MATH 103B Homework 6 - Solutions
DUE May 17, 2013
Version May 18, 2013

Assigned reading: Chapter 17 of Gallian.

Recommended practice questions: Chapter 17 of Gallian, exercises 27, 28, 35

Supplementary Exercises for Chapters 15-18 11, 13, 19, 25

Assigned questions to hand in:

(1) (Gallian Chapter 17 # 8) Suppose that \( f(x) \in \mathbb{Z}_p[x] \) and \( f(x) \) is irreducible over \( \mathbb{Z}_p \), where \( p \) is prime. If \( \deg f(x) = n \), prove that \( \mathbb{Z}_p[x]/\langle f(x) \rangle \) is a field with \( p^n \) elements.

Solution: By Corollary 1 to Theorem 17.5, since \( \mathbb{Z}_p \) is a field and \( f(x) \) is irreducible over \( \mathbb{Z}_p \), then \( \mathbb{Z}_p[x]/\langle f(x) \rangle \) is a field. It remains to argue that this field has \( p^n \) many elements. An element of this field is a coset \( p(x) + \langle f(x) \rangle \).

Since \( f(x) \) generates \( \langle f(x) \rangle \), it has minimal degree in this ideal. Therefore, we can find minimal coset representatives of cosets of this ideal by computing the remainder upon division by \( f(x) \). The remainder, by the division theorem, is either zero or has degree strictly less than \( n \), the degree of \( f(x) \). Thus, the set of possible remainders is obtained by considering all possible combinations of coefficients

\[ a_{n-1}x^{n-1} + \cdots + a_0 \]

as \( a_i \in \mathbb{Z}_p \). Since there are \( p \) choices for each coefficient, and \( n \) slots, there are \( p^n \) choices. Thus, there are \( p^n \) distinct cosets of \( \langle f(x) \rangle \) in \( \mathbb{Z}_p[x] \) and the field \( \mathbb{Z}_p[x]/\langle f(x) \rangle \) has \( p^n \) elements.

(2) (Gallian Chapter 17 # 25) Find all the zeros and their multiplicities of

\[ x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1 \]

over \( \mathbb{Z}_5 \).

Solution: Let \( f(x) = x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1 \). Evaluating \( f(x) \) at \( a = 1 \), we get

\[ 1^5 + 4 \cdot 1^4 + 4 \cdot 1^3 - 1^2 - 4 \cdot 1 + 1 = 1 + 4 + 4 - 1 - 4 + 1 = 0. \]

Therefore, this is a root. To compute its multiplicity, we divide \( f(x) \) by \( x - 1 \):

\[ x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1 = (x - 1)(x^4 + 4x^2 + 3x - 1) \]

Then

\[ 1^4 + 4 \cdot 1^2 + 3 \cdot 1 - 1 = 1 + 4 + 3 - 1 \neq 0, \]

so \((x - 1)^2\) does not divide \( f(x) \) and \( a = 1 \) has multiplicity 1.

However,

\[ 3^4 + 4 \cdot 3^2 + 3 \cdot 3 - 1 = 81 + 36 + 9 - 1 = 0, \]
so $a = 3$ is another root of $f(x)$. To compute its multiplicity, we divide $x^4 + 4x^2 + 3x - 1$ by $x - 3$:

$$x^4 + 4x^2 + 3x - 1 = (x - 3)(x^3 + 3x^2 + 3x + 2).$$

Evaluating the quotient at $a = 3$:

$$3^3 + 3 \cdot 3^2 + 3 \cdot 3 + 2 = 27 + 27 + 9 + 2 = 0,$$

so $a = 3$ has multiplicity at least 2. Dividing again:

$$x^3 + 3x^2 + 3x + 2 = (x - 3)(x^2 + x + 1).$$

However, $3^2 + 3 + 1 \neq 0$ so $a = 3$ has multiplicity 2.

The polynomial $g(x) = x^2 + x + 1$ has no roots in $\mathbb{Z}_5$:

- $g(0) = 1$
- $g(1) = 3$
- $g(2) = 2$
- $g(3) = 3$
- $g(4) = 1$

Therefore, a complete factorization of $f(x)$ is

$$f(x) = (x - 1)(x - 3)^2(x^2 + x + 1).$$

Thus, $f(x)$ has two zeros: $a = 1$ with multiplicity 1 and $a = 3$ with multiplicity 2.

