MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Homework Sheet 9
Due: Wednesday 28th November: 3:30 PM

Basic Questions

1. *Factorise* $f(x) = x^4 + 3x^3 + 2x^2 + 9x - 3$*:*

   (a) over $\mathbb{Z}_3$*.*

   Over $\mathbb{Z}_3$, we see that $f(0) = 0$, $f(1) = 0$, $f(2) = 0$, so we see that $f(x)$ factorises as $f(x) = x^2(x-1)(x-2)$.

   (b) over $\mathbb{Z}_6$*.*

   Over $\mathbb{Z}_6$, we see that $f(0) = 3$, $f(1) = 0$, $f(2) = 3$, $f(3) = 0$, $f(4) = 3$, and $f(5) = 0$, so we deduce that $f(x) = (x-1)(x-5)(x-3)^2$.

   (c) over $\mathbb{Z}$*.*

   Suppose that we can factor f over $\mathbb{Z}$. Then we must have the product of the constant terms in the factors equal to -3. Therefore, when we consider the factors in $\mathbb{Z}_6$, only one of them can have constant term divisible by 3. Therefore, the only possible factorisations in $\mathbb{Z}_6$ must have both $(x-3)$ terms in the same factor. If we had a linear factor, it would need to be $x \pm 1$, but these are not factors, since $f(1) = 12$ and $f(-1) = -12$. Therefore, if f factors over $\mathbb{Z}$, then it must be as a product of two quadratics, one of which is congruent to $(x-3)^2$, and the other of which is congruent to $(x-1)(x-5)$, modulo 6. That is, one factor must be $x^2 - 1 + 6ax$, and the other factor must be $x^2 + 3 + 6bx$. Now by multiplying these factors, we get $x^4 + 3x^3 + 2x^2 + 9x - 3 = x^4 + 6(a+b)x^3 + (2 + 36ab)x^2 + 6(3a-b)x - 3$. This gives $(a+b) = \frac{3}{6} = \frac{1}{2}$, which is not possible, so f is irreducible over $\mathbb{Z}$.

2. *Show that* $f(x) = x^4 + x^3 + x^2 + x + 1$ *is irreducible over* $\mathbb{Z}$*. [Hint: consider* $x = y + 1$ *and use Eisenstein's criterion.]*

   If we substitute $x = y+1$, then we see that $f(x) = (y+1)^4 + (y+1)^3 + (y+1)^2 + (y+1) + 1 = y^4 + 5y^3 + 10y^2 + 10y + 5 = g(y)$, which is an irreducible polynomial in y by Eisenstein's criterion. However, if $f(x)$ were reducible, then the same substitution $x = y+1$ would provide a factorisation of $g(y)$, which is impossible.

   Alternatively: observe that $(x-1)f(x) = x^5 - 1$, so $g(y) = \frac{(y+1)^5 - 1}{y} = y^4 + 5y^3 + 10y^2 + 10y + 5$. [This method allows the result to be generalised to any other prime instead of 5.]

3. *Find all solutions to the equation $x^2 + 2x - 3 = 0$ in $\mathbb{Z}_{21}$.*

   We can factor $f(x) = x^2 + 2x - 3$ as $f(x) = (x-1)(x+3)$. We therefore want to solve $(x-1)(x+3) = 0$ in $\mathbb{Z}_{21}$. There are the obvious solutions $x = 1$ and $x = -3 = 18$, but we also have the non-trivial zero products, where one factor is divisible by 3 and the other is divisible by 7. We consider the four cases:

   $x + 3 = 7$: $x = 4$, $x - 1 = 3$ is divisible by 3, so this is a solution.

   $x - 1 = 7$: $x = 8$, $x + 3 = 11$ is not divisible by 3, so this is not a solution.

   $x - 1 = 14$: $x = 15$, $x + 3 = 18$ is divisible by 3, so this is a solution.

   $x + 3 = 14$: $x = 11$, $x - 1 = 10$ is not divisible by 3, so this is not a solution.

   Therefore, the solutions are $x = 1$, $x = 4$, $x = 15$ and $x = 18$.

4. *Find all prime numbers p such that $x - 4$ is a factor of $x^4 - 2x^3 + 3x^2 + x - 2$ in $\mathbb{Z}_p[x]$.*

   $x - 4$ is a factor of $f(x)$ if and only if $f(4) = 0$, so we need to find all primes p such that $f(4) = 4^4 - 2 \times 4^3 + 3 \times 4^2 + 4 - 2 = 178 \equiv 0 \pmod{p}$. That is, we need all prime factors of 178, which are 2 and 89.

