

392 HOMEWORK 7 SOLUTIONS

- Exercises 4.1: 6, 18(a)(b)(c)

6 Prove that $\phi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, a \mapsto a^p$ is a ring homomorphism.

Solution. Obviously 1 goes to 1. Also, $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$. So it is multiplicative. The hard thing is additivity.

$$\phi(a) + \phi(b) = a^p + b^p,$$

and

$$\phi(a + b) = (a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

We need to show these are equal. This follows because $\binom{p}{k} = 0$ in \mathbb{Z}_p for each $k = 1, \dots, p-1$, i.e. the inside numbers on the p th row of Pascal's triangle are all divisible by p providing p is prime. We proved that last week when we were discussing the irreducibility of $x^{p-1} + x^{p-2} + \cdots + x + 1$.

Note this shows that $(a + b)^p = a^p + b^p$ in \mathbb{Z}_p – this is known as the “Freshman's dream” – wouldn't it be nice if that was what the binomial theorem said in general!

- 18(a) Find the nilpotent elements in \mathbb{Z}_n for $n = 6, 12, 8, 36$.

Solution.

The nilpotents in \mathbb{Z}_6 are 0 only.

The nilpotents in \mathbb{Z}_{12} are 0, 6 only.

The nilpotents in \mathbb{Z}_8 are 0, 2, 4, 6 only.

The nilpotents in \mathbb{Z}_{36} are 0, 12, 24, 18, 30, 6. Note the easiest way to do this is to use the isomorphism $\mathbb{Z}_{36} \cong \mathbb{Z}_4 \times \mathbb{Z}_9$ we just proved in class. The nilpotents in the latter ring are the pairs (a, b) where a is nilpotent in \mathbb{Z}_4 , i.e. $a = 0, 2$, and b is nilpotent in \mathbb{Z}_9 , i.e. $b = 0, 3, 6$. So there are 6 in total, $(0, 0), (0, 3), (0, 6), (2, 0), (2, 3), (2, 6)$. Now we find the numbers in \mathbb{Z}_{36} that correspond to these under the isomorphism to get the answer.

- 18(b) Find the nilpotent elements in $\mathbb{Q}[x]/(x^2)$.

Solution. Suppose $\overline{ax + b} \in \mathbb{Q}[x]/(x^2)$ is nilpotent. Then for some n , the binomial theorem gives us that

$$(ax + b)^n = \binom{n}{n-1} axb^{n-1} + b^n = 0$$

in $\mathbb{Q}[x]/(x^2)$. But that means that $b = 0$. Hence, the nilpotents are exactly the elements \overline{ax} for $a \in \mathbb{Q}$.

- 18(c) Prove that the set N of nilpotent elements of a ring R is an ideal.

Solution. It is easy to see that N contains 0 and is extra-closed under multiply. The difficult thing is to see it is closed under

addition. So let $a, b \in N$. Then, for some $m, n \geq 1$, we have that $a^m = b^n = 0$. Consider

$$(a + b)^{m+n} = a^{m+n} + \dots + \binom{m+n}{k} a^{m+n-k} b^k + \dots + b^{m+n}.$$

I claim it is zero. To see this, look at the k th term $\binom{m+n}{k} a^{m+n-k} b^k$ of the binomial expansion. If $k \geq n$ it is zero because $b^n = 0$. If $k \leq n$ then $m+n-k \geq m$ so a^{m+n-k} is zero because $a^m = 0$.

Hence, $(a + b)$ is nilpotent.

- Exercises 4.2: 3(e) Show that $F[x]/(x) \cong F$.

Solution. Let $\phi : F[x] \rightarrow F$ be the evaluation homomorphism $f(x) \mapsto f(0)$. It is onto, and the kernel is generated by the minimal polynomial of 0 over F , namely, the polynomial x . Hence, $F[x]/(x) \cong F$ by the isomorphism theorem.

- Exercises 3.3: 3(b)(d), 8, 10.

- 3(b) Find the rational roots of $x^5 - x^4 - x^3 - x^2 - x - 2$.

