MATH 103B Homework 3
DUE April 19, 2013

Recommended practice questions: Chapter 13 of Gallian, exercises
35, 45, 47, 49, 51, 62, 63

Chapter 14 of Gallian, exercises
8, 9, 12, 13, 17, 24, 28, 29

Assigned questions to hand in:

(1) (Gallian Chapter 13 # 46) Suppose that $a$ and $b$ belong to a commutative ring and $ab$ is a zero-divisor. Show that either $a$ or $b$ is a zero-divisor.

Solution: Let $a, b \in R$ be such that $ab$ is a zero-divisor. That is, $ab \neq 0$ and there is $c \neq 0$ such that $(ab)c = 0$. Since $ab \neq 0$, $a \neq 0$ and $b \neq 0$ (because, otherwise, $ab = 0$). Applying associativity to the LHS of $(ab)c = 0$, we have that
$$a(bc) = 0.$$ If $bc \neq 0$, then $a$ is a zero divisor. Otherwise, $bc = 0$ and, since $c \neq 0$, $b$ is a zero divisor.

(2) (Gallian Chapter 13 # 48) Suppose that $R$ is a commutative ring without zero-divisors. Show that the characteristic of $R$ is zero or prime.

Solution: Let $R$ be a commutative ring with no zero divisors. Suppose $\text{char} R > 0$. By question 47 (a recommended problem), all the nonzero elements of $R$ have the same additive order. Moreover, since $\text{char} R > 0$, this order is finite. Let $m = |x|$ for each nonzero $x \in R$; in particular $m \cdot x = 0$ and $n \cdot x \neq 0$ for $0 < n < m$, for each nonzero $x$. The characteristic of $R$ is defined to be the least positive integer $k$ such that $k \cdot x = 0$. Thus, $\text{char} R = m$. Let $s, t \in \mathbb{Z}^+$ be divisors of $\text{char} R$: $m = st$. Then, for any $x \in R$,
$$0 = m \cdot x = (st) \cdot x = (s \cdot x)(t \cdot x).$$ Since $R$ has no zero divisors, either $s \cdot x = 0$ or $t \cdot x = 0$. But, since $s, t \leq m$ and $m = |x|$, it must be the case that $s = m$ or $t = m$. Thus, $m$ is prime.

Solution to question 47: We will show that all elements in a commutative ring without zero divisors have the same additive order. Let $x, y \in R$ be nonzero elements and $n \in \mathbb{Z}^+$. Then
$$(n \cdot x)y = n \cdot (xy) = n \cdot (yx) = (n \cdot y)x.$$ In particular, if there is some $m \in \mathbb{Z}^+$ such that $m \cdot x = 0$ then
$$0 = (m \cdot x)y = (m \cdot y)x.$$ Since $R$ has no zero divisors and $x$ is nonzero, it must be the case that $m \cdot y = 0$ as well. Thus, if there is some element in $R$ with infinite order, then all nonzero elements in $R$ must as well. Also, if all elements in $R$ have finite order, then the above observation gives $|x||y|$ for each $x, y \in R$. Thus, the additive orders of all nonzero elements coincide.
(3) (Gallian Chapter 14 # 4) Find a subring of \( \mathbb{Z} \oplus \mathbb{Z} \) that is not an ideal of \( \mathbb{Z} \oplus \mathbb{Z} \). Justify your answer.

**Solution:** Consider the set \( D = \{(a, a) : a \in \mathbb{Z}\} \). To prove that it’s a subring:

- Nonempty? \((0, 0) \in D\).
- Closure? Let \( a, b \in \mathbb{Z} \) and consider \((a, a), (b, b) \in D\).
  - Subtraction: \((a, a) - (b, b) = (a - b, a - b) \in D\).
  - Multiplication: \((a, a)(b, b) = (ab, ab) \in D\).

But, it’s not an ideal. For example, consider \((1, 1) \in D\) and \((2, 3) \in \mathbb{Z} \oplus \mathbb{Z}\). Then \((1, 1)(2, 3) = (2, 3) \notin D\).

