Solutions of Assignment 7
Basic Algebra I

November 21, 2005

Solution of the problem 1. Recall that a field F has only two ideals: $\{0\}$, F. Also recall that the kernel of any ring homomorphism is an ideal. Now back to the problem, in order to show that f is injective, it is enough to show that $\ker(f) = \{0\}$. If not, then $\ker(f) = F$. So $1 \in \ker(f)$, i.e., $f(1) = 0$, which is a contradiction. Thus f is injective. The first isomorphism theorem now implies the other part of the problem:

$$F \cong F/\{0\} \cong F/\ker(f) \cong f(F).$$

Solution of the problem 2. Let the ideal $I = \ker(f)$ be the kernel of f, which is principal because $\mathbb{Z}_p$ is a field (F field $\Rightarrow$ every ideal of $F[x]$ is principal) . And let $p(x)$ be a generator for I. By the first isomorphism theorem we know that S is isomorphic to the quotient ring R/I. If $p(x) = 0$ (the zero polynomial), then $I = (p(x)) = (o)$ and hence S is isomorphic to $R/(o) = R$. So, suppose that $p(x)$ is not the zero polynomial, and that it has degree n. We then assert that R/I has at most p^n elements. For this, let $P(x)$ represents a class (mod $p(x)$) in R/I. Using division algorithm, we can write

$$P(x) = p(x)q(x) + r(x);$$

where $r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ is the remainder. We may replace $P(x)$ (as one representative) with $r(x)$. Hence the total number of classes in R/I is $\leq$ the total number of such $r(x)$'s, which is $p \times p \times \cdots \times p = p^n$—each p corresponds to the number of possibilities for each coefficient $a_j \in \mathbb{Z}_p$ $(0 \leq j \leq n-1)$—and we are done.

Solution of the problem 3. This is false. For example, $\mathbb{Z}$ is an integral domain, however, its quotient by the ideal $6\mathbb{Z}$, namely $\mathbb{Z}_6$, is not an integral domain.

Solution of the problem 4. This is true. Let J be an ideal of R/I. Recall that the natural homomorphism $\pi : R \longrightarrow R/I$, $\pi(a) = a + I$, is a surjective ring homomorphism. We now claim that the inverse image $\pi^{-1}(J) := \{a \in R : \ \pi(a) \in J\}$ is an ideal of R:

If $a, b \in \pi^{-1}(J)$, then $\pi(a+b) = \pi(a) + \pi(b) \in J$, so $a + b \in \pi^{-1}(J)$.

If $a \in \pi^{-1}(J), \ r \in R$, then $\pi(ra) = \pi(r)\pi(a) \in J$, so $ra \in \pi^{-1}(J)$.

Every ideal of R is assumed to be principal, so $\pi^{-1}(J) = (a_0) = a_0 R$, for some $a_0 \in R$. Now since π is onto, we conclude that

$$J = \pi(\pi^{-1}(J)) = \pi((a_0 R)) = \{\pi(a_0 r) : \ r \in R\} = \{a_0 r + I : \ r \in R\}$$

$$= \{(a_0 + I)(r + I) : \ r \in R\} = (a_0 + I).$$

This means that J is generated by the element $a_0 + I$. Done.

Solution of the problem 5. False. Let $R = \mathbb{Z}[x]$ and let $I = (x)$, the ideal generated by x. We first claim that $R/I \cong \mathbb{Z}$. To see this, define

$$\phi : R \longrightarrow \mathbb{Z}, \ \phi(f(x)) = f(0).$$

It is apparent that ϕ is a ring homomorphism. ϕ is also surjective (every integer can be regarded as a polynomial). Also note that

$$\ker(\phi) = \{f(x) : \ \phi(f(x)) = 0\} = \{f(x) : \ f(0) = 0\} = \{f(x) : \ x \mid f(x)\} = I.$$

So, $R/I \cong \mathbb{Z}$, and the claim is proved.

Since every ideal of $\mathbb{Z}$ is principal, this in fact shows that every ideal of R/I is so. We now assert that the same is not true for R by showing that the ideal $J = \{f(x) : \ 2 \mid f(0)\}$ is not principal (it is left to you to check that J is in fact an ideal). On the contrary, suppose that J principal and that is generated by some polynomial $g(x)$. Since $2, x \in J$, we would have $g(x) \mid 2, \ g(x) \mid x$. So, $g(x) = \pm 1$ (why?), which is a contradiction (again:why?).

Solution of the problem 6. Our first claim is that for **any prime** p,

$$\frac{\mathbb{Z}[x]}{(p, x^2+1)} \cong \frac{\mathbb{Z}_p[x]}{(x^2+1)}.$$

To see this, define $\phi : \mathbb{Z}[x] \longrightarrow \dfrac{\mathbb{Z}_p[x]}{(x^2+1)}$ by the rule

$$\phi(a_0 + a_1 x + \cdots + a_n x^n) = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n + (x^2+1),$$

where $\bar{a}$ denotes the congruence class of a mod p. It is readily seen that ϕ is a surjective ring homomorphism (check this!). To find the kernel, notice that since any $f(x)$ can be written as $f(x) = a + bx + g(x)(x^2+1)$ for some $g(x)$ (division algorithm), so $f(x)$ is in the kernel $\iff \ \bar{a} + \bar{b}x = 0 \iff p \mid a, p \mid b \iff f(x) \in (p, x^2+1)$. The first isomorphism theorem now concludes the proof of our first claim.

Now we specialize to the case where $p = 5$ or $p = 7$.

(I) For $p = 5$, we have the factorization $x^2 + 1 = (x - 3)(x - 2)$. Let us now define

$$\psi : \mathbb{Z}_5[x] \longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_5, \ \psi(f(x)) = (f(3), f(2)).$$

ψ is clearly a ring homomorphism with the kernel

$$\begin{aligned} \ker(\psi) &= \{f(x) : \ f(3) = f(2) = 0\} \\ &= \{f(x) : \ x - 3 \mid f(x), \ x - 2 \mid f(x)\} \\ &= \{f(x) : \ x^2 + 1 \mid f(x)\} \\ &= (x^2 + 1). \end{aligned}$$

It remains to show that ψ is surjective. Given any $(\alpha, \ \beta) \in \mathbb{Z}_5 \times \mathbb{Z}_5$, take $f(x) = (3\beta - 2\alpha) + (\alpha - \beta)x$. We then have

$$\begin{aligned} \psi(f(x)) &= (f(3), \ f(2)) \\ &= (3\beta - 2\alpha + 3\alpha - 3\beta, \ 3\beta - 2\alpha + 2\alpha - 2\beta) \\ &= (\alpha, \ \beta). \end{aligned}$$

Hence, by the first isomorphism theorem, we deduce that

$$\frac{\mathbb{Z}[x]}{(5, x^2 + 1)} \cong \frac{\mathbb{Z}_5[x]}{(x^2 + 1)} \cong \mathbb{Z}_5 \times \mathbb{Z}_5.$$

(II) Now suppose that $p = 7$. In contrast to 5, $x^2 + 1$ does not factor in $\mathbb{Z}_7[x]$, i.e., it is irreducible. Now we claim that $\dfrac{\mathbb{Z}_7[x]}{(x^2 + 1)}$ is a field. To prove this, we have to show that every nonzero class has an inverse. So, suppose that $f(x) \notin (x^2 + 1)$. Thus $\gcd(f(x), \ x^2 + 1) = 1$, and since $\mathbb{Z}_7$ is a field, we can find $g(x), h(x) \in \mathbb{Z}_7[x]$ so that $f(x)g(x) + h(x)(x^2 + 1) = 1$. Therefore $(f(x) + (x^2 + 1))(g(x) + (x^2 + 1)) = 1 + (x^2 + 1)$. In other words, the class $g(x) + (x^2 + 1)$ is the inverse of $f(x) + (x^2 + 1)$. And finally we count the number of classes in $\dfrac{\mathbb{Z}_7[x]}{(x^2 + 1)}$. Since every class has a unique representative of the form $a + bx + (x^2 + 1)$ with $0 \leq a, b \leq 6$ (could you explain why?), we conclude that the total number of classes is $7 \times 7 = 49$. Done!

Solution of the problem 7. As usual, we define the right map and will exploit it to conclude the desired result. So, consider the

$$\phi : F[[x]] \longrightarrow F, \quad \phi(\sum_{n=0}^{\infty} a_n x^n) = a_0.$$

Now we check in details that ϕ is a surjective ring homomorphism.

(i) ϕ respects addition:

$$\begin{aligned}\phi\left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n\right) &= \phi\left(\sum_{n=0}^{\infty}(a_n+b_n)x^n\right)\\ &= a_0+b_0\\ &= \phi\left(\sum_{n=0}^{\infty} a_n x^n\right)+\phi\left(\sum_{n=0}^{\infty} b_n x^n\right).\end{aligned}$$

(ii) ϕ respects multiplication:

$$\begin{aligned}\phi\left(\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n\right) &= \phi\left(\sum_{n=0}^{\infty}\left(a_0b_n+a_1b_{n-1}+\cdots+a_nb_0\right)x^n\right)\\ &= a_0\cdot b_0\\ &= \phi\left(\sum_{n=0}^{\infty} a_n x^n\right)\cdot\phi\left(\sum_{n=0}^{\infty} b_n x^n\right).\end{aligned}$$

(iii) The identity element of the ring $F[[x]]$ is the formal power series

$$1 = 1 + 0x + 0x^2 + 0x^3 + \cdots,$$

and we have $\phi(1) = 1$.