Solution. Since it's monic with integer coefficients, rational roots are integers. So we need only to think about the integer roots. For $x \geq 8$ for example clearly the term x^5 dominates all the others and it is positive. Similarly for $x \leq -8$ it is negative. Now search $-7, \dots, -1, 0, 1, \dots, 7$ by hand to see if they are roots. You deduce the only zero is at $x = 2$.

- 3(d) Same thing for $x^3 + x^2 - 2x - 3$.

Solution. Again we need to look for integer roots. A similar search shows this has no zeros. (Or you can find the turning points and sketch the graph!)

- 8 Let p be a prime. (a) Prove that $x^p - x$ has p distinct roots in $\mathbb{Z}_p[x]$. (b) Prove that $x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1))$ in $\mathbb{Z}_p[x]$. (c) Prove that $(p-1)! \equiv -1 \pmod{p}$.

Solution. (a) By Proposition 3.3 of chapter 1, $a^p = a$ for every a in \mathbb{Z}_p . Hence the numbers $0, 1, \dots, p-1$ are all roots of the equation $x^p - x$, so it has p distinct roots.

(b) Dividing by x we deduce that the numbers $1, \dots, p-1$ are all roots of the equation $x^{p-1} - 1$ over \mathbb{Z}_p . Hence it factors as $(x-1)(x-2)\dots(x-(p-1))$ in $\mathbb{Z}_p[x]$.

(c) Now compute the constant term on both sides of the equation proved in (b) to see that $-1 = (-1)^{p-1}(p-1)!$ hence $(p-1)! = (-1)^p$ in \mathbb{Z}_p . Since $(-1)^p = -1$ in \mathbb{Z}_p we are done.

- 10 Let $f(x) = x^4 - 10x^2 + 1$. Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$ but reducible in $\mathbb{Z}_p[x]$ for every prime p .

Solution. First let us show it is irreducible in $\mathbb{Q}[x]$. Its roots are $x = \pm\sqrt{5} \pm 2\sqrt{6}$ (all of which are real). Since none is rational, it has no linear factors in \mathbb{Q} . But it could factor as a product of two irreducible quadratics gotten by pairing up these four roots

in some way But in that case, either

$$(x - \sqrt{5 + 2\sqrt{6}})(x + \sqrt{5 + 2\sqrt{6}})$$

or

$$(x - \sqrt{5 + 2\sqrt{6}})(x + \sqrt{5 - 2\sqrt{6}})$$

or

$$(x - \sqrt{5 + 2\sqrt{6}})(x - \sqrt{5 - 2\sqrt{6}})$$

would have to belong to $\mathbb{Q}[x]$. Multiplying them out in each case you see that is not the case.

Now we show it is reducible in $\mathbb{Z}_p[x]$ for each prime p . We know by the hint that either 2, 3 or 6 is a square in \mathbb{Z}_p .

Suppose first that 6 is a square in \mathbb{Z}_p . Say $k^2 \equiv 6 \pmod{p}$.

Then,

$$x^4 - 10x^2 + 1 = (x^2 - 5)^2 - 24 = (x^2 - 5)^2 - (2k)^2 = (x^2 - 5 - 2k)(x^2 - 5 + 2k)$$

so it is reducible.

Suppose next that 3 is a square in \mathbb{Z}_p . Say $k^2 \equiv 3 \pmod{p}$.

Then

$$x^4 - 10x^2 + 1 = (x^2 + 1)^2 - 12x^2 = (x^2 + 1)^2 - (2kx)^2 = (x^2 - 2kx + 1)(x^2 + 2kx + 1)$$

so it is reducible.

Finally suppose that 2 is a square in \mathbb{Z}_p . Say $k^2 \equiv 2 \pmod{p}$.

Then,

$$x^4 - 10x^2 + 1 = (x^2 - 1)^2 - 8x^2 = (x^2 - 1)^2 - (2kx)^2 = (x^2 - 2kx - 1)(x^2 + 2kx - 1).$$

Either way it is reducible.