MATH 103B Homework 4 - Solutions

Due May 3, 2013

(1) (*Gallian Chapter 15 # 2*) Prove Theorem 15.2: Let φ be a ring homomorphism from a ring R to a ring S. Then $Ker\varphi$, defined as $\{r \in R : \varphi(r) = 0\}$ is an ideal of R.

Solution: We will prove that $Ker\varphi$ passes the ideal test:

- Nonempty? Since any ring homomorphism $R \to S$ maps 0_R to 0_S, $0_R \in Ker\varphi$.
- Closure under subtraction? Let $x, y \in Ker\varphi$. We will show that $x - y \in Ker\varphi$ as well. By the definition of kernel, we need to show that $\varphi(x - y) = 0_S$. We compute:
$$\varphi(x - y) \overset{\text{hom}}{=} \varphi(x) - \varphi(y) = 0_S - 0_S = 0_S,$$
as required.
- Strong closure under multiplication? Let $x \in Ker\varphi$ and $r \in R$. We will show that $xr \in Ker\varphi$ as well. By the definition of kernel, we need to show that $\varphi(xr) = 0_S$. We compute:
$$\varphi(xr) \overset{\text{hom}}{=} \varphi(x)\varphi(r) = 0_S\varphi(r) = 0_S,$$
as required.

Thus, $Ker\varphi$ is an ideal.

(2) (*Gallian Chapter 15 # 10*)

(a) Is the ring $2\mathbb{Z}$ isomorphic to the ring $3\mathbb{Z}$? Justify your answer.
Solution: No. We consider properties of homomorphism: for each positive n, and each $r \in R$, if φ is a homomorphism then $\varphi(nr) = n\varphi(r)$ and $\varphi(r^n) = (\varphi(r))^n$.
Let $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ be an arbitrary ring homomorphism. Consider $\varphi(4)$. By definition, there are some $j, k \in \mathbb{Z}$ such that $\varphi(2) = 3j$ and $\varphi(4) = 3k$. On the one hand, $4 = 2 \cdot 2$. On the other hand, $4 = 2^2$. Therefore,
$$3k = \varphi(4) = 2 \cdot \varphi(2) = 6j$$
and
$$3k = \varphi(4) = (\varphi(2))^2 = 9j^2.$$
Thus, we get $6j = 9j^2$. This is possible if $j = 0$ or $6 = 9j$. In the latter case, $j = \frac{2}{3} \notin \mathbb{Z}$. We conclude that the only homomorphism between $2\mathbb{Z}$ and $3\mathbb{Z}$ is the trivial homomorphism. This homomorphism is neither injective nor surjective so there are no ring isomorphisms between these two rings.

(b) Is the ring $2\mathbb{Z}$ isomorphic to the ring $4\mathbb{Z}$? Justify your answer.

A similar calculation to that above gives
$$4k = \varphi(4) = 2 \cdot 4j = 8j \qquad 4k = \varphi(4) = (4j)^2 = 16j^2.$$
Equating the two, we get $8j = 16j^2$. Our two solutions here are $j = 0$ and $j = \frac{1}{2}$. Thus, again, the only homomorphism is the trivial one and $2\mathbb{Z} \not\cong 4\mathbb{Z}$.

(3) (*Gallian Chapter 15 #14*) Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ and

$$H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

Show that $\mathbb{Z}[\sqrt{2}]$ and H are isomorphic as rings.

Solution: Consider the map $\varphi : \mathbb{Z}[\sqrt{2}] \to H$ given by

$$\varphi(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

We will prove this is an isomorphism.

