MATH 403 MIDTERM ANSWERS WINTER 2007

COMMON ERRORS

(1) A subset S of a ring R is a subring provided that $x \pm y$ and xy belong to S whenever x and y do. A lot of people only said that $x + y$ and xy must belong to S. But we want S to be a ring itself so $(S, +)$ has to be an abelian group; in particular, S must have additive inverses, meaning that $-y \in S$ whenever $y \in S$, and an additive identity, zero. For example, the integers ≥ 0 do not form a subring of $\mathbb{Z}$. I didn't think it was sufficient to say that a subset is a subring if it is a ring, though that is correct. Rather I was wanting you to spell out the details.

(2) In the definition of a homomorphism $f : R \to S$ you need to say that $f(x \pm y) = f(x) \pm f(y)$ and $f(xy) = f(x)f(y)$. It is NOT enough to say that $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ because my suspicion is that most of you do not actually know whether those two alternatives are equivalent or not. Why not try proving it just to see whether you can or not.

(3) If I and J are ideals, then IJ consists of all sums $a_1b_1 + \cdots + a_nb_n$ where the a_is are in I and the b_is are in J. Many people said that IJ consists of all products ab where $a \in I$ and $b \in J$; but that set is not generally closed under addition so IJ would not be an ideal. We want it to be an ideal and for that it needs to contain the sum of any two (or three, or four, or ...) elements that belong to it. In the special case when either I or J is a principal ideal IJ is equal to the set of all products ab with $a \in I$ and $b \in J$.

(4) If R is a subring of S and $a \in S$, then $R[a]$ is NOT usually equal to $\{x + ya \mid x, y \in R\}$. The definition is that $R[a]$ is the smallest subring of S containing R and a. *Sometimes* $R[a]$ is equal to $\{x + ya \mid x, y \in R\}$. But in general

$$R[a] = \{r_0 + r_1a + r_2a^2 + \cdots + r_na^n \mid r_0, \ldots, r_n \in R,\ n \geq 0\}.$$

For example, if $S = \mathbb{C}$ and $R = \mathbb{Z}$ and $a = \sqrt[3]{2}$, then

$$\mathbb{Z}[a] = \{r + sa + ta^2 \mid r, s, t \in \mathbb{Z}\}.$$

We want $R[a]$ to be a ring that contains a so it must also contain a^2. Think about why we do not need to specify an a^3 or a^4 or ... term when describing $\mathbb{Z}[\sqrt[3]{2}$.

(5) When I asked for the definition of a field I did not want you to say "commutative division ring" because that doesn't give me any information unless I know what "division ring" means. Spell out the details: every on-zero element has an inverse.

(6) When defining what it means for an ideal I to be maximal it is not sufficient to only say that the only ideals containing I are R and I itself; R satisfies those two conditions but is not counted as a maximal ideal. You need to also say $I \neq R$.

(7) Let's suppose R is commutative. The notation (a) denotes aR which is the smallest ideal containing a and consists of the elements ar as r ranges over R. Likewise, (a, b) denotes the smallest ideal that contains both a and b. It is $\{ax+by \mid x, y \in R\}$. You can also write this as $aR + bR$. In the same vein, $(a, b, c) = \{ax + by + cz \mid x, y, z \in R\}$.

(8) I wanted an informative answer as to when the image of an integer a in $\mathbb{Z}/n\mathbb{Z}$ has an inverse. I did not want you to simply rewrite the question and say when there is a b such that $[a][b] = 1$. I wanted you to say it happens when $(a, n) = 1$, i.e., when the gcd of a and n is 1.

(9) In a commutative ring the principal ideal (a) is $\{ax \mid x \in R\}$. This is also denoted by aR. It is equal to $Ra = \{xa \mid x \in R\}$. If R is *not* commutative the set aR is only a right ideal; it might not be closed under left multiplication by elements of R. It is also not generally true that $aR \cup Ra$ is an ideal, or even a left ideal, or even a right ideal, because it need not be closed under $+$ for example. Why should $xa + ay$ belong to $Ra \cup aR$ when R is not commutative? In a non-commutative ring (a) denotes the smallest (two-sided!) ideal that contains a. It consists of all sums $x_1ay_1 + x_2ay_2 + \cdots + x_nay_n$ where the x_is and y_is are arbitrary elements in R. It is sometimes denoted by RaR. Just look at the ring $R = M_2(\mathbb{R})$ in order to understand what is going on, and take a to be any non-zero, non-invertible matrix. Another interesting example is provided by the ring $R = \mathbb{R}[x, d/dx]$ of differential operators with polynomial coefficients where multiplication is composition of operators. So elements in R are operators like

