

# MATH-4010 – Abstract Algebra – Final exam

## 15:00-1800, May 7, 2008

1. This group of questions deals with finite Abelian groups.

- (a) Up to isomorphism, how many Abelian groups of order 300 exist? What are they? For example  $\mathbb{Z}_2 \times \mathbb{Z}_2$  and  $\mathbb{Z}_4$  are the only two Abelian groups of order 4, up to isomorphism.

SOLUTION:  $300 = 2^2 \times 3 \times 5^2$ . There are four Abelian groups of order 300, up to isomorphism. They are  $G_1 = \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$ ,  $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$ ,  $G_3 = \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$  and  $G_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ . These may also be written as  $G_1 = \mathbb{Z}_{300}$ ,  $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_{150}$ ,  $G_3 = \mathbb{Z}_5 \times \mathbb{Z}_{60}$  and  $G_4 = \mathbb{Z}_{10} \times \mathbb{Z}_{30}$ , respectively.

- (b) How many non-trivial proper subgroups are there of  $\mathbb{Z}/77\mathbb{Z}$ ? Give a generator for each one. Be careful to express your answers as cosets of a subgroup of  $\mathbb{Z}$ .

SOLUTION: A non-trivial proper subgroup of  $\mathbb{Z}/77\mathbb{Z}$  must have order  $d$ , where  $d > 1$ ,  $d < 77$  and  $d$  divides 77. The only possibilities are  $d = 7$  and  $d = 11$ . There is a single subgroup of each order in a cyclic group, so there are 2 proper subgroups of  $\mathbb{Z}/77\mathbb{Z}$ . One is generated by  $7 + 77\mathbb{Z}$  (order 11) and the other by  $11 + 77\mathbb{Z}$  (order 7).

- (c) Enumerate all subgroups of  $G = \mathbb{Z}_2 \times \mathbb{Z}_4$  by giving generator(s) for each one. For example,  $\{(1,0), (0,1)\}$  generate  $G$ .

SOLUTION: There are 8 subgroups of  $G$ , of which 6 are proper and non-trivial.

$H_1 = G$  is generated by  $\{(1,0), (0,1)\}$ .

$H_2 = \{(0,0), (1,0), (0,2), (1,2)\}$  is generated by  $\{(1,0), (0,2)\}$ .

$H_3 = \{0\}$  is generated by  $\{(0,0)\}$ .

$H_4 = \{(0,0), (0,1), (0,2), (0,3)\}$  is generated by  $\{(0,1)\}$ .

$H_5 = \{(0,0), (0,2)\}$  is generated by  $\{(0,2)\}$ .

$H_6 = \{(0,0), (1,0)\}$  is generated by  $\{(1,0)\}$ .

$H_7 = \{(0,0), (1,1), (0,2), (1,3)\}$  is generated by  $\{(1,1)\}$ .

$H_8 = \{(0,0), (1,2)\}$  is generated by  $\{(1,2)\}$ .

2. Group theory questions.

- (a) If  $G = \mathbb{Z}_{113} \times \mathbb{Z}$ , what is  $Z(G)$ , the center of  $G$  and what is  $C(G)$ , the commutator subgroup?

SOLUTION:  $G$  is Abelian, so  $Z(G) = G$  and  $C(G) = \{e\} = (0,0)$ , the trivial subgroup.

- (b) If  $S_n$  is the group of all permutations of  $n$  objects, what is  $C(S_n)$ , the commutator subgroup?

SOLUTION: This was covered explicitly in class.  $C(S_n) = A_n$ , the alternating subgroup  $S_n$  containing all even permutations. This is easy to show, since every commutator is an even permutation. Furthermore,  $A_n$  is generated by all the 3-cycles, and the 3-cycle,  $(i, j, k)$  can be written as the commutator  $(k, j)(i, j)(k, j)(i, j)$ .

- (c) In  $S_{26}$ , let  $\sigma$  be a permutation whose cycle decomposition is  $(1, 4, 7, 10, 13, 16, 19, 22)(2, 5, 8, 11, 14, 17, 20, 23)(3, 6, 9, 12, 15, 18, 21, 24)(25, 26)$ . Is  $\sigma$  an odd or an even permutation?

SOLUTION: An  $n$ -cycle is an even permutation if  $n$  is odd, and an odd permutation if  $n$  is even.  $\sigma$  is the product of 3 8-cycles and a 2-cycle (transposition), so it is the product of 4 odd permutations, making it an even permutation.

