Math 3110 **Final Exam** **May 6th, 2015**

Name: ANSWER KEY **Be sure to show your work!**

1. (12 points) Working in $\mathbb{Z}_{12}$.

(a) $(3) = \langle 3 \rangle = \{0, 3, 6, 9\}$ and $\mathbb{Z}_{12}/(3) = \{(3), 1+(3), 2+(3)\}$.

Notice that $|(3)| = 4$ so that $|\mathbb{Z}_{12}/(3)| = 12/4 = 3$ (three distinct cosets). Specifically, $(3) = \{0, 3, 6, 9\}$, $1+(3) = \{1, 4, 7, 10\}$, and $2+(3) = \{2, 5, 8, 11\}$ (these together partition $\mathbb{Z}_{12}$.

(b) Create addition and multiplication tables for $\mathbb{Z}_{12}/(3)$.

$+$	(3)	$1+(3)$	$2+(3)$
(3)	(3)	$1+(3)$	$2+(3)$
$1+(3)$	$1+(3)$	$2+(3)$	(3)
$2+(3)$	$2+(3)$	(3)	$1+(3)$

$\times$	(3)	$1+(3)$	$2+(3)$
(3)	(3)	(3)	(3)
$1+(3)$	(3)	$1+(3)$	$2+(3)$
$2+(3)$	(3)	$2+(3)$	$1+(3)$

Example computations: $[2+(3)]+[1+(3)] = (2+1)+(3) = 3+(3) = 0+(3) = (3)$ since $3 \in (3) = \{0, 3, 6, 9\}$. Also, $[2+(3)]+[2+(3)] = 4+(3) = 1+(3)$ since $4 \in 1+(3)$. Likewise, $(2+(3))(2+(3)) = 2^2+(3) = 4+(3) = 1+(3)$.

(c) Is $\mathbb{Z}_{12}/(3)$ a cyclic group under addition? Why or why not?

Yes. Any quotient of a cyclic group is cyclic. Specifically, we have $\mathbb{Z}_{12}/(3) = \langle 1+(3) \rangle$ (the other non-zero coset, $2+(3)$, also generates this group).

(d) Is $\mathbb{Z}_{12}/(3)$ an integral domain or field? Why or why not?

Yes, it is both. By looking at the tables, we can see that this quotient ring is a commutative ring with $1+(3) \neq 0+(3) = (3)$. Notice that non-zero cosets times non-zero cosets yield non-zero cosets, so there are no zero divisors (this is an integral domain). Also, $(1+(3))^{-1} = 1+(3)$ and $(2+(3))^{-1} = 2+(3)$ (the non-zero elements have inverses), so it is a field as well.

More briefly, we could notice that $\mathbb{Z}_{12}/(3) \cong \mathbb{Z}_3$ which is both an integral domain and field since $p = 3$ is prime.

(e) Is (3) a prime or maximal ideal in $\mathbb{Z}_{12}$? Why or why not?

It's both. Since $\mathbb{Z}_{12}/(3)$ is an integral domain, (3) is a prime ideal. Likewise, since the quotient is a field, (3) is a maximal ideal.

Note: Here we are using the theorem that states: For a commutative ring R with 1, $I \triangleleft R$ is prime iff R/I is an integral domain and $I \triangleleft R$ is maximal iff R/I is a field.

Since field $\implies$ integral domain, we get maximal $\implies$ prime (always). But for **finite** rings, integral domain $\implies$ field, so prime $\implies$ maximal. Thus our answer for an ideal in a **finite** ring (such as $\mathbb{Z}_{12}$) is necessarily either both or neither.

2. (8 points) Explain why each pair of **groups** are not isomorphic.

(a) $Q = \{\pm 1, \pm i, \pm j, \pm k\} \ncong \mathbb{Z}_8$

Both the quarternion group Q and $\mathbb{Z}_8$ have 8 elements. However, Q is not abelian while $\mathbb{Z}_8$ is abelian. Therefore, they are not isomorphic. [Alternatively, we could note: Q is not cyclic (since not abelian) vs. $\mathbb{Z}_8$ is cyclic OR Q has more elements of order 4 than $\mathbb{Z}_8$ does OR Q has no elements of order 8 while $\mathbb{Z}_8$ has several elements of order 8.]