- 1-1? Let $a, b, a', b' \in \mathbb{Z}$. Suppose $\varphi(a + b\sqrt{2}) = \varphi(a' + b'\sqrt{2})$. We will show this implies that $a = a'$ and $b = b'$. Recall that two matrices are equal iff they have the same (i, j)-entry for each i, j. Equality of the $(1, 1)$-entries guarantees that $a = a'$. Equality of the $(2, 1)$-entries guarantees that $b = b'$.
- Onto? From definition of H and φ, any matrix in H can be written as the image of some element in $\mathbb{Z}[\sqrt{2}]$.
- Ring homomorphism?
  - Preserves +? Let $a, b, a', b' \in \mathbb{Z}$. Consider

$$\begin{aligned} \varphi(a + b\sqrt{2}) + \varphi(a' + b'\sqrt{2}) &= \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a + a' & 2b + 2b' \\ b + b' & a + a' \end{pmatrix} \\ &= \begin{pmatrix} a + a' & 2(b + b') \\ b + b' & a + a' \end{pmatrix} = \varphi((a + a') + (b + b')\sqrt{2}) \end{aligned}$$

  - Preserves $\cdot$?

$$\varphi(a + b\sqrt{2})\varphi(a' + b'\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' + 2bb' & 2ab' + 2ba' \\ ba' + ab' & 2bb' + aa' \end{pmatrix}$$

$$\begin{aligned} \varphi((a + b\sqrt{2})(a' + b'\sqrt{2})) &= \varphi(aa' + ba'\sqrt{2} + ab'\sqrt{2} + 2bb') \\ &= \varphi((aa' + 2bb') + (ba' + ab')\sqrt{2}) = \begin{pmatrix} aa' + 2bb' & 2ba' + 2ab' \\ ba' + ab' & aa' + 2bb' \end{pmatrix} \end{aligned}$$

and these are equal because addition and multiplication each commute in $\mathbb{Z}$.

(4) (*Gallian Chapter 15 # 44*) Let R be a commutative ring of prime characteristic p. Show that the Frobenius map, defined by $x \mapsto x^p$ is a ring homomorphism from R to R.

Solution: We need to prove that this map respects addition and multiplication. Let $x, y \in R$.

- For addition, we use the Binomial Theorem:

$$(x + y)^p \overset{\text{Bin Thm}}{=} x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p.$$

  It would be enough to show that each of the binomial coefficients is divisible by p, since we assume that R has characteristic p and so each of the corresponding terms would then be zero.
  Combinatorial identity: For any $n > 0$ and $0 < k < n$, $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.

Therefore, since $\binom{p-1}{k-1} \in \mathbb{Z}^{\geqslant}$, $p|k\binom{p}{k}$ for each k. Since p is prime, by Euclid's Lemma,$p|k$ or $p|\binom{p}{k}$. But, p cannot divide k since $k < p$. Therefore, for each $0 < k < p$, p divides $\binom{p}{k}$, as required.

- For multiplication, we compute

$$(xy)^p = xyxy \cdots xy \overset{R \text{ comm.}}{=} x^p y^p,$$

as required.

(5) (*Gallian Chapter 16 # 12*) If the rings R and S are isomorphic, show that $R[x]$ and $S[x]$ are isomorphic.

Solution: Let $\varphi : R \to S$ be a ring isomorphism. Define $\psi : R[x] \to S[x]$ by

$$\psi(a_n x^n + \cdots + a_0) = \varphi(a_n)x^n + \cdots + \varphi(a_0)$$

We will prove that this is a ring isomorphism.