$$p_n(x)\frac{d^n}{dx^n} + \cdots + p_1(x)\frac{d}{dx} + p_0(x)$$

where the $p_i(x)$s are polynomials. You can think of R as a certain subset of the ring of all linear operators on the infinite dimensional vector space $\mathbb{R}[x]$ consisting of all polynomials with real coefficients. This ring R has lots of left ideals and lots of right ideals but its only two-sided ideals are 0 and R. For example, any ideal that contains x would also have to contain

$$\frac{d}{dx} \circ x - x \circ \frac{d}{dx}$$

which is, by the product rule for differentiation, the identity; thus $(x) = R$ even though neither xR nor yR contains the identity.

(10) When I asked you to define injective and surjective maps I was not wanting you to give a synonym for these words like *1-to-1* and *onto*. I wanted you to give *real* definitions. You should practice writing down succinct, grammatically correct definitions. The ring

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_2 \right\} \subset M_2(\mathbb{Z}_2)$$

seemed to be a bit mysterious for most of you. It has 4 elements, namely

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad 1 + x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

It is commutative. If $r \in R$, then $r + r = 0$. Also $x^2 = 0$. Knowing this, figure out reasons why it is not isomorphic to $\mathbb{F}_4$ or $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(11) In this course all rings are required to have a multiplicative identity, denoted 1. When talking about a ring we *never* use the word "identity" to refer to the additive identity 0.

ANSWERS

PART 1.

Complete the following definitions:

(1) A subset S of a ring R is a subring if ....**it is a subgroup under** $+$ **and** $xy \in S$ **whenever** x **and** y **are in** S

(2) A commutative ring R is a field if ...**every non-zero element in it has an inverse**

(3) A ring R is a domain if ....$xy \neq 0$ **if** $x \neq 0$ **and** $y \neq 0$

(4) A map $f : R \to S$ between rings R and S is a homomorphism if ... **it is a group homomorphism for** $+$ **and** $f(xy) = f(x)f(y)$ **for all** $x, y \in R$**.**

(5) A subset I of a ring R is an ideal if ...**it is an additive subgroup and** ax **and** xa **are in** I **whenever** $a \in I$ **and** $x \in R$**.**

(6) If I is an ideal in a ring R, then the elements in the quotient R/I are ...**the cosets** $x + I := \{x + a \mid a \in I\}$ **as** x **ranges over all of** R**.**

(7) The principal ideal generated by an element $a \in R$ is $\{\cdots\}$ ... $\{ax \mid x \in R\}$.

(8) An ideal I in a ring R is maximal if ...$I \neq R$ **and the only ideals containing it are** R **and** I**.**

(9) If R is a subring of S and $a \in S$, then $R[a] = \{\cdots\}$ ... **the smallest subring of** S **that contains** a **and** R

(10) If I and J are ideals in a ring R, then $I + J = \{\cdots\}$....$\{x + y \mid x \in I$ and$y \in J\}$.

(11) If I and J are ideals in a ring R, then $IJ = \{\cdots\}$....**the set of all elements of the form** $\sum_{i=1}^{n} a_i b_i$ **where** $a_i \in I$ **and** $b_i \in J$ **and** n **is arbitrary.**

(12) Let a, b, c be elements in a ring R. Then $(a, b, c) = \{\cdots\}$....$\{ax + by + cz \mid x, y, z \in R\}$.

(13) The Cartesian product $R \times S$ of two rings R and S consists of all ordered pairs (x, y) where $x \in R$ and $y \in S$ and is made into a ring by defining ... $(x, y) + (x', y') := (x + x', y + y')$ **and** $(x, y).(x', y') := (xx', yy')$**.**

(14) A function $f : X \to Y$ between two sets

(a) is injective if ....$f(x) = f(x')$ **can only happen when** $x = x'$**.**

(b) is surjective if ....**every element of** Y **is equal to** $f(x)$ **for some** $x \in X$**.**

(c) is bijective if ....**it is injective and surjective.**

(15) Define a ring. **A ring $(R, +, \times)$ is an abelian group $(R, +)$ endowed with a multiplication $\times : R \times R \to R$ such that**

- $(xy)z = x(yz)$ **for all** $x, y, z \in R$**;**
- $(x + y)z = xz + yz$ **and** $x(y + z) = xy + xz$ **for all** $x, y, z \in R$
- **there is an element** $1 \in R$**, called the** identity **with the property that** $1.x = x.1 = x$ **for all** $x \in R$**.**

Part 2.

