SOLUTIONS OF MIDTERM I, MATH 103B, WINTER 2012.

ALIREZA SALEHI GOLSEFIDY

1. (5 points each) Give either an example or a proof to support your claim.

(1) There is an integral domain of characteristic 4.

Solution 1: No, there is no such integral domain. Since we know that the characteristic of an integral domain is either 0 or prime.

Solution 2: No, since the characteristic is equal to the additive order of 1. So $0 = 4 \cdot 1_R = (2 \cdot 1_R)(2 \cdot 1_R)$ and $2 \cdot 1_R \neq 0$, which $2 \cdot 1_R$ is a zero-divisor.

(2) There is an ideal I of $\mathrm{M}_2(\mathbb{Z})$ such that $\mathrm{M}_2(\mathbb{Z})/I$ is of order 125.

Solution: No, there is no such ideal. Assume to the contrary that I is an ideal such that $|\mathrm{M}_2(\mathbb{Z})/I| = 125$. We know that any ideal of $\mathrm{M}_2(\mathbb{Z})$ is of the form $\mathrm{M}_2(n\mathbb{Z})$ for some non-negative integer n. Hence any factor ring is isomorphic to

$$\mathrm{M}_2(\mathbb{Z})/\mathrm{M}_2(n\mathbb{Z}) \simeq \mathrm{M}_2(\mathbb{Z}/n\mathbb{Z}),$$

for some n. In particular, the order of any finite factor ring is of the form n^4. So it cannot be 125.

(3) Let R be a unital ring and assume $1_R + 1_R + 1_R \in U(R)$. Then there is no ideal I such that $R/I \simeq \mathbb{Z}/\mathbb{Z}_3$.

Solution 1: No, there is no such ring. Any unit in R is mapped to a unit in R/I for any ideal I. (If $ab = 1_R$, then $(a+I)(b+I) = 1_R + I = 1_{R/I}$.) So 31_R should be mapped to a unit in R/I. If R/I is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, then $3 \cdot 1_{R/I}$ should be mapped to $3 \cdot 1_{\mathbb{Z}/3\mathbb{Z}}$, which is zero. This is a contradiction as zero is not a unit.

(4) There is a unital ring R and zero-divisors a and b such that $a + b = 1$.

Solution 1: Yes, there are. (Most of rings with a zero-divisor might work!) For instance, let $R = \mathbb{Z} \oplus \mathbb{Z}$ and $a = (1,0)$ and $b = (0,1)$. Then a and b are non-zero, $ab = 0$ and $a + b = (1,1) = 1_R$.

Solution 2: Let $R = \mathbb{Z}/6\mathbb{Z}$ and $a = 4$ and $b = 3$. Then again a and b are non-zero, $ab = 0$, and $a + b = 1_R$.

2. Let $R = \left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$.

(1) (10 points) Prove that R is a commutative subring of $\mathrm{M}_2(\mathbb{Z})$.

Proof. **Closed under subtraction:** For any $a, b, a', b' \in \mathbb{Z}$,

$$\begin{bmatrix} a & b \\ 3b & a \end{bmatrix} - \begin{bmatrix} a' & b' \\ 3b' & a' \end{bmatrix} = \begin{bmatrix} a - a' & b - b' \\ 3(b - b') & a - a' \end{bmatrix} \in R.$$

Closed under multiplication:

$$\begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ 3b' & a' \end{bmatrix} = \begin{bmatrix} aa' + 3bb' & ab' + ba' \\ 3(ba' + ab') & 3bb' + aa' \end{bmatrix} \in R. \tag{1}$$

Commutativity:

$$\begin{bmatrix} a' & b' \\ 3b' & a' \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} = \begin{bmatrix} a'a + 3b'b & a'b + b'a \\ 3(b'a + a'b) & 3b'b + a'a \end{bmatrix} \in R. \tag{2}$$

By Equations (1) and (2), we see that R is commutative. □

Date: 2/1/2012.

(2) (5 points) Let n be a positive integer and $I_n = \left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in n\mathbb{Z} \right\}$. Prove that I_n is a principal ideal of R.

Proof. We claim that I_n is equal to the ideal generated by $n \cdot 1_R = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$.

Since R is commutative, we have that

$$\begin{aligned} \langle \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} \rangle &= \{ \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \} \\ &= \{ \begin{bmatrix} na & nb \\ 3nb & na \end{bmatrix} \mid a, b \in \mathbb{Z} \} \\ &= \{ \begin{bmatrix} a' & b' \\ 3b' & a' \end{bmatrix} \mid a', b' \in n\mathbb{Z} \} \\ &= I_n. \end{aligned}$$

$\square$

(3) (5 points) Find the characteristic of R/I_n.

Solution: We claim that n is the characteristic of R/I_n. To prove this, first we show that $n(x + I_n) = 0 + I_n$ for any any $x \in R$. And then we show that n is the smallest positive integer with this property.

For any $x = \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \in R$, we have that $nx = \begin{bmatrix} na & nb \\ 3nb & na \end{bmatrix} \in I_n$. So $n(x + I_n) = 0 + I_n$.

If $0 < m < n$, then $m \cdot 1_R = \begin{bmatrix} m & 0 \\ 0 & m \end{bmatrix} \notin I_n$ (as m cannot be multiple of n).

(4) (10 points) Prove that R/I_n is isomorphic to $\left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in \mathbb{Z}/n\mathbb{Z} \right\}$. In particular, $R/I_3 \simeq \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbb{Z}/3\mathbb{Z} \right\}$.