(b) $S_5 \ncong D_{60}$ [Note: $5! = 120$]

Both S_5 and D_{60} are non-abelian groups of order 120 (since $5! = 120$ and $60 \cdot 2 = 120$). Thus they both fail to be cyclic as well. So far, no help showing they are not isomorphic.

However, if we start looking at orders of elements, we'll find data that doesn't match. The easiest mismatched data is that D_{60} has an element of order 60 (i.e. a rotation of $360/60 = 6°$) while S_5 does not have any elements of this order (the largest order appearing in S_5 is $6 = \text{lcm}(2, 3) = |(12)(345)|$).

Another approach [involving a difficult count] would be to notice that D_{60} has 61 elements of order 2 (the 180° rotation and 60 reflections) while S_5 has 25 elements of order 2 (10 transpositions and 15 pairs of disjoint transpositions – these counts are a little tricky to derive). Since D_{60} and S_5 don't have the same number of elements of order 2, they are not isomorphic.

3. (8 points) Explain why each pair of **rings** are not isomorphic.

(a) $\mathbb{Z} \ncong \mathbb{Q}$

Both of these are (countably) infinite commutative rings with 1. In fact, they're both integral domains. They both have characteristic zero as well. So far, everything matches (not helpful).

However, $\mathbb{Q}$ is a field while $\mathbb{Z}$ is not. Notice that all non-zero rational numbers are units (the reciprocal of a non-zero rational number is itself rational) while $2 \in \mathbb{Z}$ but $2^{-1} = 1/2 \notin \mathbb{Z}$. Therefore, they are not isomorphic.

(b) $(\mathbb{Z}_3)^{2\times 2} \ncong \mathbb{Z}_9 \oplus \mathbb{Z}_9$

Both of these rings are finite rings with 1 with 81 elements ($3^{2\times 2} = 3^4 = 81$ and $9 \cdot 9 = 81$). On the other hand, the matrix ring $(\mathbb{Z}_3)^{2\times 2}$ is not commutative while $\mathbb{Z}_9 \oplus \mathbb{Z}_9$ is commutative. Therefore, they are not isomorphic.

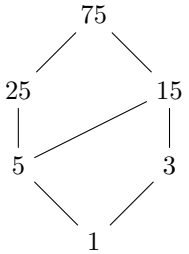
We could also see that they are not isomorphic by noting that the characteristic of $(\mathbb{Z}_3)^{2\times 2}$ is 3 while the characteristic of $\mathbb{Z}_9 \oplus \mathbb{Z}_9$ is $\text{lcm}(9, 9) = 9$ (mismatched characteristics so they cannot be isomorphic).

4. (14 points) Workin' in $\mathbb{Z}_{75}$. [Note: $75 = 3 \cdot 5^2$]

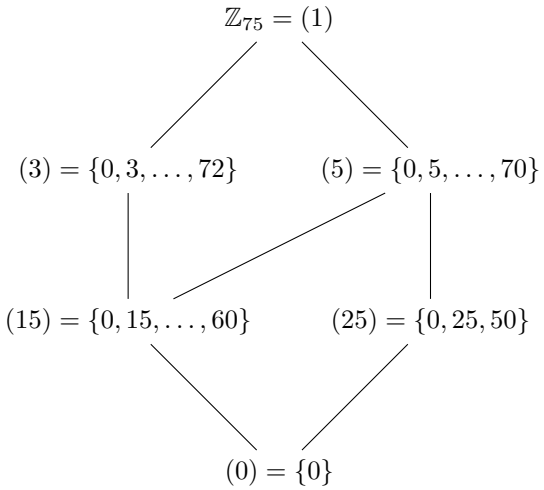
(a) Fill out the following table (for $\mathbb{Z}_{75}$):

order =	1	3	5	15	25	75
number of elements with this order =	1	$3 - 1 = 2$	$5 - 1 = 4$	$15 - 4 - 2 - 1 = 8$	$25 - 4 - 1 = 20$	$75 - 20 - 8 - 4 - 2 - 1 = 40$

(b) Draw $\mathbb{Z}_{75}$'s lattice of subgroups (= ideals).



Divisibility Lattice



Subgroup Lattice

(c) Which ideals are prime? maximal?

Recall that a maximal ideal is a *proper* (i.e. $\neq \mathbb{Z}_{75}$) ideal such that it is not contained in any other proper ideal. This means we need to find the ideals which lie directly below $\mathbb{Z}_{75}$. Looking at the lattice, we see that $\boxed{(3) \text{ and } (5)}$ are the maximal ideals of $\mathbb{Z}_{75}$. Notice that, for example, (15) isn't maximal since $(15) \subsetneq (3) \subsetneq \mathbb{Z}_{75}$.

