Math 562	**Spring 2014**
Homework 2	**Drew Armstrong**

Problems on Rings

1. Chinese Remainder Theorem. Given two ideals $I, J \leq R$ we define their product:

$$IJ := \langle \{ab : a \in I, b \in J\} \rangle.$$

This is the smallest ideal containing all the elements ab for $a \in I$ and $b \in J$.

(a) Prove that $IJ \leq I \cap J$.

(b) We say that ideals $I, J \leq R$ are coprime if $I + J = R$. In this case, prove that $I \cap J \leq IJ$, and hence $IJ = I \cap J$.

(c) If $I, J \leq R$ are coprime ideals, prove that the map

$$\varphi(x + IJ) := (x + I, x + J)$$

defines a ring isomorphism $R/(IJ) \approx R/I \times R/J$.

Proof. For part (a), consider $a \in I$ and $b \in J$. Since I and J are both ideals we have $ab \in I$ and $ab \in J$, hence $ab \in I \cap J$. Thus $I \cap J$ is an ideal containing all the elements ab for $a \in I$ and $b \in J$ and it follows that $I \cap J$ contains the smallest such ideal, i.e., $IJ \leq I \cap J$.

For part (b), assume that the ideals I and J are coprime, i.e., that $I + J = R$. Then since $1 \in I + J$ there exist $a \in I$ and $b \in J$ such that $1 = a + b$. Finally, for all $r \in I \cap J$ we have $ar \in IJ$ and $rb \in IJ$, hence

$$r = r1 = r(a + b) = ra + rb = ar + rb \in IJ.$$

It follows that $I \cap J \leq IJ$. [Note: We needed the fact that R is commutative.]

For part (c), let I and J be coprime ideals and consider the map $\varphi(x+IJ) := (x+I, x+J)$. We want to prove that this is a ring isomorphism $\varphi : R/(IJ) \to (R/I) \times (R/J)$. The fact that φ is a ring homomorphism (it preserves addition, multiplication, and 1) follows directly from the definitions. To show that φ is well-defined, assume that $x + IJ = y + IJ$, i.e., that $x - y \in IJ$. By part (a) this implies that $x - y \in I \cap J$. In other words, we have $x - y \in I$ (i.e. $x + I = y + I$) and $x - y \in J$ (i.e. $x + J = y + J$). It follows that

$$\varphi(x + IJ) = (x + I, x + J) = (y + I, y + J) = \varphi(y + IJ).$$

To show that φ is injective, suppose that $(x+I, x+J) = (y+I, y+J)$, i.e., that $x+I = y+I$ and $x + J = y + J$. Then we have $x - y \in I$ and $x - y \in J$, hence $x - y \in I \cap J$. By part (b) this implies that $x - y \in IJ$, hence $x + IJ = y + IJ$, as desired. Finally, to prove that φ is surjective, consider any $(x + I, y + J) \in (R/I) \times (R/J)$. We wish to find some $\alpha \in R$ such that $\varphi(\alpha + IJ) = (x + I, y + J)$. Recall that I and J are coprime, so we can write $1 = a + b$ with $a \in I$ and $b \in J$. Now let $\alpha := ay + bx$. (Yes this is a trick, but it's the same trick we did in class.) Then we have

$$\begin{aligned}
\varphi(\alpha + IJ) &= (\alpha + I, \alpha + J) \\
&= (ay + bx + I, ay + bx + J) \\
&= (bx + I, ay + J) \\
&= ((1 - a)x + I, (1 - b)y + J) \\
&= (x - ax + I, y - by + J) \\
&= (x + I, y + J),
\end{aligned}$$

hence φ is surjective. $\square$

[When $R = \mathbb{Z}$ the ideals are just (n) for $n \in \mathbb{Z}$ (we say $\mathbb{Z}$ is a PID). Note that for all $m, n \in \mathbb{Z}$ we have $(m)(n) = (mn)$, and note that $(m) + (n) = (1)$ if and only if m and n are coprime integers. In this case, the Chinese Remainder Theorem says:

$$\mathbb{Z}/(mn) \approx \mathbb{Z}/(m) \times \mathbb{Z}/(n).$$

The classical version of this theorem appears in *The Mathematical Classic of Sunzi* from between the 3rd and 5th century. It says that for $m, n \in \mathbb{Z}$ coprime and arbitrary $a, b \in \mathbb{Z}$ the system

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a unique solution $x \pmod{mn}$. The proof of surjectivity above gives us a method to compute the solution.]