- (d) Compute  $C(D_n)$ , the commutator subgroup of  $D_n$ , where  $D_n$  is the dihedral group of the regular  $n$ -gon. Recall that  $D_n$  can be defined as a subgroup of permutations on  $n$  objects generated by  $\rho = (1, 2, 3, \dots, n-1)$  and  $\tau = (1, n)(2, n-1), (3, n-3) \dots (i, j)$ , where  $(i, j) = (n/2, n/2+1)$  if  $n$  is even and  $(i, j) = ((n-1)/2, (n+3)/2)$  if  $n$  is odd. The  $2n$  group elements are the subgroup,  $H = \{\rho, \rho^2, \dots, \rho^n = e\}$  and the single coset,  $\tau H$ . (Hint: The answer depends on whether  $n$  is even or odd.)

SOLUTION: In  $D_n$ ,  $\tau\rho^{-1}\tau = \rho$ . The commutator,  $\tau\rho^{-1}\tau\rho$  simplifies to  $\rho^2$ . If  $n$  is odd, then  $\rho^2$  generates the same subgroup of  $D_n$  as  $\rho$ , which is  $H$  above. If  $n$  is even, only even powers of  $\rho$  can be generated. The conclusion is that  $C(D_n) = \{\rho, \rho^2, \rho^3 \dots, \rho^n = e\}$  if  $n$  is odd, so  $|C(D_n)| = n$ , and  $C(D_n) = \{\rho^2, \rho^4, \dots, \rho^{2(n/2)} = e\}$  if  $n$  is even, so  $|C(D_n)| = n/2$ .

3. In this group of questions,  $R$  is a ring and  $R_1$  is a subset of  $R$ . In each case, determine whether or not  $R_1$  is a subring of  $R$ . If  $R_1$  is a subring of  $R$ , determine whether or not it is an ideal.

- (a)  $R = \mathbb{Z}$ .  $R_1 = 613\mathbb{Z}$ .

SOLUTION:  $R_1$  is an ideal.

- (b)  $R = \mathbb{Z} \times \mathbb{Z}$ .  $R_1 = 3\mathbb{Z} \times 6\mathbb{Z}$ .

SOLUTION:  $R_1$  is an ideal.

- (c)  $R = \mathbb{Q}[x]$ .  $R_1 = \mathbb{Z}[x]$ .

SOLUTION:  $R_1$  is a subring of  $R$ , but not an ideal. The ideal generated by  $R_1$  is all of  $R$ .

- (d)  $R = \mathbb{Z}[x]$ .  $R_1$  is the set of polynomials with integer coefficients whose powers of  $x$  are prime numbers. For example,  $3x^7 - 10x^{11} + x^{41} \in R_1$ , but  $12x^{13} - x^{22} \notin R_1$ .

SOLUTION:  $R_1$  is not even a subring of  $R$ , let alone an ideal. For example,  $R_1$  is not closed under multiplication. For example,  $x^5 \times x^7 = x^{12}$ .

- (e)  $R = \mathbb{Z}[x]$ .  $R_1$  is the set of polynomials with integer coefficients whose powers of  $x$  are all multiples of 6. For example,  $9x^{66} - 17x^{42} + 1 \in R_1$ , but  $3x^{61} + 4x^6 + 6 \notin R_1$ .

SOLUTION:  $R_1$  is a subring of  $R$ , but not an ideal. In fact, if  $p(x)$  is any non-zero polynomial in  $R_1$ , then  $xp(x) \notin R_1$  since all the powers of  $x$  will be  $\equiv 1 \pmod{6}$ .

- (f)  $R = \mathbb{Z}[x]$ .  $R_1$  is the set of polynomials with integer coefficients whose powers of  $x$  are all  $\leq 5$ .

SOLUTION:  $R_1$  is not even a subring of  $R$ , let alone an ideal.  $R_1$  is not closed under multiplication, since  $x^4 \times x^3 = x^7 \notin R_1$ .

- (g)  $R = \mathbb{Z}[x]$ .  $R_1$  is the set of polynomials with integer coefficients whose powers of  $x$  are all  $\geq 5$ .

SOLUTION:  $R_1$  is an ideal of  $R$ .

- (h)  $R = \mathbb{Z}[x]$ .  $R_1 = 3\mathbb{Z}[x]$ .

SOLUTION:  $R_1$  is an ideal of  $R$ . If the coefficients of  $p(x)$  are all multiples of 3, then the coefficients of  $q(x)p(x)$  will be multiples of 3 for any polynomial,  $q(x)$ .

4. This group of questions deals with irreducible and reducible polynomials.

- (a) Prove that  $42x^7 - 75x^5 + 20x^2 - 120$  is irreducible in  $\mathbb{Q}[x]$ .

SOLUTION: Proof by the Eisenstein criterion. The prime number 5 does not divide 42, the coefficient of the highest power of the polynomial. 5 divides all the other coefficients and  $5^2 = 25$  does not divide  $-120$ , the constant term (coefficient of  $x^0$ ).

