Math 562 **Spring 2012**
Homework 1 **Drew Armstrong**

---

1. Let R be a ring. We say that $a \in R$ is nilpotent if $a^n = 0$ for some n. If a is nilpotent, prove that $1+a$ and $1-a$ are units (i.e. invertible).

Proof. Recall that in any ring we have $(-a)(-b) = -(ab)$ (see HW 3.7 from MTH 561). Thus in any ring with 1 (commutative or not) we have the following identities:

$$1 - a^n = (1-a)(1 + a + a^2 + \cdots + a^{n-1}),$$
$$1 - (-1)^n a^n = (1+a)(1 - a + a^2 - \cdots + (-1)^{-1}a^{n-1}).$$

If $a^n = 0$ then we obtain inverses for $1+a$ and $1-a$. $\square$

2. Let $I \subseteq R$ be an ideal. Prove that $I = R$ if and only if I contains a unit.

Proof. First suppose that $I = R$ then $1 \in I$ so I contains a unit. Conversely, suppose that I contains a unit u, say $uv = 1$ for $u, v \in R$. But since I is an ideal we have $uv = 1 \in I$. Then for any $a \in R$ we have $a = 1a \in I$. Hence $I = R$. $\square$

3. Let $\varphi : R \to S$ be a ring homomorphism.

(a) Prove that $\varphi(0_R) = 0_S$.
(b) Prove that $\varphi(-a) = -\varphi(a)$ for all $a \in R$.
(c) Let $a \in R$. If $a^{-1} \in R$ exists, prove that $\varphi(a)$ is invertible with $\varphi(a)^{-1} = \varphi(a^{-1})$.

Proof. To prove (a) note that $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. Then subtract $\varphi(0_R)$ from both sides to get $0_S = \varphi(0_R)$. To prove (b) consider $a \in R$. Then use part (a) to write $0_S = \varphi(0_R) = \varphi(a - a) = \varphi(a) + \varphi(-a)$. Now subtract $\varphi(a)$ from both sides to get $\varphi(-a) = -\varphi(a)$. To prove (c) consider $a \in R$ and suppose that there exists a^{-1} with $aa^{-1} = a^{-1}a = 1_R$. Applying φ to the three parts of this equation and using the fact that φ is a homomorphism gives $\varphi(a)\varphi(a^{-1}) = \varphi(a^{-1})\varphi(a) = 1_S$. We conclude that $\varphi(a^{-1}) = \varphi(a)^{-1}$. $\square$

[Note that the property $\varphi(ab) = \varphi(a)\varphi(b)$ does **not** imply $\varphi(1_R) = 1_S$ for rings, so we just **assume** $\varphi(1_R) = 1_S$ (because we want it).]

4. Let $I \subseteq R$ be an **ideal** and consider $a, b, c, d \in R$ with $a + I = c + I$ and $b + I = d + I$. Prove that $(a+b) + I = (c+d) + I$ and $ab + I = cd + I$. This shows that addition and multiplication of cosets is well-defined.

Proof. Since $a + I = c + I$ and $b + I = d + I$ there exist $x, y \in I$ with $a - c = x$ and $b - d = y$. To prove that $(a+b) + I = (b+d) + I$, first consider an arbitrary element $a + b + u \in (a+b) + I$ with $u \in I$. Then we have $a + b + u = (c+x) + (d+y) + u = (c+d) + (x+y+u) \in (c+d) + I$. Hence $(a+b) + I \subseteq (c+d) + I$. Similarly we find $(c+d) + I \subseteq (a+b) + I$ and hence $(a+b) + I = (c+d) + I$. To prove that $ab + I = cd + I$, first consider an arbitrary element $ab + u \in ab + I$ with $u \in I$. Then we have $ab + u = (c+x)(d+y) + u = cd + (cy + xd + xy + u)$. Since cy, xd, xy, u are all in I we conclude that $ab + u = cd + (cy + xd + xy + u) \in cd + I$, hence $ab + I \subseteq cd + I$. The proof of $cd + I \subseteq ab + I$ is similar. We conclude that $ab + I = cd + I$. $\square$

[Note that $(a+b) + I = (c+d) + I$ only requires that I is closed under addition. The proof that $ab + I = cd + I$ really requires that I is an ideal. In other words, if $S \subseteq R$ is an additive subgroup we can always define R/S as an additive group, but we can only define multiplication on R/S when S is an ideal.]

5. When does $ab = 1$ imply $ba = 1$? Consider $a, b \in R$ where R is a **finite** ring, and suppose that $ab = 1$. Show that $b + (1 - ba)a^i$ is a right inverse of a for all $i \geq 0$. Use this and the finiteness of R to show that $ba = 1$. [Recall: We have also seen that $AB = I$ implies $BA = I$ for square matrices over a field. Now we have two results of this sort...]

