NAME: SOLUTIONS

1. (3 points each) Give examples of the following, if they exist. Otherwise briefly explain why such examples do not exist.

   (There are many answers here.)

   (a) A subring S of a ring R such that S is not an ideal of R

   Let $R = \mathbb{R}[x]$ and let $A = \mathbb{R}$. We know A is itself a ring and since it is contained in R it is certainly a subring. It is not closed under multiplication from outside. That is $x \cdot 2 \notin A$.

   (b) A group G, subgroup H of G and an element $a \in G$ such that $aH \neq Ha$.

   Let $G = S_3$ and $H = \{(), (12)\}$. Pick $a = (23)$. Then $aH = \{(23), (13)\}$ but $Ha = \{(12), (231)\}$.

   (c) A ring R in which the group of units of R is a proper subset of the non-zero elements of R

   Pick $R = \mathbb{Z}$. The units of R are $\{-1, 1\}$ which is certainly a proper subset of the nonzero elements of R.

   (d) An infinite ring with zero divisors. (State the ring R and an example of a zero divisor.)

   Pick $R = \mathbb{Z} \oplus \mathbb{Z}$ which is certainly infinite. The element $(2, 0)$ is a zero divisor. (Multiply it by $(0, 5)$.)

   (e) A ring R with ideal A such that A is prime but not maximal

   The ring $R = \mathbb{Z}[x]$ and the ideal $A = \langle x \rangle$.

2. (10 points) List all abelian groups of order $225 = 9 \cdot 25$ up to isomorphism. Do not write any isomorphism class more than once. For each distinct group, determine the number of elements of order 3. (Note, a bald answer is acceptable here.)

		# elements of order 3
$\mathbb{Z}_9 \oplus \mathbb{Z}_{25}$	$\mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$	2 (in $\mathbb{Z}_9$, elements 3 and 6)
$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$	2+2+4=8 in $\mathbb{Z}_3 \oplus \mathbb{Z}_3$: $(1,0), (2,0), (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)$

3. (10 points) Let a be an element in the ring R. Let $S = \{r \in R \mid ar = 0\}$. Is S a subring of R? Prove your answer is correct.

Answer: S is a subring.
Proof: I will proceed by the Subring Test.
Since $a \cdot 0 = 0$, we know $0 \in S$. Thus S is nonempty and the Subring Test applies.
Let $r, s \in S$. Now $a(r - s) = ar - as = 0 - 0 = 0$. Thus, $r - s \in S$.
Let $r, s \in S$. Now, $a(rs) = (ar)s = 0 \cdot s = 0$. Thus, $rs \in S$.
Thus, by the Subring Test, S is a subring of R.

4. (15 points)

(a) State Lagrange's Theorem

Let H be a subgroup of the finite group G. Then $|H|||G|$. Moreover, $|G : H| = |G|/|H|$.

(b) Use Lagrange's Theorem to prove that the order of each element of a finite group must divide the order of the group.

Let $a \in G$ where G is a finite group. Then $\langle a \rangle \leq G$ and $|a| = |\langle a \rangle|$. Now Lagrange's Theorem implies that $|a| = |\langle a \rangle| \mid |G|$.

(c) Prove that every group of order 63 must have an element of order 3.

Let G be a group of order 63. Since $63 = 3^2 \cdot 7$, we know from part (b) above that every $a \in G$, $|a| \in \{1, 3, 7, 9, 21, 63\}$. We know that in any finite group, the number of elements of order 7 must be a multiple of $\phi(7) = 6$ and 6 does not divide 62. Thus, we know G must contain at least one nonidentity element whose order in in the set $\{3, 9, 21, 63\}$.
If $|a| = 3$, the statement follows.
If $|a| = 9$, then $|a^3| = 3$.
If $|a| = 21$, then $|a^7| = 3$.
If $|a| = 63$, then $|a^{21}| = 3$.
Thus, in all cases, G contains an element of order 3.

5. (20 points)

(a) Recall that D_6 is the group of symmetries of a regular hexagon and the center of D_6 is $Z(D_6) = \{R_0,\ R_{180}\}$. What is the order of the element $R_{60}\, Z(D_6)$ in the factor group $D_6/Z(D_6)$?

Since R_{60} and $R_{60}R_{60} = R_{120} \notin Z(D_6)$, but $R_{60}R_{60}R_{60} = R_{180} \in Z(D_6)$, we conclude that the order of $R_{60}\, Z(D_6)$ in the factor group $D_6/Z(D_6)$ is 3.

(b) Let $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and let $K = \langle (1, 2) \rangle$.

i. List the elements of K.

$K = \{(1,2),\ (2,0),\ (3,2),\ (0,0)\}$

ii. List the elements of G/K.

$G/K = \{K,\ (1,0)+K,\ (1,1)+K, (0,1)+K\}$.

iii. Is G/K isomorphic to any of the following groups?
D_4(the symmetries of a square), $\mathbb{Z}_6$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_2$
Explain your answer.

Observe that the order of element $(1,1)+K$ is 4. Thus, G/K is isomorphic to $\mathbb{Z}_4$.

6. (15 points) Define the mapping $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ as $\phi(a,b) = a - b$.

(a) Prove that ϕ is a group homomorphism.

We need to show that ϕ is operation preserving. Let $(a,b),\ (c,d) \in \mathbb{Z} \oplus \mathbb{Z}$. Then,

$\phi((a,b)+(c,d)) = \phi(a+c, b+d) = (a+c)-(b+d) = (a-b)+(c-d) = \phi(a,b)+\phi(c,d)$.

(b) Find the kernel of ϕ.

We need to find all ordered pairs (a,b) such that $\phi(a,b) = a-b = 0$. Thus, $\ker\phi = \{(a,a) \mid a \in \mathbb{Z}\}$.

(c) Find $\phi^{-1}(3)$.

Since $\phi(3,0) = 3$, we know $\phi^{-1}(3) = (3,0) + \ker\ \phi = \{(3+a, a) \mid a \in \mathbb{Z}\}$.

7. (15 points)

(a) State the definition of a field F.

A field is a commutative ring with unity such that every nonzero element has a multiplicative inverse.

(b) Prove that if F is a nontrivial field, then F has exactly two ideals.

Assume F is a nontrivial field. Let A be an ideal of F such that A contains at least one nonzero element. (That is, A is not the zero ideal.) Let $r \in A - \{0\}$. Since F is a field, $r^{-1} \in F$. Since A is an ideal, $r^{-1}r \in A$. Thus, $1 \in A$. Now for every $s \in R$, $s \cdot 1 \in A$. Thus, $A = R$. Thus, we have shown that any ideal that is not the zero ideal must be the whole field.

(c) Prove that if R is a commutative ring with unity such that the only ideals of R are $\{0\}$ and R, then R must be a field.

If the only ideals of R are R and $\{0\}$, then $\{0\}$ is a maximal ideal. Since R is commutative with 1 and $\{0\}$ is maximal, the factor ring $R/\{0\}$ is a field. But $R/\{0\} = R$. Thus, R is a field.

One can also prove it directly without much trouble. That is, we need to show that every nonzero element of R is a unit. Let $a \in R - \{0\}$ and consider the ideal generated by a, $\langle a \rangle = \{ra \mid r \in R\}$. Since by assumption $\langle a \rangle = R$, we know there exists some $r \in R$ such that $ra = 1$. Thus, $r = a^{-1}$.