Complete the following sentences:

(1) R/I is a field if and only if the ideal I is ....**maximal.**
(2) The subset of $\mathbb{Z}$ consisting of all integers that leave a remainder of 17 when divided by 26 is an element of the ring ... $\mathbb{Z}/26\mathbb{Z}$.
(3) If x and y are elements in a ring R and I an ideal of R, then the sets $x + I$ and $y + I$ are elements of the ring .... and they are equal if and only if ... R/I **and they are equal if and only if** $x - y \in I$**.**
(4) In the previous question $x + I = \{\cdots\}$.... $\{x + a \mid a \in I\}$.
(5) If I is an ideal in a ring R there is a bijection between the ideals in R/I and the ideals in ....R **that contain** I**.**
(6) $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if ...n **is prime.**
(7) The element $a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ is a unit if and only if ...a **and** n **are relatively prime, i..e, their greatest common divisor is 1.**
(8) If x, y, z belong to a domain and $xy = xz$, then .... **either** $x = 0$ **or** $y = z$.
(9) Up to isomorphism, there are four rings with 4 elements, namely $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, the field with four elements which we denote by $\mathbb{F}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, and the subring

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_2 \right\}$$

of the ring $M_2(\mathbb{Z}_2)$.
   (a) $\mathbb{Z}_4$ is not isomorphic to $\mathbb{F}_4$ because ...$\mathbb{Z}_4$ **is not a domain because** $2 \times 2 = 0$**.**
   (b) $\mathbb{F}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ because .... $\mathbb{Z}_2 \times \mathbb{Z}_2$ **is not a domain because** $(1, 0)..(0, 1) = 0$**.**
   (c) $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ because ...**in** $\mathbb{Z}_4$ **there is a non-zero element** x **in** $\mathbb{Z}_4$ **such that** $x^2 = 0$**, namely 2, but** $\mathbb{Z}_2 \times \mathbb{Z}_2$ **does not have such an element.** <u>OR</u> $\mathbb{Z}_4$ **is a cyclic group but** $\mathbb{Z}_2 \times \mathbb{Z}_2$ **is not.** <u>OR</u> $\mathbb{Z}_4$ **has only one non-zero ideal but** $\mathbb{Z}_2 \times \mathbb{Z}_2$ **has two non-zero ideals.**
   (d) R is not isomorphic to $\mathbb{Z}_4$ because ...$1 + 1 = 0$ **in** R **but** $1 + 1 \neq 0$ **in** R
   (e) R is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ because ...**there is a non-zero element** x **in** R **such that** $x^2 = 0$ **but** $\mathbb{Z}_2 \times \mathbb{Z}_2$ **does not have such an element.**

Part 3.

(1) Let $W = \{1,2,3,4,5,6\}$, $X = \{1,2,3\}$, $Y = \{1,2\}$, and $Z = X \times Y$. Give an example of
   (a) an injective function between two of these sets;
   e.g., $f : Y \to X$, $f(1) = 1$ and $f(2) = 2$
   (b) a surjective function between two of these sets;
   e.g., $f : X \to Y$, $f(1) = 1$ and $f(2) = 2$ and $f(3) = 1$.
   (c) a bijective function between two of these sets.
   $f : X \times Y \to Z$, there are lots of choices.
(2) List all the ideals in the ring of integers. **The same the subgroups, namely the principal ideals $n\mathbb{Z}$ for $n \geq 0$.**
(3) State the First Isomorphism Theorem for rings.
   If $f : R \to S$ is a ring homomorphism, then $f(R) \cong \frac{R}{\ker f}$.
(4) Let R be any ring. There is a unique homomorphism $f : \mathbb{Z} \to R$. How is it defined?
   It is completely determined by the requirement that $f(1) = 1_R$. Hence if n is a positive integer, then $f(n) = 1_R + \cdots + 1_R$, the sum of n copies of 1_R, and if n is negative $f(n) = -f(-n)$.
(5) Write [36] for the image of the integer 36 in $\mathbb{Z}_{60}$ and let R denote the subset of $\mathbb{Z}_{60}$ consisting of all multiples of [36]. Explain why R is a ring and determine the identity element of R.
   All multiples of 36 form an ideal, the principal ideal generated by 36, so R is an additive group under $+$ and closed under $\times$ (i.e., a product of two elements in R is in R), so we only need check R has an identity. Since $36+36 = 12$ in $\mathbb{Z}_{60}$ and $36 = 12+12+12$, R is also the additive group generated by 12. Now $12 \times 36 = 12 \times 6 \times 6 = 72 \times 6 = 12 \times 6 = 72 = 12$, so $1_R = 36$. OR For the last step you could just observe that $36 \times 36 = 9 \times 9 \times 4 \times 4 = 21 \times 4 \times 4 = 84 \times 4 = 24 \times 4 = 96 = 36$ so $1_R = 36$.
(6) Write down a ring isomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$.
   Define $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ by $\phi(x) = (x + (2), x + (3))$.