Next, recall that an ideal (in a commutative ring with 1) is maximal iff the corresponding quotient ring is a field. Likewise, an ideal is prime iff the corresponding quotient ring is an integral domain. Now for *finite* rings every integral domain is a field and vice-versa. Thus in a finite commutative ring with 1, prime = maximal. Therefore, since $\mathbb{Z}_{75}$ is finite, $\boxed{(3) \text{ and } (5)}$ are the prime ideals.

(d) Is 30 zero, a unit, a zero divisor, or none of the above in $\mathbb{Z}_{75}$? If 30 is a zero divisor, prove it. If 30 is a unit, find it's inverse.

In $\mathbb{Z}_n$ every element is either zero, a zero divisor, or a unit. Recall that the units, $U(n)$, of $\mathbb{Z}_n$ are precisely the elements that are relatively prime to n.

Now 30 is not zero in $\mathbb{Z}_{75}$. Also, $\gcd(30, 75) = 15 \neq 1$, so 30 is not a unit. This means 30 must be a zero divisor. To show it's a zero divisor we need to find some non-zero element x such that $30x = 0 \pmod{75}$. Well, 30 and 75 share the common factor of 15, so we just lack the factor 5 to get 30 up to a multiple of 75. So we have that $30 \cdot 5 = 150 = 0 \pmod{75}$. This shows that $\boxed{\text{30 is a zero divisor}}$.

(e) Is 11 zero, a unit, a zero divisor, or none of the above in $\mathbb{Z}_{75}$? If 11 is a zero divisor, prove it. If 11 is a unit, find it's inverse.

Notice that 11 is prime and 75 isn't divisible by 11, so $\gcd(11, 75) = 1$ (i.e. they're relatively prime). This implies that 11 is a unit. Let's use the extended Euclidean algorithm to find its inverse.

Dividing we get: $75 = 11(6) + 9$. Next, $11 = 9(1) + 2$. Next, $9 = 2(4) + 1$. Finally, $2 = 1(2) + 0$. The last non-zero remainder is 1 so that $\gcd(11, 75) = 1$ (which we already knew).

We must now reverse the above steps so that we can express 1 as an integer linear combination of 75 and 11. First, $1 = (-4)2+(1)9$. Next, $2 = (-1)9+(1)11$ plugged into our previous expression yields $1 = (-4)[(-1)9+(1)11]+(1)9$. Thus $1 = (5)9+(-4)11$. Finally, $9 = (-6)11+(1)75$ plugged into our previous expression yields $1 = (5)[(-6)11+(1)75]+(-4)11$. Thus $1 = (-34)11 + (5)75$. Therefore, $-34 \cdot 11 = 1 \pmod{75}$. This means that $\boxed{11^{-1} = -34 = 41 \pmod{75}}$.

5. (12 points) Sub-things

(a) Let G be a group. Show $Z(G) = \{g \in G \mid xg = gx \text{ for all } x \in G\}$ (the center of G) is a subgroup.

Let e be the identity of G. Notice that $eg = g = ge$ for all $g \in G$. Thus $e \in Z(G)$ so that $Z(G)$ is non-empty.

Next, suppose that $a, b \in Z(G)$. Consider $g \in G$, then $(ab)g = a(bg) = a(gb)$ since b is in the center. Now $a(gb) = (ag)b = (ga)b$ since a is in the center. Therefore, $(ab)g = g(ab)$ for all $g \in G$. Thus $ab \in Z(G)$ (we have closure under the operation).

Finally, suppose that $a \in Z(G)$. Consider $g \in G$, then $ag^{-1} = g^{-1}a$ (since a commutes with everything in G, it certainly commutes with g^{-1}). Taking inverses (and using sock-shoes) we get $(g^{-1})^{-1}a^{-1} = (ag^{-1})^{-1} = (g^{-1}a)^{-1} = a^{-1}(g^{-1})^{-1}$. Therefore, $ga^{-1} = a^{-1}g$ for all $g \in G$. Thus $a^{-1} \in Z(G)$ (we have closure under inverses).

Therefore, by the 2-step subgroup test, $Z(G)$ is a subgroup of G.

