MATH 3032: Abstract Algebra

Assignment 3 Solutions

1. **Let R be a *finite* unital ring. Show that every element of R is either a unit or a *left zero-divisor*, an element $a \in R$ such that there exists $b \neq 0$ such that $ab = 0$ [if R is noncommutative, then this might be different from being a right zero-divisor]. Explain why an element cannot be both a unit and a left zero-divisor except for one possible ring R [which one?]. Explain why the main statement implies that in a *finite* unital ring, the set of left zero-divisors is equal to the set of right zero-divisors.**

   Hint: Explain that if $r \in R$ is *not* a left zero-divisor if and only if left-multiplication by r is injective. Now use finiteness of R.

   Suppose that $ab = 0$ and that a is invertible. Then $b = 1b = a^{-1}ab = a^{-1}0 = 0$. So a left zero-divisor cannot be a unit. *Note: there is an error in the question.*

   Now suppose that R is finite. Then multiplication $a \times (-) : R \to R$ is a map from R to itself. The distributive law says that this is a map of additive groups. The b for which $ab = 0$ are precisely the kernel of $a \times (-)$, so a is a zero-divisor iff this map has a nontrivial kernel iff this map is not injective. But this is a map on a *finite* set, so it is injective iff it is surjective (pigeon hole!) iff it is bijective. But if it is bijective, then we can find a preimage of 1, which will be a right-inverse of a, so let's tentatively call it a^{-1}. So the function $a^{-1} \times (-) : R \to R$ is a right-inverse to the function $a \times (-)$. But this function was invertible, so its right-inverse is also its left-inverse. So $a^{-1}a \times (-) = \mathrm{id}$, and evaluating at 1 gives that a^{-1} is also a left-inverse to a, so that $a \in R$ is invertible.

2. (a) **Does $\mathbb{Z}_4[x]$ contain a non-constant polynomial which is a unit? Either give an example of one or prove that none exists.**

   Yes. $1 + 2x$ is an example. Indeed, $(1 + 2x)^2 = 1 + 4x + 4x^2 \equiv 1 \pmod 4$.

   (b) **Does $\mathbb{Z}_6[x]$ contain a non-constant polynomial which is a unit? Either give an example of one or prove that none exists.**

   No. A fast way to show this is to reduce further, working mod 2 and mod 3. So suppose that $f(x) \in \mathbb{Z}_6[x]$ is invertible. Then $(f \mod 2)$ is invertible in $\mathbb{Z}_2[x]$, and so a constant (namely the constant 1), so all the coefficients of f other that the constant value are even. But $(f \mod 3)$ is invertible in $\mathbb{Z}_3[x]$, so all the coefficients of f other than the constant value are divisible by 3. But a number which is even and divisible by 3 is divisible by 6. So $f(x) \in \mathbb{Z}_6[x]$ is a constant.

3. **Define the *formal derivative* $\partial_x : R[x] \to R[x]$ to be the operation $\sum_n a_n x^n \mapsto \sum_n n a_n x^{n-1} = \sum_n (n+1) a_{n+1} x^n$.**

   (a) **Is ∂_x a homomorphism of additive groups? Is ∂ a homomorphism of rings?**

   ∂_x is a homomorphism of additive groups, since addition in $R[x]$ is done coefficient-by-coefficient and for each n, and for every additive group A, the function $a \mapsto na$ is a homomorphism of additive groups. ∂_x is not a homomrophism of rings: $\partial_x(x^2) = 2x \neq (\partial_x x)^2 = 1$.

(b) **What is the kernel of $\partial_x : \mathbb{Z}[x] \to \mathbb{Z}[x]$?**
If $a_n \neq 0$ for some $n \geq 0$, then $\partial_x \sum a_n x^n$ will contain a term like $n a_n x^{n-1} \neq 0$. So the kernel consists just of the constant polynomials. We have used that a polynomial is zero iff all of its coefficients are.

(c) **What is the kernel of $\partial_x : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$?**
Working mod p, there is a kernel: $\partial_x x^{mp} = mp x^{mp-1} = 0$. This is the only kernel: if n is not divisible by p, then it is invertible mod p, so $n a_n x^{n-1} = 0$ would imply $a_n = 0$. In other words, $\ker(\partial_x : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]) = \mathbb{Z}_p[x^p]$.

(d) **What is its image of $\partial_x : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$?**
From the previous analysis, we see that x^k can be produced by ∂_x if $k + 1 \neq mp$, but not when $k + 1 = mp$. So the image is the set of polynomials of the form

$$\sum_{n \not\equiv -1 \pmod p} a_n x^n.$$

4. **For each of the following pairs $f, g \in R[x]$, use long division to write $f = qg + r$ with $\deg r < \deg g$. You should do the work by hand and show your work, but you do not need to write any words of explanation.**

(a) $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ **and** $g(x) = x^2 + 2x - 3$ **in** $\mathbb{Z}[x]$

$$\begin{array}{rrr|rrrrrrr}
 & & & x^4 & +x^3 & +x^2 & +x & +5 & & \\ \cline{4-10}
x^2 & +2x & -3 & x^6 & +3x^5 & +0x^4 & +0x^3 & +4x^2 & -3x & +2 \\
 & & & x^6 & +2x^5 & -3x^4 & & & & \\ \cline{4-6}
 & & & & x^5 & +3x^4 & +0x^3 & & & \\
 & & & & x^5 & +2x^4 & -3x^3 & & & \\ \cline{5-7}
 & & & & & x^4 & +3x^3 & +4x^2 & & \\
 & & & & & x^4 & +2x^3 & -3x^2 & & \\ \cline{6-8}
 & & & & & & x^3 & +7x^2 & -3x & \\
 & & & & & & x^3 & +2x^2 & -3x & \\ \cline{7-9}
 & & & & & & & 5x^2 & +0x & +2 \\
 & & & & & & & 5x^2 & +10x & -15 \\ \cline{8-10}
 & & & & & & & & -10x & +17
\end{array}$$

So $q = x^4 + x^3 + x^2 + x + 5$ and $r = -10x + 17$.

(b) $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ **and** $g(x) = 3x^2 + 2x - 3$ **in** $\mathbb{Z}_7[x]$**.**
Note: $3^{-1} = 5$ in $\mathbb{Z}_7$.

$$\begin{array}{rrr|rrrrrrr}
 & & & 5x^4 & & +5x^2 & -x & & & \\ \cline{4-10}
3x^2 & +2x & -3 & x^6 & +3x^5 & +0x^4 & +0x^3 & +4x^2 & -3x & +2 \\
 & & & x^6 & +3x^5 & -1x^4 & & & & \\ \cline{4-6}
 & & & & 0 & +x^4 & +0x^3 & +4x^2 & & \\
 & & & & & x^4 & +3x^3 & -x^2 & & \\ \cline{6-8}
 & & & & & & -3x^3 & +5x^2 & -3x & \\
 & & & & & & -3x^3 & -2x^2 & +3x & \\ \cline{7-9}
 & & & & & & & 0 & +x & +2
\end{array}$$

So $q = 5x^4 + 5x^2 - x$ and $r = x + 2$.