(3) (Gallian Chapter 17 # 33) Let $F$ be a field and let $p(x)$ be irreducible over $F$. Show that

$$\{a + \langle p(x) \rangle : a \in F\}$$

is a subfield of $F[x]/\langle p(x) \rangle$ isomorphic to $F$.

**Solution:** Consider the function $\varphi : F \to F[x]/\langle p(x) \rangle$ defined by

$$\varphi(a) = a + \langle p(x) \rangle.$$

We will show this is a ring isomorphism:

- **Homomorphism:** Let $a, b \in F$.
  - $\varphi(a + b) = (a + b) + \langle p(x) \rangle = (a + \langle p(x) \rangle) + (b + \langle p(x) \rangle) = \varphi(a) + \varphi(b)$.
  - $\varphi(ab) = (ab) + \langle p(x) \rangle = (a + \langle p(x) \rangle)(b + \langle p(x) \rangle) = \varphi(a) \cdot \varphi(b)$.

- **One-to-one:** It’s equivalent to prove that $\ker \varphi = \{0_F\}$. Let $a \in F$ and suppose $\varphi(a) = 0_{F[x]/\langle p(x) \rangle}$. By definition, this means that $a + \langle p(x) \rangle = 0_{F[x]/\langle p(x) \rangle} = \langle p(x) \rangle$. By properties of cosets, this means $a \in \langle p(x) \rangle$. Since $p(x)$ is irreducible, it’s nonzero and nonconstant. Therefore, the only constant in $\langle p(x) \rangle$ is the zero polynomial. That is, $a = 0$, as required.

- **Onto:** Let $a + \langle p(x) \rangle$ be a coset in the set. Then $a \in F$ and $\varphi(a) = a + \langle p(x) \rangle$, as required.

(4) (Gallian Supplementary Exercises for Chapters 15-18 # 12) Is the homomorphic image of a principal ideal domain a principal ideal domain?

**Solution:** No. Consider the rings $\mathbb{Z}, \mathbb{Z}_n$ for $n$ an integer greater than 1 that is not prime. We will prove that

I. $\mathbb{Z}$ is a PID.

II. there is a homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}_n$

III. $\mathbb{Z}_n$ is not a PID.
Recall that a PID is an integral domain with the additional property that every ideal in the ring is generated by some element in the ring. Proofs:

I. We have proved that $\mathbb{Z}$ is an integral domain (cf. Chapter 13, example 1). Let $A$ be an ideal of $\mathbb{Z}$. If $A = \{0\}$ then $A = \langle 0 \rangle$ so it is principal. Otherwise, if $x \in A$ is negative then $0 - x \in A$ as well (by closure under subtraction and since $0 \in A$ because $A$ is a subring and hence contains the additive identity). Thus, $A$ must contain a positive number as well. Let $m$ be the smallest positive number in $A$. We will prove that $A = \langle m \rangle$.

- Suppose $n \in \langle m \rangle$. Then $n = Cm$ for some $C \in \mathbb{Z}$. Since $A$ is an ideal of $\mathbb{Z}$, it is closed under this type of multiplication so $n \in A$.
- Suppose $n \in A$. By the division algorithm, $n = qm + r$ for some $q \in \mathbb{Z}$, $0 \leq r < m$. Towards a contradiction, assume that $r \neq 0$. Then $r = n - qm \in A$ is a positive number smaller than $m$, contradicting our choice of $m$. Therefore, $n =qm$ and so $n \in \langle m \rangle$.

Thus, $\mathbb{Z}$ is a PID.

II. Consider the reduction mod $n$ function. It maps $\mathbb{Z}$ onto $\mathbb{Z}_n$. Moreover, for $x, y \in \mathbb{Z}$, $(x + y) \mod n = x \mod n + y \mod n$ and $(xy) \mod n = (x \mod n)(y \mod n)$. Thus, it is a ring homomorphism.

III. $\mathbb{Z}_n$ is not a PID because it is not an integral domain. To prove that it’s not an integral domain, let $n = mr$ be a nontrivial factorization of $n$. Then, $m, r \in \mathbb{Z}_n$ are nonzero elements but $mr = 0$ in $\mathbb{Z}_n$. Thus, $\mathbb{Z}_n$ has zero divisors and is not a PID.

(5) (Gallian Supplementary Exercises for Chapters 15-18 # 20) For any integers $m$ and $n$, prove that the polynomial $x^3 + (5m + 1)x + 5n + 1$ is irreducible over $\mathbb{Z}$.