(4) (Gallian Chapter 14 # 10) If \( A \) and \( B \) are ideals of a ring, show that the sum of \( A \) and \( B \), \( A + B = \{a + b : a \in A, b \in B\} \), is an ideal.

**Solution:** We use the ideal test:

- Nonempty? Since \( A, B \) are ideal, they are nonempty. So, let \( a \in A, b \in B \). Then \( a + b \in A + B \) and so it is nonempty as well.
- Closure under subtraction? Let \( x, x' \in A + B \). Then there are \( a, a' \in A \) and \( b, b' \in B \) such that
  \[
  x = a + b \quad \text{and} \quad x' = a' + b'.
  \]
  Then
  \[
  x - x' = (a + b) - (a' + b') \overset{\text{in ring is abelian}}{=} \overset{\text{in ring is abelian}}{=} (a - a') + (b - b') \in A + B
  \]
  since \( A, B \) are ideals and so are closed under subtraction.
- Strong closure under multiplication? Let \( x \in A + B \) and \( y \in R \). There are elements \( a \in A \) and \( b \in B \) such that \( x = a + b \). Consider
  \[
  xy = (a + b)y \overset{\text{dist.}}{=} ay + by \in A + B
  \]
  \[
  yx = y(a + b) \overset{\text{dist.}}{=} ya + yb \in A + B
  \]
  since \( A, B \) are ideals.

Thus, \( A + B \) is an ideal.

(5) (Gallian Chapter 14 # 15) If \( A \) is an ideal of a ring \( R \) and \( 1 \) belongs to \( A \), prove that \( A = R \).

**Solution:** By definition of ideal, \( A \subseteq R \). It remains to prove that \( R \subseteq A \). By strong closure under multiplication, for any \( a \in A \) and \( r \in R \), \( ar \in A \). Let \( r \in R \). Then, by definition of unity, \( r = 1r \). By assumption on \( A \), \( 1 \in A \). Therefore, strong closure (with \( a = 1 \)), gives that \( r \in A \). Since this works for an arbitrary \( r \in R \), \( A \subseteq R \) and also \( A = R \).

(6) (Gallian Chapter 14 # 22) Let \( I = \langle 2 \rangle \). Prove that \( I[x] \) is not a maximal ideal of \( \mathbb{Z}[x] \), even though \( I \) is a maximal ideal of \( \mathbb{Z} \).

**Solution:** We will find a proper ideal of \( \mathbb{Z}[x] \) which contains \( I \). Consider \( E \), the set of all polynomials with even constant term. In Quiz 2, we proved that this is an ideal of
\[ Z[x]. \] Moreover, it is a proper ideal since, for example, \( 1 \notin E \) but \( 1 \in Z[x] \). Also, \( I \subseteq E \) because any polynomial in \( I \) is such that all of its coefficients are even, so in particular the coefficient of its constant term is even. Finally, \( I \subseteq E \) because \( x + 2 \in E \setminus I \).

We also prove that \( I \) is a maximal ideal of \( Z \). Let \( B \) be an ideal such that \( I \subseteq B \subseteq Z \). We want to show that \( B = I \) or \( B = Z \). Suppose that \( B \neq I \). We will show that \( 1 \in B \) and hence, by the previous question, that \( B = Z \). Let \( x \in B \setminus I \). Since \( I \) is the set of even integers, \( x \) is odd. In particular, this means that \( \gcd(x, 2) = 1 \). By properties of \( \gcd \), there are \( s, t \in Z \) such that

\[ 1 = xs + 2t. \]

That is, we have written 1 as a sum of products of \( x, 2 \) with ring elements. But \( x, 2 \) are both in \( B \) (\( 2 \) by definition and 2 because \( I \subseteq B \)) so by definition of an ideal, \( 1 \in B \) as well and we are done.