(b) Let $H = \{(1), (12)\}$. Explain why H is a subgroup of S_3, then show it is **not** a **normal** subgroup of S_3.

Note that $\sigma(1) = (1)\sigma = \sigma$ for any permutation σ. Also, $(12)(12) = (1)$. Therefore, H is a non-empty subset of S_3 which is closed under composition. Thus, by the finite subgroup test, H is a subgroup of S_3. Briefly, why is H a subgroup? $\boxed{\text{Closure.}}$

To show H is *not* a normal subgroup, we can either show that it fails to be closed under conjugation: $(123)(12)(123)^{-1} = (23) \notin H$ or we can compute some left/right cosets of H and show that they don't match: $(13)H = \{(13)(1), (13)(12)\} = \{(13), (123)\}$ whereas the right coset containing (13) is $H(13) = \{(1)(13), (12)(13)\} = \{(13), (132)\}$.

(c) Let $S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}$. Show S is a **subring** of $\mathbb{R}^{2\times 2}$.

Clearly S is a non-empty subset of $R^{2\times 2}$. So to show that it is a subring, we merely need to check closure under subtraction and closure under multiplication.

Let $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, X = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \in S$. Then $A - X = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} - \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} a-x & b-y \\ 0 & c-z \end{bmatrix} \in S$. Also, $AX = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} ax & ay+bz \\ 0 & cz \end{bmatrix} \in S$. Therefore, S is closed under subtraction and multiplication so it is a subring.

Note: S contains the identity and it isn't too hard to find to non-commuting matrices in S. Therefore, S is a non-commutative ring with unity.

6. (10 points) An ideal question.

(a) Let R be a commutative ring with 1 and let $x \in R$. Show that $(x) = \{rx \mid r \in R\}$ is an ideal of R.

First, notice that $x = 1 \cdot x \in (x)$, so (x) is clearly a non-empty subset of R (we could have skipped this step).

To show that (x) is an ideal, we need to prove closure under subtraction and the absorption properties.

Let $a, b \in (x)$. Then there exists $r_1, r_2 \in R$ such that $a = r_1 x$ and $b = r_2 x$ (since elements of (x) are multiples of x). Notice that $a - b = r_1 x - r_2 x = (r_1 - r_2)x \in (x)$.

Now let $a \in (x)$ and $r \in R$. Then there exists $s \in R$ such that $a = sx$. Therefore, $ar = ra = r(sx) = (rs)x \in (x)$ (notice that we used the fact that R is commutative here). This establishes both absorption properties. Therefore, $(x) \triangleleft R$ (i.e. (x) is an ideal).

Here is a very brief proof: "(x) is an ideal since the difference of two multiples of x is itself a multiple of x and any multiple of a multiple of x is itself a multiple of x."

(b) Let R be a commutative ring with 1 and let $x, y \in R$. Show $(x) \subseteq (y)$ if and only if y divides x (i.e. there exist some $z \in R$ such that $yz = x$).

We have two directions to take care of.

Suppose $(x) \subseteq (y)$. Consider $x = 1 \cdot x \in (x)$. Since $(x) \subseteq (y)$, we have that $x \in (y)$. Therefore, there exists some $r \in R$ such that $x = ry$. This means that $y \mid x$.

Conversely, suppose that $y \mid x$. This implies that there is some $r \in R$ such that $ry = x$. Therefore, $x \in (y)$. Now (y) is an ideal, so if $x \in (y)$, then $sx \in (y)$ for all $s \in R$ (i.e. the absorption property). Therefore, all multiples of x belong to (y) (i.e. $(x) \subseteq (y)$).

7. (10 points) The Fundamental Theorem of Finite Abelian Groups.

(a) How many non-isomorphic abelian groups are there of order $2^4 3^2 5^3 7^2$. [Keep in mind that there are **5** non-isomorphic abelian groups of order $2^4 = 16$.]

Recall that $p(n)$ is the number of partitions of n and that there are $p(n)$ non-isomorphic abelian groups of order q^n where q is any prime.

Therefore, there are $p(4) = 5$ non-isomorphic groups of order 2^4 and $p(2) = 2$ non-isomorphic abelian groups of order 3^2 etc. Multiplying the number of possibilities (chosen *independently*) for each prime power yields the total number of non-isomorphic abelian groups of this order: $p(4)p(2)p(3)p(2) = 5 \cdot 2 \cdot 3 \cdot 2 = \boxed{60}$.