Solution: Let $f(x) = x^3 + (5m + 1)x + 5n + 1$. Applying the mod 5 irreducibility test, we compute

$$f(x) = x^3 + x + 1.$$ 

This is a degree 3 polynomial, like $f(x)$. Moreover it is irreducible over $\mathbb{Z}_5$ if and only if it has no roots in $\mathbb{Z}_5$, by Theorem 17.1. To look for roots of $f(x)$ in $\mathbb{Z}_5$, we evaluate the polynomial at the five elements of $\mathbb{Z}_5$:

- $\bar{f}(0) = 1$
- $\bar{f}(1) = 3$
- $\bar{f}(2) = 8 + 2 + 1 = 1$
- $\bar{f}(3) = 27 + 3 + 1 = 1$
- $\bar{f}(4) = 64 + 4 + 1 = 4$.

Thus, $\bar{f}(x)$ has no roots in $\mathbb{Z}_5$ and hence is irreducible over $\mathbb{Z}_5$. By the mod 5 irreducibility test, we conclude that $f(x)$ is irreducible over $\mathbb{Q}$. Moreover, we showed that $f(x)$ has nontrivial factorizations in $\mathbb{Q}[x]$ if and only if it has no proper factorizations in $\mathbb{Z}[x]$. Therefore, $f(x)$ has no proper factorizations in $\mathbb{Z}[x]$. The only other nontrivial factorization over $\mathbb{Z}[x]$ it may have are of the form $c q(x)$, where $c \in \mathbb{Z}$ a nonunit and $q(x) \in \mathbb{Z}[x]$ with $\text{deg } q(x) = \text{deg } f(x)$. However, no such factorizations are possible in this case because the only divisors of 1 (the leading and constant coefficients of $f(x)$) are $\pm 1$, the units of $\mathbb{Z}[x]$. Thus, $f(x)$ is irreducible over $\mathbb{Z}$.

(6) (Gallian Supplementary Exercises for Chapters 15-18 # 23) Is $\langle 3 \rangle$ a maximal ideal in $\mathbb{Z}[i]$?
Solution: Yes, it is a maximal ideal. To prove this, we use Theorem 14.4, which states that \( \langle 3 \rangle \) is a maximal ideal in \( \mathbb{Z}[i] \) if and only if \( \mathbb{Z}[i]/\langle 3 \rangle \) is a field. By exercise 26 in Chapter 14, since \( \langle 3 \rangle \) is a proper ideal and \( \mathbb{Z}[i] \) is a commutative ring with unity, the factor ring is a commutative ring with unity, \( 1 + \langle 3 \rangle \). It remains to prove that every nonzero element of this factor ring has a unit. We begin by listing the elements of the factor ring:

- \( 0_{\mathbb{Z}[i]/\langle 3 \rangle} = \langle 3 \rangle \).
- \( 1_{\mathbb{Z}[i]/\langle 3 \rangle} = 1_{\mathbb{Z}[i]} + \langle 3 \rangle = 1 + \langle 3 \rangle \).

Note that the zero of a field does not have a multiplicative inverse and the unity of a ring is its own inverse. The other cosets of \( \langle 3 \rangle \) are determined by the remainder modulo 3 of the real and imaginary parts of each of the coset representatives:

- \( 2 + \langle 3 \rangle \) Mutliplicative inverse: \( 2 + \langle 3 \rangle \).
- \( i + \langle 3 \rangle \) Mutliplicative inverse: \( 2i + \langle 3 \rangle \).
- \( 1 + i + \langle 3 \rangle \) Mutliplicative inverse: \( 2 + i + \langle 3 \rangle \).
- \( 2 + i + \langle 3 \rangle \) Mutliplicative inverse: \( 1 + i + \langle 3 \rangle \).
- \( 2i + \langle 3 \rangle \) Mutliplicative inverse: \( i + \langle 3 \rangle \).
- \( 1 + 2i + \langle 3 \rangle \) Mutliplicative inverse: \( 2 + 2i + \langle 3 \rangle \).
- \( 2 + 2i + \langle 3 \rangle \) Mutliplicative inverse: \( 1 + 2i + \langle 3 \rangle \).

Since each nonzero element of the commutative ring with unity \( \mathbb{Z}[i]/\langle 3 \rangle \) has a multiplicative inverse, this is a field.