- (b)  $p(x) \in \mathbb{R}[x]$ , and  $p(x)$  has an odd degree. Is  $p(x)$  reducible? Give a reason.

SOLUTION:  $p(x)$  is reducible over the real numbers because it must have at least one root. To see this, we may as well assume that  $p(x)$  is monic. As  $x \rightarrow -\infty$ ,  $p(x) \rightarrow -\infty$  and as  $x \rightarrow \infty$ ,  $p(x) \rightarrow \infty$ . Thus  $p(x)$  must be negative for some  $x_1$  and positive for some  $x_2 > x_1$ . Since  $p(x)$  is a continuous function,  $p(x_3) = 0$  for some  $x_3 \in (x_1, x_2)$ .

- (c) Prove that  $x^3 + 2x^2 + 1$  is irreducible in  $\mathbb{Z}_7[x]$ .

SOLUTION: Brute force. It suffices to show that  $p(x) = x^3 + 2x^2 + 1$  has no roots. Trying all possible values of  $x$  yields:

$x$	$p(x)$
0	1
1	4
-1	2
2	3
-2	1
3	4
-3	6

(d) Prove that  $x^5 + x^3 + 1$  is irreducible in  $\mathbb{Z}_2[x]$ .

SOLUTION: First observe that  $p(x) = x^5 + x^3 + 1$  has no root, since  $p(0) = p(1) = 1$  in  $\mathbb{Z}_2$ . The only way it could be reducible would be if it were the product of a cubic polynomial and a quadratic polynomial. The coefficients of  $x^3$  in the cubic and of  $x^2$  in the quadratic would have to both be 1, as would the constant terms of these polynomials. It suffices to show that  $x^5 + x^3 + 1 = (x^3 + ax^2 + bx + 1)(x^2 + cx + 1)$  is impossible.

i. Coefficient of  $x^4$ :  $a + c = 0$

ii. Coefficient of  $x^3$ :  $1 + ac + b = 1$

iii. Coefficient of  $x^2$ :  $1 + bc + a = 0$

iv. Coefficient of  $x$ :  $b + c = 0$ .

i. and iv. imply  $a = c = b$  in  $\mathbb{Z}_2$ . Then  $1 + bc + a = 1 + a^2 + a = 1 + 2a = 1$ , which contradicts iii.

5. In Dingbatland, the smallest unit of currency is the “foo”. The “buck” is a coin that is worth eight foos, while the “bock” is a coin that is worth 7 foos. Tweedledum walks into a shop where all items sell for under 100 foos and buys a widget. He pays in bucks and receives 3 foos in change. A bit later, Tweedledee walks into the same shop and buys a widget at the same price as Tweedledum. He pays in bocks and receives 5 foos in change. What is the cost of a widget? If the answer is not unique, what are the possible values?

SOLUTION: If a widget costs  $x$  foos, then we know that

$$\begin{aligned}x &\equiv -3 \pmod{8} \quad \text{and} \\x &\equiv -5 \pmod{7}.\end{aligned}$$

8 and 7 are relatively prime, and by inspection,  $8 - 7 = 1$ , so  $-2 \times 8 + 2 \times 7 = -2 = -5 + 3$ , yielding  $-2 \times 8 - 3 = -2 \times 7 - 5$ . This gives a “solution” of  $-19$ , which is nonsense, but it shows that all possible solutions are  $-19 + 56\mathbb{Z}$ . The only positive solutions less than 100 are 37 and 93, so a widget costs either 37 foos or 93 foos.

6. Compute  $2629^{893} \pmod{13}$ .

SOLUTION: Note that  $2629 \equiv 3 \pmod{13}$  and that  $893 = 12 \times 74 + 5$ . Thus  $2629^{893} \equiv (3^{12})^{74} 3^5 \pmod{13} \equiv 1^{74} 3^5 \pmod{13} = 3^5 = 9 \times 9 \times 3 \equiv 9 \pmod{13}$ .

7. Review. Sum of terms in a geometric progression.  $F$  is a field and  $a, r \in F, r \neq 1$ , then  $a + ar + ar^2 + \dots + ar^m = a \frac{1 - r^{m+1}}{1 - r}$ . You may or may not find this useful in answering the following question.

Let  $p$  be a prime number such that  $p \equiv 1 \pmod{6}$ . For example,  $p = 13 = 2 \times 6 + 1, p = 613 = 102 \times 6 + 1$ . Prove that there are three distinct positive integers,  $x, y$  and  $z$ , all  $< p$  such that  $x^2 + y^2 + z^2 \equiv 0 \pmod{p}$ . Compute an explicit solution for  $p = 13$ .