Part 4.

The following questions should be answered TRUE OR FALSE. Just write T or F. NO REASON IS NEEDED. You get +2 for each correct answer and -2 for each wrong answer.

(1) The subset of $M_n(\mathbb{C})$ consisting of all invertible matrices is a subring.
   F It is not a group under $+$ because it doesn't contain 0. More generally, it is not closed under $+$ because a sum of invertible matrices need not be invertible. Think of an example.
(2) If are isomorphisms $f : A \to B$ and $g : B \to C$ then there is an isomorphism $\phi : C \to A$.
   T take $\phi = f^{-1} \circ g^{-1}$.
(3) If $A \cong B$ and $B \ncong C$, then $A \ncong C$.

T because $\cong$ is an equivalence relation. In particular, if $f : C \to A$ and $g : A \to B$ are isomorphisms, then $gf : C \to B$ would be an isomorphism.

(4) Let A and B be subrings of a ring R. Then $A \cap B$ is a subring.
T

(5) Let A and B be subrings of a ring R. Then $A \cup B$ is a subring.
F If we add an element of A to an element of B we need not get an element in $A \cup B$.

(6) Let A and B be subrings of a ring R. Then $A + B$ is a subring.
F It might not be closed under multiplication—if $a \in A$ and $b \in B$ there is no reason why ab should be in $A + B$.

(7) Let R be a ring that is not necessarily commutative. Then $\{x \in R \mid xy = yx \text{ for all } y \in R\}$ is a subring of R.
T This is called the center of R. You should check the details and convince yourself that it is a subring.

(8) Let $f : R \to S$ be a homomorphism and $u \in R$. If u has an inverse so does $f(u)$.
T If $uv = vu = 1$, then $f(u)f(v) = f(v)f(u) = f(1) = 1$.

(9) Let $f : R \to S$ be a homomorphism and $u \in R$. If $f(u)$ has an inverse so does u.
F The map $f : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ has the property that $f(3) = 1$ but 3 is not a unit in $\mathbb{Z}$.

(10) Let $f : R \to S$ be a homomorphism and $u \in R$. If u has an inverse so does u.
OOPS!!

(11) If two elements of a commutative ring generate the same principal ideal then each is a multiple of the other.
T Suppose $xR = yR$. Then $x = x.1$ so is in $xR = yR$ so $x = yz$ for some z; i.e., x is a multiple of y. The same argument with the roles of x and y reversed shows that y is also a multiple of x.

(12) If two elements of a commutative ring are multiples of each other they generate the same principal ideal.
T If $x = yz$, then every multiple of x is a multiple of y so $xR \subset yR$. Likewise, if $y = xw$, then $yR \subset xR$. Hence $xR = yR$.

(13) Suppose R is subring of a ring S and $xy \in R$. Then $x \in R$ and $y \in R$.
F Look at Exercise 5 in part 3: neither 4 nor 9 is in R but 4×9 is.

(14) Suppose I is an ideal of a ring S and $xy \in I$. Then $x \in I$ and $y \in I$.
F The ideal $6\mathbb{Z}$ contains 2×3 but neither 2 nor 3.

(15) The subset of $\mathbb{Z}$ consisting of all odd integers is a subring.
F It is not closed under $+$.

(16) The subset of $\mathbb{Z}$ consisting of all positive integers is a subring.
F It does not have an identity (see the instructions at the beginning of the test.

(17) The subset of $\mathbb{Z}$ consisting of all odd integers is an ideal.
F It is not closed under $+$.

(18) The subset of $\mathbb{Z}$ consisting of all even integers is an ideal.
T

(19) The subset of $\mathbb{Z}$ consisting of all positive integers is an ideal.
F It is not a subgroup.

(20) If two rings have different numbers of elements they are not isomorphic.
T An isomorphism is a *bijective* map.