2. Groups of Units. Let R and S be rings. Prove that we have an isomorphism of groups:

$$(R \times S)^\times \approx R^\times \times S^\times.$$

Proof. Consider the inclusion map $\iota : R^\times \times S^\times \hookrightarrow R \times S$. It is obviously injective. Given units $r \in R^\times$ and $s \in S^\times$, note that (r, s) is a unit in $R \times S$ because

$$(r, s)(r^{-1}, s^{-1}) = (rr^{-1}, ss^{-1}) = (1, 1).$$

Thus we obtain an injective group homomorphism $\iota : R^\times \times S^\times \hookrightarrow (R \times S)^\times$. To see that ι is **surjective**, consider any $(r, s) \in (R \times S)^\times$. By definition this mean that there exists $(a, b) \in R \times S$ such that

$$(1, 1) = (r, s)(a, b) = (ra, sb).$$

But then $ra = 1$, hence $r \in R^\times$, and $sb = 1$, hence $s \in S^\times$. Thus $\iota : R^\times \times S^\times \to (R \times S)^\times$ is a group isomorphism. □

3. Diamond Isomorphism for Rings. Let R be a ring, let $S \subseteq R$ be a subring, and let $I \leq R$ be an ideal.

(a) Prove that $S + I$ is a subring of R.
(b) Prove that I is an ideal of $S + I$.
(c) Prove that $S \cap I$ is an ideal of S.
(d) Prove that we have an isomorphism of rings:

$$\frac{S}{S \cap I} \approx \frac{S + I}{I}.$$

[Hint: Consider the natural map $\varphi : S \to R/I$ defined by $a \mapsto a + I$. What is the image? What is the kernel? Now use the First Isomorphism Theorem.]

Proof. Let $S \subset R$ be a subring and let $I \leq R$ be an ideal. For part (a), consider $r + a$ and $s + b$ in $S + I$, i.e., consider $r, s \in S$ and $a, b \in I$. Then we have

$$(r + a) + (s + b) = (r + s) + (a + b) \in S + I$$

because $r + s \in S$ and $a + b \in I$ and

$$(r + a)(s + b) = rs + as + rb + ab = (rs) + (as + rb + ab) \in S + I$$

because $rs \in S$ and $as + rb + ab \in I$. Finally note that $1 = 1 + 0 \in S + I$ because $1 \in S$ and $0 \in I$. We conclude that $S + I \subseteq R$ is a subring.

For part (b), first note that I is an additive subgroup of $S + I$. To see that $I \leq S + I$ is an ideal, consider $a \in I$ and $s + b \in S + I$, i.e., $s \in S$ and $b \in I$. Then we have

$$a(s + b) = as + ab \in I$$

because $as \in I$ and $ab \in I$.

For part (c), first note that $S \cap I$ is an additive subgroup of S. Now consider any $a \in S \cap I$ and $s \in S$. Then we have $as \in S$ because S is closed under multiplication and $as \in I$ because I is an ideal. Hence $as \in S \cap I$ and we conclude that $S \cap I \leq S$ is an ideal.

Finally, for part (d) consider the natural map $\varphi : S \to R/I$ defined by $a \mapsto a + I$. By definition $a \in S$ is in the kernel if and only if $a + I = 0 + I$, in other words, if and only if $a \in I$. Thus we have $\ker \varphi = S \cap I$. I claim that $\operatorname{im} \varphi = (S + I)/I$. Indeed, given any $s \in S$ we have $\varphi(s) = s + I = (s + 0) + I \in (S + I)/I$. Conversely, given any $s + a \in S + I$ (i.e. with $s \in S$ and $a \in I$) we have $(s + a) + I = s + I = \varphi(s)$. By the First Isomorphism Theorem we conclude that

$$\frac{S}{S \cap I} = \frac{S}{\ker \varphi} \approx \operatorname{im} \varphi = \frac{S + I}{I}.$$

□

[I will a draw a picture in class to show you why this is called the "Diamond Isomorphism".]

Problems on Polynomials

4. Descartes' Factor Theorem. Let K be a field and consider the ring $K[x]$ of polynomials. Given $f(x) \in K[x]$ and $\alpha \in K$ such that $f(\alpha) = 0$, prove that $f(x) = (x - \alpha)h(x)$ where $h(x) \in K[x]$ 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 $d - 1$. □

5. Constructing the Complex Numbers. 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 $x^2 + 1$:

$$\ker \varphi = (x^2 + 1) := \{(x^2 + 1)g(x) : g(x) \in \mathbb{R}[x]\}.$$

(d) Conclude that $\mathbb{C}$ is isomorphic to the quotient ring $\mathbb{R}[x]/(x^2 + 1)$.

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**. (This is why we 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. Then for part (d), the First Isomorphism Theorem says that

$$\frac{\mathbb{R}[x]}{(x^2+1)} = \frac{\mathbb{R}[x]}{\ker\varphi} \approx \operatorname{im}\varphi = \mathbb{C}.$$

$\square$