SOLUTION: Let  $p = 6k + 1$  and let  $r$  be a primitive root of unity. Compute  $1 + (r^k)^2 + (r^{2k})^2 = (1 - r^{6k}) / (1 - r^{2k}) = 0$  in  $\mathbb{Z}_p$ . Let  $x = 1, y = r^k$  and  $z = r^{2k}$ . Then  $x^2 + y^2 + z^2 \equiv 0 \pmod{p}$ . For  $p = 13, k = 2$  and  $r = 2$  is a primitive root of unity. Let  $x = 1, y = 2^2 = 4$  and  $z = 2^4 \equiv 3 \pmod{13}$ . Then  $1^2 + 3^2 + 4^2 \equiv 0 \pmod{13}$ . Check:  $1 + 9 + 16 = 26 = 2 \times 13$ .

Note that, in  $\mathbb{Z}_p$ , if  $z = r^{2k}$ , as above, then  $1^2 + z^2 + (z + 1)^2 = 2(r^{4k} + r^{2k} + 1) = 2(1 - r^{6k}) / (1 - r^{2k}) = 0$ , so  $x = 1$  can always be used, and  $y$  and  $z$  differ by 1.

8. Fields and extension fields.

- (a) Which of the following rings is a field?  $\mathbb{Z}, \mathbb{Z}_{30}, \mathbb{Z}_{31}$ .

SOLUTION:  $\mathbb{Z}$  is an integral domain, but not a field.  $\mathbb{Z}_{30}$  has zero divisors  $5 \times 6 = 0$ , so cannot be a field.  $\mathbb{Z}_{31}$  is a field because 31 is prime.

- (b) Assume that  $\pi$  is transcendental. Let  $R = \left\{ \frac{a_1 + a_2\pi + a_3\pi^2 + \dots + a_m\pi^m}{b_1 + b_2\pi + b_3\pi^2 + \dots + b_n\pi^n} \right\}$ , where  $a_i$  and  $b_j$  are integers, at least one of the  $b_j$ s is  $\neq 0$ , and  $m, n$  are non-negative integers. Is  $R$  a field?

SOLUTION: Yes,  $R$  is a field. In fact,  $R$  is isomorphic to the field of quotients of  $\mathbb{Z}[\pi]$ , which is also isomorphic to the field of quotients of  $\mathbb{Q}[\pi]$ .

- (c) In the extension field,  $\mathbb{Q}(\sqrt{19})$ , what is the multiplicative inverse of  $a + b\sqrt{19}$ ? Express your answer in the form  $c + d\sqrt{19}$ , where  $c, d \in \mathbb{Q}$ . Compute the multiplicative inverse of  $170 + 39\sqrt{19}$ .

SOLUTION:  $(a + b\sqrt{19})(a - b\sqrt{19}) = a^2 - 19b^2$ . Since  $\sqrt{19}$  is irrational, this difference can never be zero unless both  $a$  and  $b$  are 0. Then the multiplicative inverse of  $a + b\sqrt{19}$  is  $\frac{a}{\Delta} - \frac{b}{\Delta}\sqrt{19}$ , where  $\Delta = a^2 - 19b^2$ . For  $170 + 39\sqrt{19}$ ,  $\Delta = 170^2 - 19 \times 39^2 = 28900 - 1521 \times 19 = 28900 - 28899 = 1$ , so the multiplicative inverse of  $170 + 39\sqrt{19}$  is  $170 - 39\sqrt{19}$ .

- (d) In  $\mathbb{Z}_2[x]$ , prove that the polynomial,  $x^3 + x + 1$ , is irreducible. Let  $\alpha$  be a root of this polynomial in an extension field. (For example, the coset,  $x + \langle x^3 + x + 1 \rangle$ , is a root of this polynomial in the field  $F = \mathbb{Z}_2[x] / \langle x^3 + x + 1 \rangle$ . What is the order of  $F$ ? What is the order of the multiplicative group of non-zero elements of  $F$ ? Determine a generator,  $a$ , of this group, and write down all elements of the group as powers  $a$ .

SOLUTION:  $x^3 + x + 1$  is irreducible because it has no roots. The polynomial evaluates to 1 for  $x = 0$  and for  $x = 1$ . Let  $\alpha$  be a root of this polynomial in an extension field of  $\mathbb{Z}_2$ . Then  $|\mathbb{Z}_2(\alpha)| = 2^3 = 8$ , and so the multiplicative group of non-zero elements has order 7, which is prime. This means that any non-zero element of  $\mathbb{Z}_2(\alpha)$ , with the exception of 1, generates the group. We may as well choose  $a = \alpha$ . The group elements are:

$n$	$a^n$			
1				$a$
2	$a^2$			
3			$a$	+ 1
4	$a^2$	+	$a$	
5	$a^2$	+	$a$	+ 1
6	$a^2$			+ 1
7				1