain. □

Page 269

4. Find a subring of $\mathbb{Z} \oplus \mathbb{Z}$ which is not an ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

Solution: Let $S = \{(n, n) | n \in \mathbb{Z}\}$. Then S is a subring of $\mathbb{Z} \oplus \mathbb{Z}$. However, note that $(1, 1) \in S$, and $(2, 7) \cdot (1, 1) = (2, 7) \notin S$. Therefore, S is not an ideal. □

7. Let a belong to a commutative ring. Show that $aR = \{ar | r \in R\}$ is an ideal of R. If R is the ring of even integers, list the elements of $4R$.

Proof. Let $x, y \in aR$. Then we can choose $r, s \in R$, with $x = ar$ and $y = as$. Now, $x - y = ar - as = a(r - s) \in aR$, and $xy = (ar)(as) = a(ras) \in aR$. Thus, by the subring test, aR is a subring of R. Let $z \in R$, and $ar \in aR$. Then $(ar)z = a(rz) \in aR$. Moreover, since R is commutative,$z(ar) = a(rz) \in aR$, and thus aR is an ideal of R.

If $R = \{0, \pm 2, \pm 4, \pm 6, \dots\}$, then

$$R = \{4 \cdot 0, \pm 4 \cdot 2, \dots\} = \{0, \pm 8, \pm 16, \pm 24, \dots\} = 8\mathbb{Z}.$$

□

14. Let A and B be ideals of a ring R. Prove that $AB \subseteq A \cap B$.

Proof. Recall that

$$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n | a_i \in A, b_i \in b, n > 0\},$$

(see problem 10).

Suppose that $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in AB$. Since each $a_1 \in A$, and A is an ideal, we see that $a_ib_i \in A$ for each i. Since A is an ideal, it is closed under the ring addition, so $x = a_1b_1 + \cdots + a_nb_n \in A$. Similarly, since each $b_i \in B$, we have $a_ib_i \in B$ for each i. Therefore, $x \in B$. Since each $x \in AB$ is an element of both A and B, we see that $AB \subset A \cap B$. □

33. How many elements are in $\mathbb{Z}_3[i]/ < 3 + i >$? Give reasons for your answer.

Solution: Note that $(3 + i)(3 - i) = 10 \in < 3 + i >$. Therefore, for any $a, b, k \in \mathbb{Z}$, we have $a + bi + < 3 + i >= a - 10k + bi + < 3 + i >$. Thus, we can always

choose a coset representative $a_0 + b_0 i$ for $a + bi + < 3 + i >$ with $0 \leq a_0 \leq 9$. Further note that $i + < 3 + i >= i - (3 + i) + < 3 + i >= -3 + < 3 + i >$. Thus, $a + bi + < 3 + i >= a + b(-3) + < 3 + i >= a - 3b + < 3 + i >$. Thus, every coset has a representative in $\mathbb{Z}$, i.e. $a + bi + < 3 + i >= k + < 3 + i >$, for some $k \in \mathbb{Z}$. Moreover by the above discussion, we can choose $0 \leq k \leq 9$. Now, suppose that $0 \leq a, b \leq 9$, and $a + < 3 + i >= b + < 3 + i >$. Then $a - b \in < 3 + i >$, so $k = a - b = (3 + i)(c + di)$. Notice that $k(3 - i) = 10(c + di) = 10c + 10di$. Since $-ki = 10di$, we have $10|k$, so $10|a - b$, and therefore, $a = b$. Thus, all the cosets $k + < 3 + i >$, with $0 \leq k \leq 9$ are distinct. $\mathbb{Z}_3[i]/ < 3 + i >$ has ten elements. □

56 Show that $\mathbb{Z}[i]/ < 1 - i >$ is a field. How many elements does this field have?

We give two proofs.