(21) Let R be a field. Then every ring isomorphic to R is also a field.
T

(22) If R has infinitely many ideals so does every ring isomorphic to R.
T

(23) Let R and S be isomorphic rings. If $1+1+1$ has an inverse in R, then $1+1+1$ has an inverse in S.
T

(24) If R has infinitely many ideals so does every ring that contains R.
F Look at $\mathbb{Z} \subset \mathbb{Q}$.

(25) If the only elements in R having an inverse are ± 1 the same is true of every quotient of R.
F Look at $\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$.

(26) In every ring R, $(-x)(-y) = xy$.
T This is an easy exercise from the axioms.

(27) There are non-zero elements $x, y, z \in \mathbb{Z}_{100}$ such that $xy = xz \neq 0$ but $y \neq z$.
T Take $x = 5$, $y = 2$, $z = 22$.

(28) There are non-zero elements $x, y, z \in \mathbb{Z}_{101}$ such that $xy = xz \neq 0$ but $y \neq z$.
F Because 101 is prime, the ring is a field, so x has an inverse because it is non-zero, whence $y = x^{-1}.xy = x^{-1}.xz = z$.

(29) The ring $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_2 \right\}$ is commutative.
T Check it!

(30) If I and J are ideals in a ring R so is $I \cap J$.
T

(31) If I and J are ideals in a ring R so is $I \cup J$.
F Look at $I = 2\mathbb{Z}$ and $J = 3\mathbb{Z}$.

FOLLOW-UP QUESTIONS

The midterm enabled me to identify some gaps in your knowledge. I will try to probe those in the next test. Perhaps a little surprise test in a week or two. Here are some questions that would address some of the misunderstandings.

(1) The non-negative integers are not a subring of $\mathbb{Z}$ because ....
(2) In a non-commutative ring R the elements in the smallest two-sided ideal containing a are ....
(3) List all the two-sided ideals in the ring $M_3(\mathbb{R})$ of 3×3 matrices with real entries.
(4) Let a be the element

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

in the ring $R = M_3(\mathbb{R})$.

(a) The elements in the left ideal Ra are the matrices that have zeroes everywhere except possibly in ...
(b) The elements in the right ideal aR are the matrices that have zeroes everywhere except possibly in ...
(c) Find matrices u, v, w, x, y, z such that $uav + wax + yaz = 1$.

An element u is a unit in a ring R if it has an inverse. The element $a + n\mathbb{Z}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if ...

(5) In a commutative ring R, the notation (a, b, c) denotes the set $\{\cdots\}$.
(6) A subset S of a ring R is a subset if ....
(7) Let $f : R \to S$ be a map between two rings such that $f(x + y) = f(x) + f(y)$ for all x and y. Prove that $f(x - y) = f(x) - f(y)$.
(8) Let $a = \sqrt[4]{2}$. The ring $\mathbb{Z}[a]$ consists of the elements ....
(9) If I and J are ideals, then IJ denotes the ideal ...
(10) Define a field.
(11) An ideal I in a ring R is maximal if ...
(12) Let $X = \{*, +, x\}$ and $Y = \{1, 2\}$ and $Z = \{a, b, c\}$. Give examples of injective, surjective, and bijective maps between these sets.
(13) A function $f : X \to Y$ is not injective if ...
(14) A function $f : X \to Y$ is not surjective if ...
(15) The subset of $\mathbb{Z}$ consisting of all integers that leave a remainder of 5 when divided by 17 is an element of the ring ...
(16) If $f : R \to S$ is a ring homomorphism and A is a subring of R, is $f(A)$ a subring of S? True or False.
(17) Let $f : R \to S$ be a ring homomorphism and A a subring of S. Define

$$f^{-1}(A) := \{r \in R \mid f(r) \in A\}.$$

Is $f^{-1}(A)$ a subring of R? Explain.
(18) Let $f : R \to S$ be a ring homomorphism and I a ideal of S. Define

$$f^{-1}(I) := \{r \in R \mid f(r) \in I\}.$$

Is $f^{-1}(I)$ an ideal of R? Explain.
(19) If I is an ideal in a ring R, there is a homomorphism $\pi : R \to R/I$ given by the formula $\pi(x) = \cdots$.
(20) The first isomorphism theorem says that if $f : R \to S$, then $R/\ker f \cong \operatorname{im} f$. The isomorphism $\phi : R/\ker f \to \operatorname{im} f$ is given by the formula $\phi(?) = ?$.