(b) List all of the non-isomorphic abelian groups of order $36 = 2^2 3^2$. Circle any that are cyclic.

Using the same thought process as the previous part, we can see that we should be able to find $p(2)p(2) = 2 \cdot 2 = 4$ non-isomorphic abelian groups of order 36. These come from the different ways of combining $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ with $\mathbb{Z}_9$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

- $\boxed{\mathbb{Z}_{36} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$
- $\mathbb{Z}_3 \oplus \mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
- $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

Recall that element orders are computed using lcm's. Thus the first group listed has elements of order 36 (i.e. it's cyclic). However, the largest order appearing in the next group is $\text{lcm}(2, 18) = 18$ and the next is $\text{lcm}(3, 12) = 12$ and the last is $\text{lcm}(6, 6) = 6$.

In any case, since any two cyclic groups of the same order are isomorphic, once we've identified one group that's cyclic, we shouldn't be able to find another – unless we made a mistake! For example, $\text{lcm}(4, 9) = 36$ so $\mathbb{Z}_4 \oplus \mathbb{Z}_9$ is cyclic. If we had this group listed as distinct from $\mathbb{Z}_{36}$, we would've been mistaken!

(c) Which of the abelian groups of order 36 contain elements of order 18?

From our discussion in the previous part we see that only $\boxed{\mathbb{Z}_{36} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9}$ [take $2 \in \mathbb{Z}_{36}$ or $(2, 1) \in \mathbb{Z}_4 \oplus \mathbb{Z}_9$] and $\boxed{\mathbb{Z}_2 \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9}$ [take $(1, 1) \in \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$ or $(1, 1, 1) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$] have elements of order 18 .

8. (12 points) Homomorphisms

(a) Show that $\varphi : \mathbb{Z}_9 \to \mathbb{Z}_6$ defined by $\varphi(x) = 2x$ is a **well-defined** group **homomorphism**.

Well-Defined: Suppose that $[x] = [y] \in \mathbb{Z}_9$. Then there exists $k \in \mathbb{Z}$ such that $x = y + 9k$ so that $2x = 2y + 18k = 2y + 6(3k)$. Therefore, $[2x] = [2y]$ in $\mathbb{Z}_6$. Thus $[x] = [y]$ (in $\mathbb{Z}_9$) implies that $\varphi([x]) = [2x] = [2y] = \varphi([y])$ (in $\mathbb{Z}_6$), so φ is well-defined.

Homomorphism/Operation Preserving: $\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$ [Keep in mind that $\mathbb{Z}_n$ is a group under *addition* not multiplication modulo n].

(b) Find the Kernel and image of φ. Is φ 1-1, onto, both, or neither? Explain.

Just map all 9 elements of $\mathbb{Z}_9$ and keep in mind that outputs should be reduced mod 6: $0 \mapsto 2(0) = 0$, $1 \mapsto 2(1) = 2$, $2 \mapsto 2(2) = 4$, $3 \mapsto 2(3) = 0$, $4 \mapsto 2(4) = 2$, $5 \mapsto 2(5) = 4$, $6 \mapsto 2(6) = 0$, $7 \mapsto 2(7) = 2$, and $8 \mapsto 2(8) = 4$.

From our calculation we see that $\boxed{\text{Ker}(\varphi) = \{x \in \mathbb{Z}_9 \mid \varphi(x) = 0\} = \{0, 3, 6\} = \langle 3 \rangle}$ and $\boxed{\varphi(\mathbb{Z}_9) = \{0, 2, 4\} = \langle 2 \rangle}$ (the image = range = outputs).

So φ is **not one-to-one**, in fact, it's $|\text{Ker}(\varphi)|$-to-1 (i.e. 3-to-1) and φ is **not onto** since $\varphi(\mathbb{Z}_9) \neq \mathbb{Z}_6$.

(c) Although φ a **group** homomorphism, it is **not** a **ring** homomorphism. Explain why φ fails to be a ring homomorphism.

Notice that $2 = \varphi(1) = \varphi(1 \cdot 1) \neq \varphi(1)\varphi(1) = 2 \cdot 2 = 4$, so φ does not preserve multiplication.