Proof. Suppose that $ab = 1$ and note that for all $i \geq 0$ we have

$$a[b + (1 - ba)a^i] = ab + (a - aba)a^i = 1 + a^{i+1} - aba^{i+1} = 1 + a^{i+1} - a^{i+1} = 1.$$

Hence $b + (1 - ba)a^i$ is a right inverse of a for all $i \geq 0$. Since our ring is finite there must exist $i < j$ such that $b + (1 - ba)a^i = b + (1 - ba)a^j$. Multiply both sides on the right by b^j and use the fact that $ab = 1$ to get $b + (1 - ba)b^{j-i} = b + (1 - ba)$. Now subtract b from both sides and use the fact that $(1 - ba)b = b - bab = b - b = 0$ to find $0 = 1 - ba$. We conclude that $ba = 1$ as desired. $\square$

6. Recall that a group G is simple if for **any** group homomorphism $\varphi : G \to H$ we have $\ker \varphi = G$ (the whole group) or $\ker \varphi = 1$ (the trivial group). We can define a simple ring similarly in terms of ring homomorphisms. **Prove** that a ring is simple if and only if it is a field. (Hence the term "simple ring" is unnecessary.) [Hint: Look in the book.]

Proof. Recall that $I \subseteq R$ is an ideal if an only if I is the kernel of a ring homomorphism. Thus we can say that a ring R is simple if it has only two ideals: $(1) = R$ and $(0) = \{0\}$.

First suppose that R is a field and let $I \subseteq R$ be an ideal. If $I \neq (0)$ then I contains a nonzero element a. But since R is a field, a is a unit, and we conclude by Problem 2 that $I = (1) = R$. Hence R is a simple ring.

Conversely, suppose that R is a simple ring and let $a \in R$ be a nonzero element (if $R = (0)$ then R is not really a field, but I forgot to worry about this silly case when I wrote the question). Since (a) is an ideal and $(a) \neq (0)$ we must have $(a) = (1)$. That is, a is a multiple of 1, which means that a is a unit. Since this is true for all nonzero $a \in R$, R is a field (or, I guess, a division ring — I also forgot to say that R is commutative (oh well); in any case, the term "simple ring" is unnecessary). $\square$

7. Prove Descartes' Factor Theorem. Let $\mathbb{F}$ be a field and consider the ring $\mathbb{F}[x]$ of polynomials. Given $f(x) \in \mathbb{F}[x]$ and $\alpha \in \mathbb{F}$ such that $f(\alpha) = 0$, prove that $f(x) = (x - \alpha)h(x)$ where $h(x) \in \mathbb{R}[x]$ with $\deg(h) = \deg(f) - 1$. [Hint: Observe that $x^n - \alpha^n = (x - \alpha)(x^{n-1} + \alpha x^{n-2} + \cdots + \alpha^{n-2}x + \alpha^{n-1})$ for all $n \geq 0$. Consider the polynomial $f(x) - f(\alpha)$.]

Proof. To save space, we define the polynomial $[n]_{x,\alpha} := (x^{n-1} + x^{n-2}\alpha + \cdots + x\alpha^{n-2} + \alpha^{n-1})$ for each positive integer n and real number α. Suppose that $f(x) \in \mathbb{R}[x]$ has degree d and write

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots a_1 x + a_0$$

for $a_0, \ldots, a_d \in \mathbb{R}$ with $a_d \neq 0$. Then applying the identity $x^n - \alpha^n = (x - \alpha)[n]_{x,\alpha}$ we can write

$$\begin{aligned} f(x) - f(\alpha) &= a_d(x^d - \alpha^d) + a_{d-1}(x^{d-1} - \alpha^{d-1}) + \cdots + a_1(x - \alpha) \\ &= a_d(x - \alpha)[d]_{x,\alpha} + a_{d-1}(x - \alpha)[d-1]_{x,\alpha} + \cdots + a_1(x - \alpha)[1]_{x,\alpha} \\ &= (x - \alpha)(a_d[d]_{x,\alpha} + a_{d-1}[d-1]_{x,\alpha} + \cdots + a_1[1]_{x,\alpha}) \\ &= (x - \alpha)(a_d x^{d-1} + \text{ lower order terms }). \end{aligned}$$

If $f(\alpha) = 0$ then we obtain $f(x) = (x - \alpha)h(x)$ where $h(x) \in \mathbb{R}[x]$ has degree $d - 1$. $\square$

8. Let $\mathbb{R}$ and $\mathbb{C}$ be the real and complex fields. Let $\varphi : \mathbb{R}[x] \to \mathbb{C}$ be the map that sends a polynomial $f(x)$ to its evaluation $f(i) \in \mathbb{C}$ at $x = i$.

(a) Prove that φ is a surjective ring homomorphism.

(b) Recall the definition of complex conjugation: $\overline{a + ib} := a - ib$ for $a, b \in \mathbb{R}$. **Prove** that $f(-i) = \overline{f(i)} \in \mathbb{C}$ for all $f(x) \in \mathbb{R}[x]$.