Proof. **1.** We know that it is enough to prove that $< 1 - i >$ is a maximal ideal. Note that $(1 - i)^2 = -2i \in < 1 - i >$, and therefore, $2 = i(-2i) \in < 1 - i >$. Now, suppose that B is an ideal of $\mathbb{Z}[i]$ with $B \supsetneq < 1 - i >$. We need to show that $B = \mathbb{Z}[i]$. Let $a + bi \in B$ with $a + bi \notin < 1 - i >$. Note that we can write $a + bi = a(1 - i) + (a + b)i$. Since $a(1 - i) \in < 1 - i > \subset B$ and $a + bi \in B$, we have $(a + b)i = a + bi - a(1 - i) \in B$. We claim that $a + b$ is odd. Suppose to the contrary that $a + b$ is even. Then $(a + b)i = 2(ki)$ for some $k \in \mathbb{Z}$, and since $2 \in < 1 - i >$ $(a + b)i \in < 1 + i >$ and then $a + bi = a(1 - i) + (a + b)i \in < 1 - i >$, which contradicts our choice of $a + bi$. Thus, we have substantiated our claim that $a + b$ is odd. Write $a + b = 2k + 1$ for some integer k. Note that we know that $2ki \in < 1 - i >$ and $(a + b)i = (2k + 1)i \in B$. Thus, since B is an ideal

$$1 = -i\left((2k + 1)\, i - 2ki\right) \in B.$$

Thus, $B \supset < 1 >= Z[i]$, which implies $B = \mathbb{Z}[i]$, and thus $< 1 - i >$ is maximal. Consequently, $\mathbb{Z}[i]/ < 1 - i >$ is a field.

Note that if $a+bi \in \mathbb{Z}[i]$, then $a = 2k+\varepsilon$ and $b = 2j+\delta$, with $\varepsilon, \delta \in \{0,1\}$. Thus,

$$a+bi+ < 1-i >= (\varepsilon+\delta i) + (2k+2ji)+ < 1-i >= \varepsilon+\delta i+ < 1-i >,$$

since 2 and $2i$ are elements of $< 1-i >$. Thus, every element of $\mathbb{Z}[i]/ < 1-i >$ is of the form $\varepsilon+\delta i+ < 1-i >$. However, these are not distinct.Note that $1+ < 1-i >= i+ < 1-i >$ and, since $1+i = i(1-i)$ we have $1+i+ < 1-i >=< 1-i >$. Thus, there are two elements of $\mathbb{Z}[i]/ < 1-i >$, namely, $< 1-i >$ and $1+ < 1-i >$. □

2.We start again by noting that $2, 2i \in < 1-i >$. and thus if $a+bi \notin < 1-i >$ then $a+b$ is odd. Now suppose that $a+bi+ < 1-i > \neq < 1-i >$. Then, in the factor ring

$$(a+bi+ < 1-i >)^2 = a^2-b^2+2abi+ < 1-i >= a^2-b^2+ < 1-i >,$$

since $2abi \in < 1-i >$. But now, $(a^2-b^2) = (a+b)(a-b)$ is odd, so

$$(a^2-b^2)+ < 1-i >= 1+ < 1-i >,$$

which is the identity of $\mathbb{Z}[i]/ < 1-i >$. Thus, for every non-zero element $x \in \mathbb{Z}[i]/ < 1-i >$, we see $x^2 = 1+ < 1-i >$, and thus x is invertible. Therefore, $\mathbb{Z}[i]/ < 1-i >$ is a field. The counting argument is then as in Proof 1. □

Page 287

5. Show the correspondence $x \mapsto 5x$ from $\mathbb{Z}_5 \to \mathbb{Z}_{10}$ does not preserve addition.

Solution: Note we have $0 \mapsto 0$, $1 \mapsto 5$, $2 \mapsto 0$, $3 \mapsto 5$, $4 \mapsto 0$. Note $3+3 = 1 \bmod 5$, and if the map preserved addition, then we would have $5+5 = 5 \bmod 10$, which does not hold. □