(7) (Gallian Chapter 14 # 26) If \( R \) is a commutative ring with unity and \( A \) is a proper ideal of \( R \), show that \( R/A \) is a commutative ring with unity.

Solution: By Theorem 14.2, \( R/A \) is a ring. It remains to prove that it is commutative and has unity. Let \( X, Y \in R/A \). These cosets have representatives, say \( x, y \in R \). Then

\[ XY = (x + A)(y + A) = (xy) + A = (yx) + A = (y + A)(x + A) + YX. \]

So, \( R/A \) is a commutative ring.

Let \( 1 \) be the unity of \( R \). We will prove that \( 1 + A \) is the unity of \( R/A \). To do so, let \( X \in R/A \) and let \( x \in R \) be such that \( X = x + A \). Then

\[ (1 + A)X = (1 + A)(x + A) = (1x) + A = x + A = X \]

and

\[ X(1 + A) = (x + A)(1 + A) = (x1) + A = x + A = X. \]

(8) (Gallian Chapter 14 # 35) In \( Z \oplus Z \), let \( I = \{(a, 0) : a \in Z \} \). Show that \( I \) is a prime ideal but not a maximal ideal.

Solution: By Theorems 14.3 and 14.4, it suffices to prove that \( Z \oplus Z/I \) is an integral domain but not a field. By the previous question, since \( Z \oplus Z \) is a commutative ring with unity \((1, 1)\) and \( I \) is a proper ideal of this ring, we know that \( Z \oplus Z/I \) is a commutative ring with unity. It remains to prove that \( Z \oplus Z/I \) has no zero divisors and that some nonzero element is not a unit.

Let \( X, Y \in Z \oplus Z/I \) and suppose \( XY = I \). (Recall that the “zero”, additive identity, of the factor group when we divide by \( I \) is \( I \) itself.) We want to show that \( X = I \) or \( Y = I \). Let \( a_1, a_2, b_1, b_2 \in Z \) be such that

\[ X = (a_1, a_2) + I \quad Y = (b_1, b_2) + I. \]

Then, by definition of \( I \),

\[ X = \{(x, a_2) : x \in Z\} \quad Y = \{(y, b_2) : y \in Z\}. \]

Using the assumption:

\[ I = XY = (a_1, a_2)(b_1, b_2) + I = (a_1b_1, a_2b_2) + I. \]
Therefore, by Lemma on cosets (p. 145)

\[(a_1b_1, a_2b_2) \in I.\]

That is, \(a_2b_2 = 0\). Since \(\mathbb{Z}\) has no zero divisors, this means that \(a_2 = 0\) or \(b_2 = 0\). In the first case, we get \(X = \{(x, 0) : x \in \mathbb{Z}\} = I\); in the second case, we get \(Y = \{(y, 0) : y \in \mathbb{Z}\} = I\). Thus, \(Z \oplus Z/I\) has no zero divisors.

Consider the coset \((2, 2) + I\). Note that it is nonzero because \((2, 2) \notin I\). We will prove that this coset is not a unit of \(Z \oplus Z/I\). Recall that (by the previous question) the unity of \(Z \oplus Z/I\) is \((1, 1) + I\). Suppose, towards a contradiction, that there were \(a, b \in \mathbb{Z}\) such that \(((2, 2) + I)((a, b) + I) = (1, 1) + I\). Then

\[2a, 2b + I = (1, 1) + I.\]

By the Lemma on cosets, this happens if and only if \((2a, 2b) \in (1, 1) + I\). That is, if and only if there is \(x \in \mathbb{Z}\) such that

\[(2a, 2b) = (1, 1) + (a, 0) = (a, 1).\]

We obtain the system of simultaneous equations

\[
\begin{align*}
2a &= a \\
2b &= 1
\end{align*}
\]

The first of these equations can be solved \((a = 0)\) but the second cannot, since \(2\) is not a unit of \(\mathbb{Z}\). Thus, \((2, 2) + I\) is not a unit of \(Z \oplus Z/I\) and this ring is not a field.