(c) Use Descartes' Factor Theorem to prove that the kernel of φ is the principal ideal generated by x^2+1:
$$\ker\varphi = (x^2+1) := \{(x^2+1)g(x) : g(x) \in \mathbb{R}[x]\}.$$

Proof. The multiplicative identity of $\mathbb{R}[x]$ is the constant polynomial $\mathbf{1}(x) = 1$, so clearly $\varphi(\mathbf{1}) = \mathbf{1}(i) = 1 \in \mathbb{C}$, which is the multiplicative identity of $\mathbb{C}$. To prove (a) we must show that $\varphi(f+g) = \varphi(f) + \varphi(g)$ and $\varphi(fg) = \varphi(f)\varphi(g)$ for all $f, g \in \mathbb{R}[x]$. To this end, let $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$. Then we have
$$\varphi(f) + \varphi(g) = f(i) + g(i) = \sum_k a_k i^k + \sum_k b_k i^k = \sum_k (a_k + b_k) i^k = (f+g)(i) = \varphi(f+g)$$
and also
$$\varphi(f)\varphi(g) = f(i)g(i) = \sum_k \left(\sum_{u+v=k} (a_u i^u)(b_v i^v) \right) = \sum_k \left(\sum_{u+v=k} a_u b_v \right) i^k = (fg)(i) = \varphi(fg).$$
Notice that the proof of $\varphi(f)\varphi(g) = \varphi(fg)$ **uses the fact that $\mathbb{C}$ is commutative**. (For this reason we will only consider polynomials over commutative rings.) Finally, note that the map is surjective since for any $a + ib \in \mathbb{C}$ we have $a + ib = \varphi(f)$ with $f(x) = a + xb \in \mathbb{R}[x]$.

Given complex numbers $a + ib$ and $c + id$ note that
$$\begin{aligned}\overline{a+ib} + \overline{c+id} &= (a - ib) + (c - id) = (a + c) - i(b + d) \\ &= \overline{(a+c) + i(b+d)} = \overline{(a+ib) + (c+id)}\end{aligned}$$
and
$$\begin{aligned}(\overline{a+ib})(\overline{c+id}) &= (a - ib)(c - id) = (ac - bd) - i(ad + bc) \\ &= \overline{(ac-bd) + i(ad+bc)} = \overline{(a+ib)(c+id)}.\end{aligned}$$
Combined with the fact that $\overline{1} = 1$ we conclude that complex conjugation $z \to \overline{z}$ is a ring isomorphism $\mathbb{C} \to \mathbb{C}$ (we call it a field automorphism). Furthermore, we have $\overline{z} = z$ for all $z \in \mathbb{R} \subseteq \mathbb{C}$. Now we will prove (b). Let $f(x) = \sum_k a_k x^k$ and consider any complex number $z \in \mathbb{C}$. Then using the homomorphism properties of conjugation we have
$$\overline{f(z)} = \overline{\sum_k a_k z^k} = \sum_k \overline{a_k} (\overline{z})^k = \sum_k a_k (\overline{z})^k = f(\overline{z}).$$
In particular, taking $z = i$ gives $f(-i) = \overline{f(i)}$.

Finally consider the surjective homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{C}$ given by $\varphi(f) = f(i)$. To prove (c) we will show that $\ker\varphi = (x^2+1)$. Indeed, if $f(x) \in (x^2+1)$ then we can write $f(x) = (x^2+1)g(x)$ and then $\varphi(f) = (i^2+1)g(i) = 0 \cdot g(x) = 0$, hence $f \in \ker\varphi$ and $(x^2+1) \subseteq \ker\varphi$. Conversely, suppose that $f \in \ker\varphi$; i.e. $f(i) = 0$. By Descartes' Factor Theorem applied to $f(x) \in \mathbb{C}[x]$ (a slightly tricky point) we have $f(x) = (x - i)g(x)$ for some $g(x) \in \mathbb{C}[x]$. But by part (b) we know that $f(i) = 0$ implies $f(-i) = 0$ hence $f(-i) = -2i \cdot g(-i) = 0$, which implies that $g(-i) = 0$. Then Descartes' Factor Theorem implies that $g(x) = (x+i)h(x)$ for some $h(x) \in \mathbb{C}[x]$. Putting this together we get
$$f(x) = (x - i)(x + i)h(x) = (x^2+1)h(x)$$
for some $h(x) \in \mathbb{C}[x]$. The only problem left is to show that $h(x) \in \mathbb{R}[x]$. But since $f(x)$ and (x^2+1) are in $\mathbb{R}[x]$ we must also have $h(x) \in \mathbb{R}[x]$ (for example, we could do long division to compute $f(x)/(x^2+1) = h(x)$). We conclude that $h(x) \in \mathbb{R}[x]$ and hence $f(x)$ is in the ideal (x^2+1) as desired. $\square$