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 6 questions worth a total of 100 points.

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

   (a) a nonabelian group G and nontrivial subgroup H of G such that $H \triangleleft G$

   $G = S_n$, $H = A_n$

   (b) a nonabelian group of order 7

   not possible. All groups of order 7 are cyclic and therefore abelian.

   (c) a group G whose only subgroups are G and $\{e\}$

   $\mathbb{Z}_p$, where p is prime

   (d) three nonisomorphic groups of order 44

   $\mathbb{Z}_{44}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{22}$, and D_{44}, the dihedral group with 44 elements (or the symmetries of an 22-gon)

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

   $R = \mathbb{Z}[x]$, $S = \mathbb{Z}$

   (f) a *nontrivial* ring homomorphism from the ring $2\mathbb{Z}$ to $3\mathbb{Z}$

   not possible. Such a map ϕ would have to send 2 to some element of the form $3z$ where $z \in \mathbb{Z}$. In order to be operation preserving, $6z = \phi(2) + \phi(2) = \phi(2+2) = \phi(4) = \phi(2 \cdot 2) = \phi(2)\phi(2) = 9z^2$, which has no nonzero solutions in the integers.

   (g) a maximal ideal in $\mathbb{Q}[x]$

   $\langle x \rangle$

(h) an infinite ring R such that $\text{char}(R) = 15$

$R = Z_{15}[x]$

2. (15 points total) Fill in the following FOUR blanks with the correct statement.

(a) Suppose $A = \langle x \rangle$ is a finite cyclic group of finite order n such that $d \mid n$ (where d is a positive integer.
Then A has exactly __ONE__ subgroup(s) of order d and exactly __$\phi(d)$__ element(s) of order d.

(b) Let $\sigma = (123)(234)(345) \in S_5$.

i. The order of σ is __TWO__.

(It's disjoint cycle representation is: (12)(45)

ii. The element σ (is/is not) __IS__ an element in A_5.

(c) The order of the element $15 + \langle 6 \rangle$ in the factor group $\mathbb{Z}_{24}/\langle 6 \rangle$ is __TWO__.

Observe that $15 + 15 = 30 \equiv 6 \mod 24$ and $\langle 6 \rangle = \{0, 6, 12, 18\}$.

3. (16 points) Note that here $\mathbb{Z}_n$ will denote a group under the operation of addition modulo n.

(a) Determine all group homomorphisms from $\mathbb{Z}_{20}$ **onto** $\mathbb{Z}_{10}$. Explain your answer. (Note: the "onto" really does mean *surjective*.)

(answer:) There are $\phi(10) = |\{1, 3, 7, 9\}| = 4$ distinct homomorphisms from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_{10}$. Specifically, they are $\phi(x) = kx$ for $k \in \{1, 3, 7, 9\}$.

(rationale:) Since $\mathbb{Z}_{20}$ is cyclic, any homomorphism is determined by where it sends 1. Because the homomorphism is supposed to be onto, we must send 1 to a generator of $\mathbb{Z}_{10}$. Thus the set $\{1, 3, 7, 9\}$ is a complete list of possible images of 1 under a surjective homomorphism.

(b) Determine all group homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{14}$. Explain your answer. (Note: these homomorphism are not required to be one-to-one or onto.)

(answer:) There are two homomorphisms: $1 \to 0$ or $1 \to 7$.

(rationale:) As above, we know it is sufficient to determine the possible images of element 1 in $\mathbb{Z}_{20}$. Let $a = \phi(1)$, the image of 1 under a group homomorphism. We know that in $\mathbb{Z}_{20}$ element 1 has order 20. Therefore, we know that the image of 1, namely a,

must have an order that divides 20 and 14. But $\gcd(20, 14) = 2$. As $\mathbb{Z}_{14}$ is cyclic, we know there exists exactly two elements with order dividing 20, 0 and 7.

4. (15 points)

   (a) State the definition of an ideal I in ring R.

   The subset I of ring R is an ideal if I is a subring such that for all $r \in R$ and for all $x \in I$, rx and xr are elements of I.

   (b) Prove that if A and B are ideals in the ring R, then the *sum* of A and B,

   $$A + B = \{a + b \mid a \in A,\ b \in B\},$$

   is also an ideal in R.

   Proof: We will use the Ideal Test and show that I is nonempty, closed under subtraction, and closed under multiplication from elements of R.

   (nonempty:) Since $0 \in A \cap B$, $0 = 0 + 0 \in A + B$.

   (closed under subtraction:) Let $a + b$ and $a' + b'$ be elements in $A + B$ where $a, a' \in A$ and $b, b' \in B$. Observe that

   $$(a + b) - (a' + b') = (a - a') + (b - b') \in A + B,$$

   since A and B are rings implying $a - a' \in A$ and $b - b' \in B$.

   (closed under multiplication from R) Let $a + b \in A + B$ and $r \in R$. Observe that since A and B are ideals, ar, $ra \in A$ and br, $rb \in B$. Hence,

   $$r(a + b) = ra + rb \in A + B \quad \text{and} \quad (a + b)r = ar + br \in A + B.$$

   Thus, we have shown that if A and B are ideals, then $A + B$ is an ideal.

5. (15 points)

   (a) Define *prime ideal.*

   The set I is a prime ideal of a commutative ring R if I is a proper ideal such that for every $a, b \in R$ such that $ab \in I$, either $a \in I$ or $b \in I$.

   (b) Prove that if R is an commutative ring with unity and A is a prime ideal of R, then R/A is an integral domain.

   proof: We need to show that the factor ring R/A is commutative, with unity, and has no zero divisors.

(commutativity:) Let $x+A$, $y+A \in R/A$. Recall that since R is commutative, $xy = yx$. Thus $(x + A)(y + A) = xy + A = yx + A = (y + A)(x + A)$.

(unity:) Recall that R has unity, 1. Let $x + A \in R/A$. Thus, we knoe $1 \cdot x = x \cdot 1$. Then $(1 + A)(x + A) = 1 \cdot x + A = x + A = x \cdot 1 + A = (x + A)(1 + A)$.

(no zero divisors:) Proceed by contradiction and assume there exists $x+A$, $y+A \in R/A$ such that neither are the additive identity (ie $0_{R/A}$ or A) but $(x+A)(y+A) = xy+A = A$. Then $xy \in A$. But A is prime and thus by definition of prime either $x \in A$ or $y \in A$. But this would imply $x + A = A$ or $y + A = A$, a contradiction. Thus R/A had no zero divisors.

Thus, we have shown that R/A is an integral domain.

6. (15 points) Let $\phi : R \to S$ be a ring homomorphism such that the image of ϕ is not $\{0_S\}$. (Another way to say it is that ϕ is NOT the trivial ring homomorphism that sends all elements to 0_S.)

   (a) If R has unity and S is an integral domain, show that ϕ carries the unity of R to the unity of S.

   Proof: Let $\phi(1) = a$. Then $a = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = a^2$. Using $a = a^2$, we know $0 = a^2 - a = a(a - 1)$. But S is an integral domain. Thus either $a = 0$ or $a - 1 = 0$. If $a = 0$, then ϕ is the trivial homomorphism which is impossible. Thus $a - 1 = 0$. Thus $a = 1$, which is what we wanted to show.

   (b) Give an example to show that the statement in part (a) need not be true if S is not an integral domain.

   Pick $R = S = \mathbb{Z}_4$. Let $\phi(x) = 2x$. (Or alternately, $0 \to 0$, $1 \to 2$, $2 \to 0$, $3 \to 2$.)