NAME: Solutions

Instructions: Answer questions in the space provided. You will be graded both on correctness and presentation. Note that some problems may ask you to prove theorems stated in your text. Such questions require you to construct a proof, not reference the statement of the Theorem. This test has 7 questions worth a total of 100 points.

1. (10 points) List up to isomorphism all abelian groups of order $392 = 2^3 \cdot 7^2$. Do not list any group more than once. An answer without explanation is sufficient here.

$\mathbb{Z}_8 \oplus \mathbb{Z}_{49}$ $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{49}$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{49}$

$\mathbb{Z}_8 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$

2. (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) cyclic groups G_1 and G_2 such that $G_1 \oplus G_2$ is not cyclic

Pick $G_1 = G_2 = \mathbb{Z}_2$.

(b) an infinite nonabelian group

$GL_2(\mathbb{R})$

(c) a nontrivial normal subgroup of a nonabelian group

A_n is normal in S_n, a nonabelian group

(d) an infinite group such that every element of the group has finite order

$\mathbb{Z}_3[x]$

(e) a ring that is not an integral domain

$\mathbb{Z}_{12}$

(f) an integral domain that is not a field

$\mathbb{Z}$

(g) a finite field

$\mathbb{Z}_7$

(h) a prime ideal I in ring R that is not maximal

$\langle x \rangle$ in $\mathbb{Z}[x]$.

(This one's for Parker: $\{0\}$ in $\mathbb{Z}$.)

3. (16 points)

(a) Write the permutation $\alpha = (14256)(24)(36512)$ as a product of disjoint cycles.

$\alpha = (123)(45)(6)$

(b) Determine whether α is even or odd.

$\alpha = (13)(12)(45)$. So α is odd.

(c) Determine $|\alpha|$.

Since the order of (123) is 3 and the order of (45) is 2, the order of $(123)(45)$ is 6.

(d) Let $H = \{\alpha \in S_n \mid \alpha(1) = 1\}$. (That is, H consists of the subset of permutations of S_n that fix the element 1. For example the permutation $(234)(12)(21)$ fixes 1 but the permutation (123) does not.)
Prove that H is a subgroup of S_n.

Proof: I will apply the 1-step subgroup test. The permutation $()$ fixes 1. Thus H is nonempty. Let a and b be elements of H. Observe that if $b(1) = 1$, then by the definition of an inverse function, $b^{-1}(1) = 1$. Thus, $b^{-1} \in H$. Now $ab^{-1}(1) = 1$. Thus, $ab^{-1} \in H$. So the 1-step subgroup test implies that H is indeed a subgroup.

4. (10 points) Let G be a group such that $|G : Z(G)| = 4$. Prove that $G/Z(G) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

proof: Since $|G : Z(G)| = 4$, we know $|G/Z(G)| = 4$. Further, we know that if $G/Z(G)$ is cyclic, then it is abelian. If $G/Z(G)$ is abelian, Theorem 9.3 implies G is abelian, forcing $G = Z(G)$, a contradiction. So $G/Z(G)$ is not cyclic.

Theorem 9.7 says that every group of order p^2 where p is a prime is either isomorphic $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Since our group as order 2^2 and we know it cannot be isomorphic to the cyclic group $\mathbb{Z}_4$, by process of elimination it must be isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

NOTE: First, it is possible to prove this result directly without depending on the Theorems I quoted above. It isn't that hard because the group is small, it just takes longer. Second, one does not have to quote the Theorem numbers. It is sufficient to correctly state the result. I supplied the Theorem numbers so that the student can easily find the result.

5. (16 points) Let R be a ring with a unity, 1, and let $\phi : R \to S$ be a ring homomorphism from R onto the nontrivial ring S.

   (a) Prove that $\phi(1)$ must be the unity of S.

   Proof: First I want to show that $\phi(1) \neq 0_S$ by contradiction. If $\phi(1) = 0$, then for every $a \in R$,
   $$\phi(a) = \phi(1 \cdot a) = \phi(1) \cdot \phi(a) = 0 \cdot \phi(a) = 0.$$
   This means that $\phi(R) = \{0_S\}$. Since S is nontrivial and ϕ is onto, $\phi(R) \neq \{0_S\}$, a contradiction. Thus, $\phi(1) \neq 0$.

   Let $s \in S$. Since ϕ is onto, there exists an $r \in R$ such that $\phi(r) = s$. (Just FYI, do you understand why I cannot say $\phi^{-1}(s) = r$?) Using the fact that ϕ is operation preserving, we know
   $$s = \phi(r) = \phi(r \cdot 1) = \phi(r) \cdot \phi(1) = s \cdot \phi(1).$$
   Since s is arbitrary and since the argument above can be duplicated with multiplication on the left, we have shown that $\phi(1)$ must act like 1_S.

   (b) Show that part (a) above does not hold if ϕ is not onto.

   The easiest example: $\phi(R) = \{0_S\}$.

   A nontrivial example: $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ defined by $\phi(x) = 5x$.

6. (12 points) In both parts of the problem below, $\mathbb{Z}_n$ is a ring.

   (a) Let $a \in \mathbb{Z}_n$, a ring, such that $a^2 = a$. Prove that the function $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ defined as $\phi(z) = az$ is a ring homomorphism.

   We will check that the function as defined is operation preserving.

   Let $x, y \in \mathbb{Z}_n$. Then

   $$\begin{aligned} \phi(x+y) &= a(x+y) && \text{definition of } \phi \\ &= ax + ay && \text{by distribution properties of rings} \\ &= \phi(x) + \phi(y) && \text{by definition of } \phi. \end{aligned}$$

Also,

$$\begin{aligned}
\phi(xy) &= a(xy) && \text{definition of } \phi \\
&= a^2(xy) && \text{definition of } a \\
&= axay && \text{because } \mathbb{Z}_n \text{ is abelian} \\
&= (ax)(ay) && \text{by associative properties of rings} \\
&= \phi(x)\phi(y) && \text{by definition of } \phi.
\end{aligned}$$

(b) Prove that every ring homomorphism ϕ from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ has the form $\phi(z) = az$ where $a^2 = a$.

Let $a \in \mathbb{Z}_n$ such that $\phi(1) = a$. Since ϕ is a ring homomorphism, then it must be operation preserving. Thus, $a = \phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1) = a^2$.

7. (12 points)

(a) 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.

(b) Prove that if R is a commutative ring with unity such that the only ideals in R are $\{0\}$ and R, then R is 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, $r = a^{-1}$.