Abstract Algebra I - Lecture 26

Adam Chapman

Department of Mathematics, Michigan State University, East Lansing, MI 48824

Review for Midterms Exam 2.

Exercise.
Find the inverse of $2x + 7$ in $\mathbb{Q}[x]/(x^2 - 12)$.
Solution.

$$x^2 - 12 = (2x + 7)(\frac{1}{2}x - \frac{7}{4}) + \frac{1}{4}$$
$$\frac{1}{4} = (x^2 - 12) + (\frac{7}{4} - \frac{1}{2}x)(2x + 7)$$
$$1 = 4(x^2 - 12) + (7 - 2x)(2x + 7)$$

so the inverse of $2x + 7$ is $7 - 2x$.
Exercise.
Find $\gcd(x^4 + x^2 + 1, x^3 + x^2 + x)$ in $\mathbb{Z}_2[x]$.
Solution.

$$x^4 + x^2 + 1 = (x + 1)(x^3 + x^2 + x) + x^2 + x + 1$$
$$x^3 + x^2 + x = x(x^2 + x + 1)$$

so $\gcd(x^4 + x^2 + 1, x^3 + x^2 + x) = x^2 + x + 1$.
Exercise.
Say if the following polynomials are irreducible:

- $x^2 + 1$ in $\mathbb{Z}_2[x]$.
- $x^2 + 1$ in $\mathbb{Z}_3[x]$.

Email address: adam1chapman@yahoo.com (Adam Chapman)

Preprint submitted to Elsevier *October 31, 2015*

- $x^2 + 1$ in $\mathbb{R}[x]$.
- $x^2 + 1$ in $\mathbb{C}[x]$.

Solution.
Note that a polynomial in $F[x]$ of degree 2 has a root in F if and only if it is reducible.

The polynomial $f(x) = x^2 + 1 \in \mathbb{Z}_2[x]$ has a root in $\mathbb{Z}_2$: $f(1) = 1 + 1 = 0$, so it is reducible.

The polynomial $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ has no root in $\mathbb{Z}_2$: $f(0) = 0 + 1 = 1, f(1) = 1 + 1 = 2, f(2) = 2^2 + 1 = 1 + 1 = 2$, so it is irreducible.

The polynomial $f(x) = x^2 + 1 \in \mathbb{R}[x]$ has no root because its discriminant is $-4 < 0$, so it is irreducible.

The polynomial $f(x) = x^2 + 1 \in \mathbb{C}[x]$ has a root: $f(i) = i^2 + 1 = -1 + 1 = 0$, so it is reducible.

Exercise.
What is the additive order of $[72]$ in $\mathbb{Z}_{45}$?

Solution.
The additive order of $[m]$ in $\mathbb{Z}_n$ is $\frac{n}{\gcd(m,n)}$. Now $72 = 2^3 \cdot 3$ and $45 = 3^2 \cdot 5$, so $\gcd(72, 45) = 3$. Consequently the additive order of $[72]$ in $\mathbb{Z}_{45}$ is $\frac{45}{3} = 15$.

Exercise.
Find the multiplicative order of $[2]$ in $\mathbb{Z}_9$.

Solution.
We know that if $\gcd(m, n) = 1$ then $[m]$ is invertible in $\mathbb{Z}_n$ and $[m]^{\varphi(n)} = [1]$. Therefore the multiplicative order of $[m]$ in $\mathbb{Z}_n$ in that case divides $\varphi(n)$.

In this case, $\varphi(9) = 6$, so the possible orders are $2, 3$ and 6. (Note that by definition, the identity is the unique element whose multiplicative order is 1.)

$[2] \cdot [2] = [4]$ so the order is not 2. $[2] \cdot [2] \cdot [2] = [8]$ so the order is not 3. Therefore the order is 6.

Exercise.
Is $f : \mathbb{R} \times \mathbb{R} \to M_2(\mathbb{R})$, $f(a, b) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ a homomorphism? Is it injective? Is it surjective?

Solution.
It is a homomorphism: $f((a_1, b_1)+(a_2, b_2)) = f(a_1+a_2, b_1+b_2) = \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & b_1 + b_2 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = f(a_1, b_1)+f_(a_2, b_2)$ and $f((a_1, b_1)\cdot(a_2, b_2)) = f(a_1a_2, b_1b_2) =$

$$\begin{pmatrix} a_1a_2 & 0 \\ 0 & b_1b_2 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = f(a_1, b_1) + f_(a_2, b_2).$$

It is injective: If $\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}$ then $a_1 = a_2$ and $b_1 = b_2$, which means $(a_1, b_1) = (a_2, b_2)$.

It is not surjective, e.g. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is not in the image of f.