- One-to-one: Suppose $p(x), q(x) \in R[x]$ and $\psi(p(x)) = \psi(q(x))$. That is, the coefficients of each pair of corresponding terms in the polynomials $\psi(p(x)), \psi(q(x)) \in S[x]$ are equal. By definition of ψ, each of these coefficients is the image of a coefficient of $p(x)$ or $q(x)$ under φ. Since φ is one-to-one, if the coefficients in $\psi(p(x)), \psi(q(x))$ are equal then so are the coefficients in $p(x), q(x)$. Thus, by definition of equality of polynomials, $p(x) = q(x)$.
- Onto: Let $r(x) = c_n x^n + \cdots + c_0 \in S[x]$. We want to find $p(x) \in R[x]$ such that $\psi(p(x)) = r(x)$. Since φ is onto S, there are $a_n, \ldots, a_0 \in R$ such that $\varphi(a_n) = c_n, \ldots, \varphi(a_0) = c_0$. Let $p(x) = a_n x^n + \cdots + a_0$. Then, by definition of ψ, $\psi(p(x)) = \varphi(a_n)x^n + \cdots + \varphi(a_0) = c_n x^n + \cdots + c_0 = r(x)$, as required.
- Respects $+$: Let $p(x) = a_n x^n + \cdots + a_0, q(x) = b_n x^n + \cdots + b_0 \in R[x]$. (Without loss of generality, we write these with the same top power; if $p(x), q(x)$ have different degrees, the top terms of the lower degree of the two will be all zero.) Then

$$\begin{aligned}
\psi(p(x) + q(x)) &= \psi([a_n + b_n]x^n + \cdots + [a_0 + b_0]) \\
&= \varphi(a_n + b_n)x^n + \cdots + \varphi(a_0 + b_0) \\
&\overset{\varphi \text{ hom.}}{=} [\varphi(a_n) + \varphi(b_n)]x^n + \cdots + \varphi(a_0) + \varphi(b_0) \\
&= \varphi(a_n)x^n + \cdots + \varphi(a_0) + \varphi(b_n)x^n + \cdots + \varphi(b_0) = \psi(p(x)) + \psi(q(x)),
\end{aligned}$$

as required.

- Respects $\cdot$: Let $p(x) = a_n x^n + \cdots + a_0, q(x) = b_m x^m + \cdots + b_0 \in R[x]$. Then

$$\begin{aligned}
\psi(p(x)q(x)) = \psi\Big(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j}\Big) &= \sum_{i=0}^{n}\sum_{j=0}^{m} \varphi(a_i b_j) x^{i+j} \\
&\overset{\varphi \text{ hom.}}{=} \sum_{i=0}^{n}\sum_{j=0}^{m} \varphi(a_i)\varphi(b_j)x^{i+j} = \psi(p(x))\psi(q(x)),
\end{aligned}$$

as required.

(6) (*Gallian Chapter 16 # 24*) Let F be an infinite field and let $f(x), g(x) \in F[x]$. If $f(a) = g(a)$ for infinitely many elements a of F, show that $f(x) = g(x)$.

Solution: Consider the polynomial $h(x) = f(x) - g(x)$. For each $a \in F$ with $f(a) = g(a)$, $h(a) = 0$. Therefore, h is a polynomial with infinitely many roots. By corollary to Theorem 16.2, a polynomial of degree n can have at most n many roots. Therefore, h can't have degree n for any n. The only polynomial with no degree is the zero polynomial. Thus, $h(x) = 0$. In particular, this means that each of the coefficients of h is zero. But, each of these coefficients is the difference between the coefficients of $f(x)$ and $g(x)$. Therefore, $f(x) = g(x)$.

(7) (*Gallian Chapter 16 #32*) Let F be a field and let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$. Prove that $x - 1$ is a factor of $f(x)$ if and only if $a_n + \cdots + a_1 + a_0 = 0$.

Solution: Suppose $x - 1$ is a factor of $f(x)$. Then, by Corollary to Theorem 16.2, 1 is a root of $f(x)$. Substituting 1 for x in $f(x)$ gives

$$0 = f(1) = a_n 1^n + \cdots + a_1 1 + a_0 = a_n + \cdots + a_1 + a_0.$$

Conversely, suppose $a_n + \cdots + a_1 + a_0 = 0$. As we just saw, this implies that $f(1) = 0$ or that 1 is a zero of f. The corollary is an "if and only if" statement and guarantees that $x - 1$ is a factor of $f(x)$.

