MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Midyear Examination
Friday 7th December: 7:00-10:00 PM

Basic Questions

1. *Compute the factor group* $\mathbb{Z}_3 \times \mathbb{Z}_9/\langle(1,6)\rangle$.

   The subgroup generated by $(1,6)$ is $\{(1,6),(2,3),(0,0)\}$, so the factor group has $\frac{27}{3} = 9$ elements. It must also be abelian, so it is either $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$. We need to check whether the factor group has an element of order 9. Consider $[(0,1)]$: it is easy to see that the cube of this is $[(0,3)]$, which is not the identity coset. Therefore, this element does not have order 3 in the factor group. Therefore, the factor group is isomorphic to $\mathbb{Z}_9$.

2. *Are the following rings: Justify your answers.*

   (a) The integers with the usual addition, and multiplication given by $a * b$ *is the least common multiple of* a *and* b.

   This is not a ring because multiplication does not distribute over addition. For example $3 * (2 + 1) = 3 * 3 = 3$, but $3 * 2 + 3 * 1 = 6 + 3 = 9$.

   (b) The positive integers with addition given by $a+b$ *is the greatest common divisor of* a *and* b*, and multiplication given by* $a * b$ *is the least common multiple of* a *and* b.

   This is not a ring because it is not a group under $+$ — there is no identity element for greatest common divisor. [If we include 0, then that is an identity element, but we don't have inverses, since 0 is not the greatest common divisor of any two numbers.

3. *Let* P *be the ring of subsets of a set* X *with 5 elements, with addition given by symmetric difference and multiplication given by intersection. [The symmetric difference of two sets* A *and* B *is the set of elements that occur in exactly one of them.] Is* P *an integral domain? (Justify your answer.) [You may assume that* P *is a ring.]*

   P is not an integral domain, because for example if $X = \{1,2,3,4,5\}$, we have that $\{1\} \cap \{2\} = \emptyset$.

4. *What are the units in the ring* $\mathbb{Z}_{15}$*?*

   The units in this ring are numbers coprime to 15, i.e. $\{1,2,4,7,8,11,13,14\}$.

5. *Show that the set of numbers of the form* $a+b\sqrt{5}$ *where* a *and* b *are rational numbers is a field.*

It is clear that this set is closed under addition, multiplication, since $(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (ad + bc)\sqrt{5}$, and additive inverses, and so it is a subring of the real numbers, so it is a commutative ring. It clearly contains the unity, so we just need to show it is closed under multiplicative inverses. We have that $\frac{1}{a+b\sqrt{5}} = \frac{a}{a^2-5b^2} - \frac{b}{a^2-5b^2}\sqrt{5}$, so it is closed under multiplicative inverses, so it is a field.

6. *Factorise* $x^4 + 5x^3 + 3x^2 - 3x - 18$

   (a) over $\mathbb{Z}_6$.

   Looking for zeros, we see

x	$x^4 + 5x^3 + 3x^2 - 3x - 18$
0	0
1	0

   So we know that x and $x - 1$ are factors. Dividing through, we see $x^4 + 5x^3 + 3x^2 - 3x - 18 = x(x - 1)(x^2 + 3)$ in $\mathbb{Z}_6$.

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

   Substituting $x = y+2$, we get $f(x) = (y+2)^4-(y+2)^3+3(y+2)^2+3(y+2)+2 = y^4 + 7y^3 + 21y^2 + 35y + 28$. Therefore by Eisenstein's criterion with $p = 7$, this is irreducible.

8. *Find all solutions to the equation* $x^2 - 9x + 14 = 0$ *in* $\mathbb{Z}_{42}$.

   Trying a few values:

x	$x^2 - 9x + 14$
0	14
1	6
2	0

   We see that 2 is a zero. This allows us to factorise the polynomial as $(x - 2)(x - 7)$. This immediately gives that 2 and 7 are zeros. Also, we can get zeros by setting $x-2$ and $x-7$ to zero divisors. $41 = 2 \times 3 \times 7$, so we need to look at multiples of these numbers which differ by 5. Looking at all the cases, we get the following zeros.

$x-2$	$x-7$	x
0	-5	2
5	0	7
21	16	23
14	9	16
35	30	37
12	7	14
33	28	35
26	21	28

9. *Show that* $f(x) = x^3 - 2x^2 + 2$ *is irreducible in* $\mathbb{Z}_5$.

If it is irreducible, it must have a linear factor, so it must have a zero. We try all possibilities:

x	$x^3 - 2x^2 + 2$
0	2
1	1
2	1
3	3
4	4

Therefore f has no zeros, so it is irreducible.

10. *Find the remainder when 8^{1025} is divided by 17.*

    We know that $8^{16} \equiv 1 \pmod{17}$, so $8^{1024} \equiv 1 \pmod{17}$. Therefore $8^{1025} \equiv 8 \pmod{17}$, so the remainder is 8.

11. *Find the remainder when $2^{3^{4^{5^{6^{7^{8^{9}}}}}}}$ is divided by 11.*

    We know that $2^{10} \equiv 1 \pmod{11}$, so we need to find $3^{4^{5^{6^{7^{8^{9}}}}}}$ modulo 10. We know that $3^4 \equiv 1 \pmod{10}$, so $3^{4^{5^{6^{7^{8^{9}}}}}} \equiv 1 \pmod{10}$, so $2^{3^{4^{5^{6^{7^{8^{9}}}}}}} \equiv 2^1 \equiv 2 \pmod{11}$.

12. *Solve:*

    (a) $21x \equiv 22 \pmod{33}$

    21 and 33 are both divisible by 3, but 22 is not, so this has no solutions.

    (b) $2x \equiv 6 \pmod{21}$

    2 and 21 are coprime so this has a unique solution, which is $x = 3$.

Theoretical Questions

13. *Let H be a subgroup of G. Show that $N_G(H) = \{x \in G | xHx^{-1} = H\}$ is a subgroup of G, and contains H as a normal subgroup.*

    We first need to show that $N_G(H)$ is a subgroup.

    - Let $x, y \in N_G(H)$. Now $xyH(xy)^{-1} = xyHy^{-1}x^{-1} = xHx^{-1} = H$, so $xy \in N_G(H)$.
    - Let $x \in N_G(H)$. Then $xHx^{-1} = H$, so $xH = Hx$ and so $H = x^{-1}Hx$. Therefore $x^{-1} \in N_G(H)$.
    - Clearly $e \in N_G(H)$.

    Next we need to show that H is a normal subgroup of $N_G(H)$, but this is automatic by the definition of $N_G(H)$. Finally we need to show that H is contained in $N_G(H)$. For $h \in H$, we clearly have $hHh^{-1} = H$, since H is a subgroup of G.

14. Show that the intersection of two subrings of a ring is a ring.

The characteristic of a field must be prime or 0. Let F be a field with 6 elements. The additive subgroup generated by 1 must have 1, 2, 3, or 6 elements. It can't have 1 or 6 elements, since the characteristic of F is prime. Suppose F has characteristic 3. Now all the non-zero elements can be partitioned into pairs of the form $\{x, 2x\}$. However, there are 5 non-zero elements, so this is not possible. Therefore, F must have characteristic 2. However, the additive group of F is an abelian group with 6 elements, so must be isomorphic to $\mathbb{Z}_6$, or $\mathbb{Z}_2 \times \mathbb{Z}_3$. However, either possibility involves an element of order 3, but this contradicts characteristic 2.

15. Show that there is no field with exactly 6 elements.

The characteristic of a field must be prime or 0. Let F be a field with 6 elements. The additive subgroup generated by 1 must have 1, 2, 3, or 6 elements. It can't have 1 or 6 elements, since the characteristic of F is prime. Suppose F has characteristic 3. Now all the non-zero elements can be partitioned into pairs of the form $\{x, 2x\}$. However, there are 5 non-zero elements, so this is not possible. Therefore, F must have characteristic 2. However, the additive group of F is an abelian group with 6 elements, so must be isomorphic to $\mathbb{Z}_6$, or $\mathbb{Z}_2 \times \mathbb{Z}_3$. However, either possibility involves an element of order 3, but this contradicts characteristic 2.

16. Prove that addition and multiplication are well defined in the field of quotients of an integral domain.

Recall that addition and multiplication are defined by $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$ and $[(a, b)][(c, d)] = [(ac, bd)]$ respectively. Showing that these are well-defined means showing that the pairs $(ad + bc, bd)$ and (ac, bd) are valid pairs in the field of quotients (recall that the field of quotients consists of equivalence classes of pairs (x, y) with $y \neq 0$, so this just means showing that $bd \neq 0$) and that the answer doesn't depend on the choice of representatives of the equivalence classes. That is, we need to show that if $(a', b') \sim (a, b)$ and $(c', d') \sim (c, d)$, then $(ad + bc, bd) \sim (a'd' + b'c', b'd')$ and $(ac, bd) \sim (a'c', b'd')$. For showing that $bd \neq 0$, since R is an integral domain, and we have that $b \neq 0$ and $d \neq 0$, we must have $bd \neq 0$.

Recall that $(a, b) \sim (a', b')$ if and only if $ab' = a'b$, so given that

$$ab' = a'b$$
$$cd' = c'd$$

We need to show

$$(ad + bc)(b'd') = (a'd' + b'c')(bd)$$
$$acb'd' = a'c'bd$$

The second of these is easy — $acb'd' = ab'cd' = a'bcd' = a'bc'd = a'c'bd$. For the first, we have that $adb'd' = ab'dd' = a'bdd' = a'd'bd$, and $bcb'd' = bb'cd' = bb'c'd = b'c'bd$, and adding these gives the required equation.

17. *State and prove the factor theorem for the polynomial ring over a field.*

Theorem 1 (Factor Theorem)**.** *For a field F, and a polynomial $f \in F[x]$, an element $\alpha \in F$ is a zero of f if and only if $x - \alpha$ is a factor of f.*

Proof. Let α be a zero of f. By the division algorithm, we have $f(x) = (x - \alpha)q(x) + r(x)$, where the degree of r is less than 1 (the degree of $(x - \alpha)$). This means that r is a constant polynomial of the form c for some $c \in F$, so we have $f(x) = (x - \alpha)q(x) + c$. Now applying the evaluation homomorphism ϕ_α, we get $\phi_\alpha(f) = \phi_\alpha(x - \alpha)\phi_\alpha(q) + \phi_\alpha(c)$. Since α is a zero of f, we have that $\phi_\alpha(f) = 0$, and clearly, $\phi_\alpha(x - \alpha) = 0$, so this equation gives that $c = \phi_\alpha(c) = 0$. That is $f(x) = (x - \alpha)q(x)$, so $x - \alpha$ is a factor of f.

Conversely, suppose $(x - \alpha)$ is a factor of f. Then we have $f(x) = (x - \alpha)g(x)$ for some $g \in F[x]$. Applying ϕ_α gives $\phi_\alpha(f) = 0\phi_\alpha(g) = 0$. Therefore α is a zero of f. □

18. *Let G be a group of order pq for distinct odd primes p and q with $p < q$. Show that G contains an element of order p. [Hint: show that otherwise all elements have order q, and in that case, consider the cyclic subgroups.]*

The order of an element divides the order of the group, so the only possible orders of elements of G are 1, p, q and pq. The only element of order 1 is the identity. If x is an element of order pq, then x^q is of order p. Therefore, if G does not contain an element of order p, then all non-identity elements are of order q. Now the cyclic groups generated by each element must either be equal, or have only the identity in common, any non-identity element in a cyclic group of prime order generates the group, so if two cyclic supgroups H and K of G have an element $x \neq e$ in common, then they also both contain $\langle x \rangle = H = K$, so they are the same subgroup. Therefore, the non-identity elements of G are a disjoint union of the non-identity elements in these cyclic subgroups. Each cyclic subgroup has $q - 1$ elements, so the total number of non-identity elements in G (which is $pq - 1$) is divisible by $q - 1$. However, subtracting from $p(q - 1)$, this would give that $p(q - 1) - (pq - 1) = p - 1$ is divisible by $q - 1$. However, since $p < q$, we have that $p - 1 < q - 1$, so it is not divisible by $q - 1$.

19. *(a) Show that a polynomial of degree n in $F[x]$ for a field F can have at most n zeros.*

Proof by induction. It is clear that a non-zero polynomial of degree 0 has no zeros.

Now suppose the result is true for $n - 1$. Let $f \in F[x]$ be a polynomial of degree n. If f has no zeros, then we are done. Otherwise, suppose α is a

zero of f. By the factor theorem, we have $f(x) = (x - \alpha)q(x)$ for some q of degree $n - 1$. Now since F is a field, and therefore an integral domain, any zero of f must either be a zero of $x - \alpha$, or a zero of q. Clearly, the only zero of $x - \alpha$ is α, and by the induction hypothesis, q has at most $n - 1$ zeros, so the most zeros f can have is $1 + (n - 1) = n$ as required.

(b) Deduce that the multiplicative group of non-zero elements in a finite field is cyclic. (Recall the classification theorem for finitely generated abelian groups.)

Let F be a finite field with q elements. The multiplicative group of non-zero elements is a finite (and therefore finitely generated) abelian group, so by the classification of finitely generated abelian groups, it is isomorphic to $\mathbb{Z}_{{p_1}^{n_1}} \times \cdots \times \mathbb{Z}_{{p_k}^{n_k}}$, for primes $p_1, \ldots, p_k$ and positive integers $n_1, \ldots, n_k$. Now let m be the least common multiple of the ${p_i}^{n_i}$. Any element of any $\mathbb{Z}_{{p_i}^{n_i}}$ has order dividing m, so every element of $\mathbb{Z}_{{p_1}^{n_1}} \times \cdots \times \mathbb{Z}_{{p_k}^{n_k}}$ has order dividing m. This means that any $x \in F \setminus \{0\}$ satisfies $x^m - 1 = 0$. That is, the polynomial $x^m - 1$ has $q - 1$ zeros in F. Therefore, we must have $m \geqslant q - 1 = {p_1}^{n_1} \cdots {p_k}^{n_k}$. However, if the least common multiple of the ${p_i}^{n_i}$ is also their product (it clearly can't be larger than their product), then they must be coprime, i.e. the p_i must all be distinct. In this case, the product $\mathbb{Z}_{{p_1}^{n_1}} \times \cdots \times \mathbb{Z}_{{p_k}^{n_k}}$ is cyclic of order m, as required.