(d) It can be shown that $\varphi : \mathbb{Q}[x] \to \mathbb{Q} \oplus \mathbb{Q}$ defined by $\varphi(f(x)) = (f(1), f(-1))$ is an onto (ring) homomorphism. Moreover, it can be shown that $\text{Ker}(\varphi) = (x^2 - 1)$ (the principal ideal generated by $x^2 - 1 = (x + 1)(x - 1)$). What does the first isomorphism theorem tell us here? Is $(x^2 - 1)$ a prime ideal of $\mathbb{Q}[x]$? Why or why not?

The first isomorphism theorem states that $\mathbb{Q}[x]/\text{Ker}(\varphi) \cong \varphi(\mathbb{Q}[x])$ so that $\mathbb{Q}[x]/(x^2 - 1) \cong \mathbb{Q} \oplus \mathbb{Q}$.

Now $(x^2 - 1)$ is a prime ideal of $\mathbb{Q}[x]$ iff $\mathbb{Q}[x]/(x^2 - 1)$ is an integral domain. However, $\mathbb{Q}[x]/(x^2 - 1) \cong \mathbb{Q} \oplus \mathbb{Q}$ is not an integral domain (it has zero divisors: $(1, 0)(0, 1) = (0, 0)$). Therefore, $(x^2 - 1)$ is **not a prime ideal**.

It turns out that $(f(x))$ is prime (and in fact maximal) in $\mathbb{Q}[x]$ iff $f(x)$ is an irreducible polynomial. Accepting this fact, we can see that $(x^2 - 1)$ isn't prime since $x^2 - 1 = (x - 1)(x + 1)$ factors in $\mathbb{Q}[x]$.

9. (14 points) Various Stuff

(a) Let R be a commutative ring and I an ideal of R. Prove that R/I is commutative.

Let $x+I, y+I \in R/I$. Then $(x+I)(y+I) = xy+I = yx+I = (y+I)(x+I)$ where $xy = yx$ since R is commutative. Therefore, R/I is commutative.

(b) Although quotients of commutative rings are commutative and quotients of rings with 1 are rings with 1. It is not the case that quotients of integral domain are integral domains. Give an example which illustrates this fact.

Example: $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$ is not (it has zero divisors: $(2+6\mathbb{Z})(3+6\mathbb{Z}) = 6+6\mathbb{Z} = 0+6\mathbb{Z}$).

Alternatively, we could use our example from 8(d): $\mathbb{Q}[x]$ is an integral domain, but $\mathbb{Q}[x]/(x^2-1)$ is not.

(c) H is a subgroup of K which is a subgroup of G. Suppose that $H \neq K$ and $K \neq G$. In addition assume $|H| = 6$ and $|G| = 24$. What can be said about the order of K?

By Lagrange's theorem (i.e. the order of a subgroup must divide the order of its group), $|K|$ divides $|G| = 24$ and $|H| = 6$ divides $|K|$. So $|K|$ must be a multiple of 6: 6, 12, 18, etc. but also a divisor of 24. This just leaves: 6, 12, and 24 as possibilities. Now $H \neq K$ so $|K| \neq 6$ (otherwise, $H \subseteq K$ and $|H| = |K| = 6$ imply that $H = K$) and likewise $K \neq G$ implies $|K| \neq 24$. Therefore, $\boxed{|K| = 12}$.

(d) Let R be an integral domain and S a subring of R which contains the multiplicative identity of R. Show S must be an integral domain (i.e. a sub-domain of R).

R is an integral domain so $1 \neq 0$. Next, any subring of a commutative ring is itself a commutative ring: $a, b \in S$ implies that $a, b \in R$ so that $ab = ba$ since R is a commutative ring (because it's an integral domain). Therefore, we have established that S is a commutative ring with $1 \neq 0$.

Now suppose that $a, b \in S$ and that $ab = 0$. Then because $S \subseteq R$, we have $a, b \in R$ and $ab = 0$. But R is an integral domain, so it has no zero divisors. Thus either $a = 0$ or $b = 0$. Thus S is has no zero divisors. [Briefly, a zero divisor in S yields a zero divisor in R (which is impossible) so S has no zero divisors.]

Therefore, S is a commutative ring with $1 \neq 0$ and has no zero divisors. It's an integral domain.

(e) Part (d) says that subrings (containing 1) of integral domains are themselves integral domains. The analogous statement does *not* hold for fields. Give an example of a subring (containing 1) of a field which is itself *not* a field.

Example: $\mathbb{Z}$ is a subring of $\mathbb{R}$. $\mathbb{R}$ is a field, but $\mathbb{Z}$ is not a field (it is, however, an integral domain).