Proof. Let $f : R \to \left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in \mathbb{Z}/n\mathbb{Z} \right\}$ be given by

$$f(\begin{bmatrix} a & b \\ 3b & a \end{bmatrix}) = \begin{bmatrix} a + n\mathbb{Z} & b + n\mathbb{Z} \\ 3b + n\mathbb{Z} & a + n\mathbb{Z} \end{bmatrix}.$$

f **is a homomorphism:**

$$\begin{aligned} f(\begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \begin{bmatrix} c & d \\ 3c & d \end{bmatrix}) &= f(\begin{bmatrix} ac + 3bd & ac + bd \\ 3(ac + bd) & ac + 3bd \end{bmatrix}) \\ &= \begin{bmatrix} (ac + 3bd) + n\mathbb{Z} & (ac + bd) + n\mathbb{Z} \\ 3(ac + bd) + n\mathbb{Z} & (ac + 3bd) + n\mathbb{Z} \end{bmatrix} \\ &= \begin{bmatrix} (a + n\mathbb{Z})(c + n\mathbb{Z}) + 3(b + n\mathbb{Z})(d + n\mathbb{Z}) & (a + n\mathbb{Z})(c + n\mathbb{Z}) + (b + n\mathbb{Z})(d + n\mathbb{Z}) \\ 3(a + n\mathbb{Z})(c + n\mathbb{Z}) + (b + n\mathbb{Z})(d + n\mathbb{Z}) & (a + n\mathbb{Z})(c + n\mathbb{Z}) + 3(b + n\mathbb{Z})(d + n\mathbb{Z}) \end{bmatrix} \\ &= \begin{bmatrix} a + n\mathbb{Z} & b + n\mathbb{Z} \\ 3b + n\mathbb{Z} & a + n\mathbb{Z} \end{bmatrix} \begin{bmatrix} c + n\mathbb{Z} & d + n\mathbb{Z} \\ 3c + n\mathbb{Z} & d + n\mathbb{Z} \end{bmatrix} \\ &= f(\begin{bmatrix} a & b \\ 3b & a \end{bmatrix}) f(\begin{bmatrix} c & d \\ 3c & d \end{bmatrix}). \end{aligned}$$

f **is onto:** It is clear from the definition.

$\ker f = I_n$:

$$\begin{aligned}\begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \in \ker(f) &\iff a + n\mathbb{Z} = 0 + n\mathbb{Z} \text{ and } b + n\mathbb{Z} = 0 + n\mathbb{Z} \\ &\iff a, b \in n\mathbb{Z} \\ &\iff \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \in I_n.\end{aligned}$$

So by the first isomorphism theorem we have $R/I_n \simeq \left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in \mathbb{Z}/n\mathbb{Z} \right\}$.

When $n = 3$, since $3b = 0$ for any $b \in \mathbb{Z}/3\mathbb{Z}$, we have that

$$\left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in \mathbb{Z}/3\mathbb{Z} \right\} = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbb{Z}/3\mathbb{Z} \right\}.$$

□

(5) (5 points) Find the necessary and the sufficient condition for n such that R/I_n is a field.

Solution: We claim that the necessary and sufficient condition is that $n = p$ is prime and $x^2 = 3$ has no solution in $\mathbb{Z}/p\mathbb{Z}$.

Proof of the claim. If R/I_n is a field, then its characteristic is either 0 or prime. So $n = p$ has to be prime. Moreover any non-zero element of

$$\left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \mid a, b \in \mathbb{Z}/p\mathbb{Z} \right\}$$

should be invertible. In particular, for any $x \in \mathbb{Z}/p\mathbb{Z}$, we have

$$0 \neq \det\left(\begin{bmatrix} x & 1 \\ 3 & x \end{bmatrix} \right) = x^2 - 3,$$

which implies that $x^2 = 3$ has no solution in $\mathbb{Z}/p\mathbb{Z}$.

Now let p be a prime where $x^2 = 3$ has no solution in $\mathbb{Z}/p\mathbb{Z}$. Then if either a or b is non-zero in $\mathbb{Z}/p\mathbb{Z}$, then $a^2 - 3b^2 \neq 0$ (why?). So $a^2 - 3b^2$ is invertible in $\mathbb{Z}/p\mathbb{Z}$ if either a or b is not zero in $\mathbb{Z}/p\mathbb{Z}$. Hence

$$\begin{bmatrix} \frac{a}{a^2-3b^2} & \frac{-b}{a^2-3b^2} \\ 3\frac{-b}{a^2-3b^2} & \frac{a}{a^2-3b^2} \end{bmatrix} \in \left\{ \begin{bmatrix} a' & b' \\ 3b' & a' \end{bmatrix} \mid a', b' \in \mathbb{Z}/p\mathbb{Z} \right\},$$

which shows that any non-zero element of R/I_p is invertible.

(6) (15 points) Let $3 \neq p$ be a prime such that R/I_p is not a field. Prove that $R/I_p \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Proof. By the previous step, we know $x^2 = 3$ has a solution in $\mathbb{Z}/p\mathbb{Z}$. Let $x_0 \in \mathbb{Z}/3\mathbb{Z}$ be such that $x_0^2 = 3$. Let $f : R/I_p \to \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ be given as

$$f(\begin{bmatrix} a & b \\ 3b & a \end{bmatrix}) := (a + x_0 b, a - x_0 b).$$

You should show why f is an isomorphism! □

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu