MATH 4107 (Prof. Heil) PRACTICE PROBLEMS WITH SOLUTIONS Spring 2018

Here are a few practice problems on rings. **You should first work through these WITHOUT LOOKING at the solutions!** After you write your own solution, you can compare to my solution. Your solution does not need to be identical to mine—there are often many ways to solve a problem—but it does need to be CORRECT.

1. Work out the rule of computation in the ring $\mathbb{R}[x]/(f)$, where $f(x) = x^3 - 1$. Note that the quotient ring consists of elements $a + bx + cx^2 + (f)$.

Solution

For easier notation, let $I = (f)$. Addition is easy:

$$\big(a_1 + b_1x + c_1x^2 + I\big) + \big(a_2 + b_2x + c_2x^2 + I\big) \;=\; (a_1 + a_2) + (b_1 + b_2)x + (c_1 + c_2)x^2 + I.$$

Multiplication is harder. The key fact is that $x^3 - 1$ is in I, so $x^3 - 1 + I = I$. Therefore $x^3 + I = 1 + I$. Similarly,

$$x^4 + I \;=\; xx^3 + I \;=\; \big(x + I\big)\big(x^3 + I\big) \;=\; \big(x + I\big)\big(1 + I\big) \;=\; x + I.$$

Hence,

$$\begin{aligned}
&\big(a_1 + b_1x + c_1x^2 + I\big)\big(a_2 + b_2x + c_2x^2 + I\big) \\
&= a_1a_2 + (b_1a_2 + a_1b_2)x + (c_1a_2 + b_1b_2 + a_1c_2)x^2 + (a_1c_2 + c_1a_2)x^3 + c_1c_2x^4 + I \\
&= a_1a_2 + (b_1a_2 + a_1b_2)x + (c_1a_2 + b_1b_2 + a_1c_2)x^2 + (a_1c_2 + c_1a_2) + c_1c_2x + I \\
&= (a_1a_2 + a_1c_2 + c_1a_2) + (b_1a_2 + a_1b_2 + c_1c_2)x + (c_1a_2 + b_1b_2 + a_1c_2)x^2 + I. \quad \square
\end{aligned}$$

2. Let F be a field. Show that a cubic polynomial in $F[x]$ either has a root in F or is irreducible over F.

Solution

Suppose that f is a cubic polynomial in $F[x]$. If f has a root in F we're done. So, we must show that if f has no root in F, then it is irreducible. I'll prove the contrapositive of this.

If f is reducible, then $f = pq$ with p, $q \in F[x]$ not units (constant polynomials). Since F is a field, the degrees of p and q must sum to the degree of f, which is 3, so one of p or q must have degree 1. So, we can suppose that $p(x) = ax - b$ and q has degree 2 (note that q might actually be further factorizable as a product of two linear polynomials in $F[x]$, or it might be irreducible). In any case, $\alpha = b/a$ is a root of p, and hence is a root of f, and $\alpha \in F$ since a, $b \in F$ (and $a \neq 0$ since otherwise the degree of p wouldn't be 1). Thus, we've shown that reducible implies there is a root in F. $\square$

3. (a) Let $f(x) = ax^{2p} + bx^p + c \in \mathbb{Z}_p[x]$. Let $Df(x)$ be the "derivative" of $f(x)$, i.e., $Df(x)$ is the polynomial $Df(x) = 2pax^{2p-1} + pbx^{p-1}$. Prove that $Df = 0$, the zero polynomial. That is, show that $Df(k) = 0$ for every $k \in \mathbb{Z}_p$.

Solution

The coefficients of this polynomial are elements of $\mathbb{Z}_p$, and in $\mathbb{Z}_p$ we have $2pa = 0$ and $pb = 0$. Therefore $Df(x) = 0x^{2p-1} + 0x^{p-1} = 0$, the zero polynomial. □

(b) State and prove a necessary and sufficient condition for an arbitrary polynomial $f(x) \in \mathbb{Z}_p[x]$ to have $Df = 0$.

Solution

Part (a) of this problem is a hint on how to proceed. It appears that if $f(x)$ has only terms of the form x^{kp}, then its derivative will be zero. Let's state that as our theorem and try to prove it.

Theorem 1. A polynomial $f(x) \in \mathbb{Z}_p[x]$ has $Df = 0$ if and only if

$$f(x) \;=\; a_0 + a_1x^p + a_2x^{2p} + \cdots + a_nx^{np}.$$

Proof. $\Leftarrow$. This argument is exactly the same as the one we gave for part (a) of this problem. That is, if we suppose that $f(x) = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_nx^{np}$, then we can compute the derivative and see that $Df = 0$.

$\Rightarrow$. Suppose that $f(x) \in \mathbb{Z}_p[x]$ has $Df = 0$. Now, we don't know what $f(x)$ is, so let's write it out as $f(x) = b_0 + b_1x + b_2x^2 + \cdots b_mx^m$. We just have to show that $b_j = 0$ except when $j = kp$. We do know that $0 = Df(x) = b_1 + 2b_2x + \cdots + mb_mx^m$. That is, $jb_j = 0$ for $j = 1, \ldots, m$. Note here that j is an integer, while b_j is an element of $\mathbb{Z}_p$. That is, we are saying that adding b_j to itself j times gives zero, i.e., $b_j + b_j + \cdots + b_j = 0$. However, $\mathbb{Z}_p$ is a group under addition. Therefore, if $jb_j = 0$ then the order of b_j must divide j. But since $\mathbb{Z}_p$ has order p, the order of b_j can only be 1 (if $b_j = 0$) or p (if $b_j \neq 0$). Therefore, if $b_j \neq 0$ then p must divide j. Hence b_j must be zero for all j that are not multiples of p. □

4. (i) If F is a field, show that a polynomial in $F[x]$ is a unit if and only if it is a nonzero constant.

Solution

$\Rightarrow$. Suppose that $f(x) \in F[x]$ is a unit. Then there is a polynomial $g(x) \in F[x]$ such that $f(x)g(x) = 1$. Note that this implies that $f(x)$ is not the zero polynomial, hence has a degree $\deg(f) \geq 0$. Now, since F is a domain, we know by Lemma 3.18 that $\deg(fg) = \deg(f) + \deg(g)$, i.e., the degree of the polynomial $f(x)g(x)$ equals the degree of $f(x)$ plus the degree of $g(x)$. However, $f(x)g(x) = 1$, and this polynomial has degree 0! Therefore $\deg(f) + \deg(g) = 0$. But $\deg(f)$ and $\deg(g)$ are both nonnegative numbers, so both these degrees must be zero. Therefore $f(x)$ is a constant polynomial, i.e., $f(x) = a_0$ for some $a_0 \in F$. Since $f(x)$ is nonzero, we must have $a_0 \neq 0$.

$\Leftarrow$. Suppose that $f(x) = a_0$, a nonzero constant. Since F is a field, every nonzero constant in F has an inverse. Therefore we can define $g(x) = a_0^{-1}$, and compute $f(x)g(x) = a_0 a_0^{-1} = 1$. Hence $f(x)$ is a unit in $F[x]$. $\square$

(ii). If R is an integral domain, show that a polynomial in $R[x]$ is a unit if and only if it is a constant that is a unit in R.

Solution

The argument is exactly the same. The only difference is that upon reaching the point $f(x) = a_0$, we further note that we have also shown $g(x) = b_0$ since $\deg(g) = 0$, and that $1 = f(x)g(x) = a_0 b_0$. Therefore a_0 is a unit in R because it has a multiplicative inverse in R. $\square$

(iii). Show that $([2]x + [1])^2 = [1]$ in $\mathbb{Z}_4[x]$. Conclude that the hypothesis in (ii) that R be a domain is necessary.

Solution

The point is that that if R isn't a domain, then there may be nonconstant polynomials that are units. Let's just check the example that they give. Computing in $\mathbb{Z}_4[x]$, we have

$$\begin{aligned} ([2]x + [1])^2 &= ([2]x + [1])([2]x + [1]) \\ &= [2][2]x^2 + [2][1]x + [1][2]x + [1][1] \\ &= [4]x^2 + [4]x + [1] \\ &= [1], \end{aligned}$$

since $[4] = [0]$ in $\mathbb{Z}_4$. Thus the polynomial $[2]x + [1]$ is a unit in $\mathbb{Z}_4[x]$, since it equals its own multiplicative inverse. $\square$