5. *Find a generator for the multiplicative group of non-zero elements of $\mathbb{Z}_{19}$.*

   We know that there are 18 non-zero elements in $\mathbb{Z}_{19}$, so we are looking for an element of order 18 in this group. The prime factors of 18 are 2 and 3 (repeated twice), so a non-zero element of $\mathbb{Z}_{19}$ generates the multiplicative group of non-zero elements if and only if it does not occur as a square or a cube. We calculate the following in $\mathbb{Z}_{19}$:

x	x^2	x^3
1	1	1
2	4	8
3	9	8
4	16	7
5	6	11
6	17	7
7	11	1
8	7	18
9	5	7
10	5	12
11	7	1
12	11	18
13	17	12
14	6	8
15	16	12
16	9	11
17	4	11
18	1	18

So the generators are 2, 3, 10, 13, 14, and 15.

6. *Show that $f(x) = x^2 + 3x + 2$ does not factorise uniquely over $\mathbb{Z}_6$.*

   In $\mathbb{Z}_6$, we have $(x+1)(x+2) = f(x) = (x+4)(x+5)$, so the factorisation is not unique.

7. *Show that $f(x) = x^3 + 4x^2 + 1$ is irreducible in $\mathbb{Z}_7$. [Hint: if it is not irreducible then it must have a linear factor.]*

   Since $f(x)$ is cubic, then if it is not irreducible, then one of the factors must be linear. But by the factor theorem, $f(x)$ must have a zero in $\mathbb{Z}_7$. However, we have:

x	$f(x)$
0	1
1	6
2	4
3	1
4	3
5	2
6	4

   So we see that f has no zeros, and is therefore irreducible.

Standard Questions

8. *Show that if D is an integral domain, then so is $D[x]$.*

   We already know that $D[x]$ is a commutative ring, and the constant unity function is the unit element, so we just need to show that $D[x]$ has no zero divisors. Suppose we have $f(x)g(x) = 0$ in $D[x]$, then let $f(x) = a_1x^n + a_2x^{n-1} + \cdots + a_{n-1}x + a_n$, and $g(x) = b_1x^m + b_2x^{m-1} + \cdots + b_{m-1}x + b_m$. Now let a_i and b_j be the last non-zero coefficients. That is $a_i \neq 0$, but $a_k = 0$ for all $k > i$, and $b_j \neq 0$, but $b_k = 0$ for all $k > j$. Now since $f(x)g(x) = 0$, we must have that the coefficient of $x^{n+m+2-i-j}$ is zero. However, this coefficient is a_ib_j, so a_i and b_j must be zero-divisors in D, contradicting the assumption that D is an integral domain.

9. *Let R be a ring. (a) Show that the ring of functions from R to R is a ring with pointwise addition and multiplication. That is:*

$$(f+g)(x) = f(x) + g(x)$$
$$fg(x) = f(x)g(x)$$

We need to check the axioms. These all follow from the corresponding axioms for R. For example, 0 is the constantly 0 function. $(-f)(x) = -(f(x))$. The axioms are all straightforward to check — for example, we check associativity and commutativity of + and distributivity of multiplication over addition:

- Commutativity: $(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$
- Associativity: $((f+g)+h)(x) = (f+g)(x)+h(x) = (f(x)+g(x))+h(x)) = f(x)+(g(x)+h(x)) = f(x)+(g+h)(x) = (f+(g+h))(x)$
- Distributivity: $(f(g+h))(x) = f(x)(g+h)(x) = f(x)(g(x)+h(x)) = f(x)g(x)+f(x)h(x) = fg(x)+fh(x) = (fg+fh)(x)$

(b) Show that the set of all functions describable by polynomials gives a subring of the ring of all functions.

We need to show that the functions describable by polynomials are closed under addition, multiplication and additive inverse, and include the constantly 0 function.

The constantly 0 function is describable by the 0 polynomial. The sum $f+g$ is describable by the sum of polynomials describing f and g; the additive inverse of f is describable by the additive inverse of a polynomial describing f, and the product is describable by the product of polynomials describing f and g.

(c) Show that this ring is not always isomorphic to the polynomial ring $R[x]$. [Hint: let R be a finite field $\mathbb{Z}_p$ for some prime p.]

If R is a finite field with n elements, then the number of functions from R to R is finite with n^n elements, while the number of elements in the polynomial ring $R[x]$ is infinite, so the two rings cannot be isomorphic.

10. *Show that the remainder when a polynomial $f(x) \in F[x]$ is divided by $x-a$ is $f(a)$.*

Consider $g(x) = f(x) - f(a)$. Clearly, $g(a) = 0$, so $x-a$ is a factor of $g(x)$. Let $g(x) = (x-a)h(x)$. Now we have $f(x) = (x-a)h(x) + f(a)$ as required.

Bonus Questions