(iv) ϕ is surjective: for any $a \in F$, we have

$$\phi(a + 0x + 0x^2 + 0x^3 + \cdots) = a.$$

(v) The kernel of ϕ is the ideal generated by x:

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \in \ker(\phi) \iff a_0 = 0 \iff f(x) = xg(x) \iff f(x) \in (x).$$

Therefore, the first isomorphism theorem implies that

$$R = \frac{F[[x]]}{(x)} \cong F.$$

To prove the second part, suppose now that

$$p(x) = \sum_{n=0}^{\infty} a_n x^n \notin (x)$$

which is equivalent to $a_0 \neq 0$. We are looking for a formal power series $q(x) = \sum_{n=0}^{\infty} b_n x^n$ such that

$$p(x)q(x) = 1. \tag{1}$$

Notice that (1) holds if and only if the following system of equations has a solution in b_n's:

$$a_0 b_0 = 1,$$

$$a_0 b_1 + a_1 b_0 = 0,$$

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0,$$

$$\cdots\cdots$$

$$a_0 b_n + \cdots + a_n b_0 = 0,$$

$$\cdots\cdots\cdots\cdots$$

Since $a_0 \neq 0$, there is a solution for b_0, namely $b_0 = a_0^{-1}$. Applying this in the next equation we easily find

$$b_1 = -a_0^{-1}(a_1 b_0).$$

Continuing this way, one can inductively find all b_n's, the only requirement that guarantees the existence of the solutions being $a_0 \neq 0$. So, given any $a_0 + a_1 x + a_2 x^2 + \cdots$ with $a_0 \neq 0$, there exits a (unique) $b_0 + b_1 x + b_2 x^2 + \cdots$ such that their product is 1.

And now the last part is immediate: if an ideal of R is not contained in $I = (x)$, it has to have an invertible element, hence it is the entire ring $F[[x]]$. Done!

Solution of the problem 8a. We show that $R/I \cong \mathbb{R} \times \mathbb{R}$, the direct product of $\mathbb{R}$ with itself. To do this, let us define

$$\phi : R \longrightarrow \mathbb{R} \times \mathbb{R}, \quad \phi(f) = (f(1),\ f(2)).$$

We leave it for the reader to verify that ϕ is a surjective ring homomorphism whose kernel is readily seen to be the given ideal I. Now the first isomorphism theorem yields the affirmation.

Solution of the problem 8b. We show $R/I \cong \mathbb{Z}_n[x]$.
Once again, it is just the matter of defining the right mapping:

$$\phi : R \longrightarrow \mathbb{Z}_n[x], \quad \phi(a_0 + a_1 x + \cdots + a_k x^k) = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_k x^k,$$

where $\bar{a}$ denotes the congruence class of a mod n. The details are left to the reader!

Solution of the problem 8c. Here is the claim: $R/I \cong \mathbb{C}$, the field of complex numbers. To this end, we set

$$\phi : R \longrightarrow \mathbb{C}, \quad \phi(p(x)) = a + bi,$$

where the coefficients a and b are the result of performing the division algorithm

$$p(x) = (x^2 + 1)q(x) + a + bx,$$

and i is the imaginary number $\sqrt{-1}$. It is again(!) a routine matter to check the details!

Solution of the problem 8d. This time the quotient ring R/I is isomorphic to something less familiar! We assert that

$$R/I \cong \mathbb{Z}_{(2)},$$

where $\mathbb{Z}_{(2)}$ (not to be confused with $\mathbb{Z}_2$) stands for the subring of $\mathbb{Q}$ consisting of all rational numbers whose denominator is a power of 2. Coming up with the right mapping is again easy! One defines

$$\phi : R \longrightarrow \mathbb{Z}_{(2)}, \quad \phi(p(x)) = p\left(\frac{1}{2}\right).$$

Note that if $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, then

$$p\left(\frac{1}{2}\right) = \frac{a_0 2^n + a_1 2^{n-1} + \cdots + a_n}{2^n} \in \mathbb{Z}_{(2)}.$$

One readily verifies that ϕ is a surjective ring homomorphism whose kernel is

$$\begin{aligned}
\ker(\phi) &= \{p(x) \in \mathbb{Z}[x] \; : \; p(\tfrac{1}{2}) = 0\} \\
&= \{p(x) \; : \; 2x - 1 \mid p(x)\} \\
&= (2x - 1)\mathbb{Z}[x] \\
&= I.
\end{aligned}$$

The result follows.