(8) (*Gallian Chapter 16 # 46*) Prove that $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is ring-isomorphic to $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

Solution: We will use the First Isomorphism Theorem. In particular, we will find an onto ring homomorphism

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$$

whose kernel is the ideal $\langle x^2 - 2\rangle$. Define

$$\varphi(a_n x^n + \cdots + a_0) = a_n(\sqrt{2})^n + \cdots + a_0.$$

The following claims finish the proof:

- The function φ has codomain $\mathbb{Q}[\sqrt{2}]$, since

$$\begin{aligned} a_n(\sqrt{2})^n + \cdots + a_0 &= \sum_{\text{even powers}} a_{2k}(\sqrt{2})^{2k} + \sum_{\text{odd powers}} a_{2j+1}(\sqrt{2})^{2j+1} \\ &= \sum_{\text{even powers}} a_{2k}2^k + \sum_{\text{odd powers}} a_{2j+1}2^j\sqrt{2}. \end{aligned}$$

  Since the rational numbers are closed under addition and multiplication, we've expressed the image under φ of an arbitrary element of $\mathbb{Q}[x]$ as an element of $\mathbb{Q}[\sqrt{2}]$.
- The function φ is onto. Why? Let $r + s\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Then $r, s \in \mathbb{Q}$ so $sx + r \in \mathbb{Q}[x]$. Moreover, $\varphi(sx + r) = s\sqrt{2} + r$, as required.
- The function φ is a ring homomorphism: note that φ is a restriction of the evaluation function $\varphi_{\sqrt{2}}$ defined in quiz 2 from $\mathbb{R}[x] \to \mathbb{R}$. In that quiz, we proved that the function respects $+, \cdot$ for all pairs of polynomials in $\mathbb{R}[x]$; hence, it will also respect these operations for polynomials in the subset $\mathbb{Q}[x]$.
- The kernel of φ is $\langle x^2 - 2\rangle$:
  ($\subseteq$) Let $p(x) \in Ker\varphi$. That is, $\varphi(p(x)) = 0$. By definition of φ, this means that $p(\sqrt{2}) = 0$. Suppose, towards a contradiction that $p(x) \notin \langle x^2 - 2\rangle$. Since $\mathbb{Q}$

is a field, Theorem 16.2 gives us the Division Algorithm for $\mathbb{Q}[x]$ and we have $q(x), r(x) \in \mathbb{Q}[x]$ such that

$$p(x) = (x^2 - 2)q(x) + r(x), \qquad r(x) \neq 0 \text{ and } deg\ r(x) < 2.$$

Evaluating both sides at $x = \sqrt{2}$, we get

$$0 = p(\sqrt{2}) = (2 - 2)q(\sqrt{2}) + r(\sqrt{2}) = 0 + r(\sqrt{2}) = r(\sqrt{2}).$$

But, r is of the form $r(x) = a + b\sqrt{x}$ for some $a, b \in \mathbb{Q}$, not both zero. Therefore,

$$0 = a + b\sqrt{2}.$$

But then, either $b = 0$ (which forces $a = 0$, contradicting that $r(x)$ is nonzero) or

$$\sqrt{2} = \frac{-a}{b} \in \mathbb{Q},$$

contradicting the irrationality of $\sqrt{2}$. Thus, $p(x) \in \langle x^2 - 2\rangle$.

($\supseteq$) Let $p(x) \in \langle x^2 - 2\rangle$. Then there is some $q(x) \in \mathbb{Q}[x]$ such that $p(x) = q(x)(x^2 - 2)$. By definition of φ,

$$\varphi(p(x)) = p(\sqrt{2}) = q(\sqrt{2})(\sqrt{2}^2 - 2) = q(\sqrt{2})0 = 0.$$

Thus, $p(x) \in Ker\varphi$.

The First Isomorphism Theorem for rings now implies that $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is ring isomorphic to $\mathbb{Q}[\sqrt{2}]$.