Exam 3: Algebra. Module 7, Codes 201400483 & 201800141

Discrete Structures & Efficient Algorithms

Friday, 8 April 2022, 13:45-16:45

At the end of the exam:

1. Carefully check that your name and S-number is on the top of each page.
2. Scan your work with your smartphone
3. Hand in your paper
4. Convert your scan into a SINGLE pdf file
5. Upload the pdf on the Module site of Canvas in the Assignment field Algebra Exam.

All answers need to be motivated. You can also consult a two-page handwritten summary. There are **five** exercises. This third exam of Module 7 consists of the **Algebra part** only, and is a **3h exam**. The total is 90 points. The grade, when you have P points, equals

$$1 + \frac{9P}{90}.$$

---

1. Consider the group S_7, the group of permutations of seven symbols.

   (a) (1p) How many elements does S_7 have?

   (b) (2p) Let $\alpha \in S_7$ be given by

   $$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 7 & 2 & 4 & 6 \end{bmatrix}$$

   What is the order, $|\alpha|$, of α?

   (c) (3p) If, for example, we want to write a non-identity permutation of 4 elements as a product of disjoint cycles (without 1-cycles), the possibilities are: a 4-cycle, a 3-cycle, a 2-cycle, or a product of two 2-cycles. What are the possibilities for non-identity permutations of 7 elements?

   (d) (2p) Does there exist $\alpha \in S_7$ such that $|\alpha| = 8$?

   (e) (3p) What are the possible orders of the permutations in S_7?

   (f) (4p) Determine for each possible divisor of $|S_7|$, an $\alpha \in S_7$ with precisely that order.

   (g) (3p) Is S_7 isomorphic to D_{360}, the symmetry group of a regular 360-gon?

2. Let the ring R be given by

   $$R = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$$

   and let S be given by

   $$S = \{(a, b, c) \in R \mid c = a + b\}$$

PTO

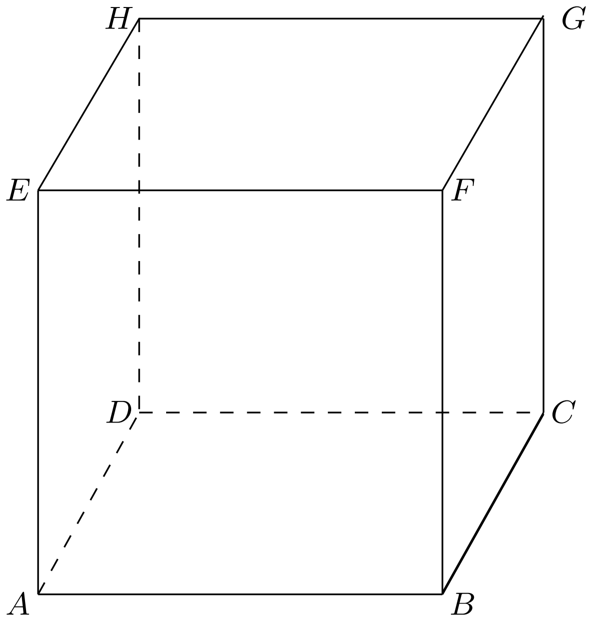

Figure 1: Cube

(a) (6p) Describe addition and multiplication in R.

(b) (6p) Determine all units of R.

(c) (6p) Is S a subring of R?

3. Consider the cube in Figure 1 and let G be the group of rotations that transform the cube into itself. We want to paint the faces of the cube using red, yellow and blue and all three colours have to be used. The goal of this exercise is to find out how many different configurations there are when we take the rotational symmetries into account. Face 1: $ABCD$ (the base face or ground face), Face 2: $ABFE$, Face 3: $BCGF$, Face 4: $CGHD$, Face 5: $ADHE$, Face 6: $EFGH$ (the top face).

   (a) (3p) Describe the rotations that leave Face 1 invariant, and determine $|\text{Stab}_G(1)|$.

   (b) (3p) Describe the rotations that rotate Face 1 to each of the other faces, and determine $|\text{Orb}_G(1)|$.

   (c) (3p) Show that G contains 24 elements, that is $|G| = 24$.

   (d) (3p) G acts on the set S of different colour configurations for the cube in the position as depicted (so without taking into account the symmetries). Describe the set S. How many elements does S have?

   (e) (2p) For each pair of opposite faces there are three rotations in G, disregarding the identity. Determine for each of these rotations ϕ, $|\text{fix}(\phi)|$. Hint: the rotations permute the faces. Write the corresponding permutation in disjoint cycle form. For instance a rotation of 90 degrees has order 4, and leaves 2 faces invariant. Therefore the corresponding permutation is of the form $(a)(b)(cdef)$. Notice that all faces in each cycle should have the same colour.

   (f) (2p) For each pair of opposite edges there is one rotation ϕ in G, disregarding the identity. Determine $|\text{fix}(\phi)|$. Hint: modify the hint in the previous item.

   (g) (2p) For each pair of opposite vertices there are two rotations in G, disregarding the identity. Determine for each of these rotations ϕ, $|\text{fix}(\phi)|$. Hint: modify the hint in the previous item.

   (h) (3p) Use Burnside's Theorem to determine the number of different orbits, that is, the number of different colour schemes.

4. Let $p(x) \in \mathbb{Z}_2[x]$ be given by

$$p(x) = x^3 + p_1 x + p_0.$$

(a) (4p) Determine all possible values of $p_0, p_1 \in \mathbb{Z}_2$ such that

$$\mathbb{F} = \mathbb{Z}_2[x] / < p(x) >$$

is a field.

(b) (3p) Describe the elements of $\mathbb{F}$. How many elements does $\mathbb{F}$ have?

(c) (4p) Determine the multiplicative order of $x+ < p(x) >$ in $\mathbb{F} \backslash \{0\}$.

(d) (4p) Determine $(x+ < p(x) >)^{-1}$.

5. (a) (10 points) Alice and Bob are using RSA to exchange messages. Let us assume that Alice has published modulus $n = 119$, and exponent $e = 35$. Bob sends ciphertext $C = 5$ to Alice. You are eavesdropper Eve and you want to intercept Bob's secret message M by facorising n. Compute Bob's secret message M from ciphertext C. In doing that, please write down all of the computational steps that you need to perform in order to obtain Bob's secret message M.

(b) (8 points) For each of the following two claims, decide if true or false. A correct answer counts **four points**, an incorrect answer counts **minus three points** (minimum for 5b is 0 points). **Instead of guessing, it may be better not giving an answer.**

i. Consider the RSA method for public modulus $n = p \cdot q$ with primes p, q, and public exponent e relatively prime with $\phi(n)$, secret message $M \in \mathbb{Z}_n$, and cyphertext $C = M^e \pmod n$. **Claim:** If gcd$(M, n) > 1$, then the cryptosystem can be broken in polynomial computation time by only using the publicly available information C, n, e.

True . . . . □
False . . . . □
I prefer not to give an answer . . . . □

ii. Consider once more the RSA method. **Claim:** If there is an efficient (polynomial computation time) algorithm to tell whether an arbitrary given number $n \in \mathbb{Z}$ is a prime or not, then the RSA cryptosystem can be broken in polynomial computation time by only using the publicly available information C, n, e.

True . . . . □
False . . . . □
I prefer not to give an answer . . . . □

1a S_7 has $7! = 5040$ elements

b $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 7 & 2 & 4 & 6 \end{bmatrix}$

in disjoint cycle form:

$\alpha = (1\ 3\ 5\ 2)(4\ 7\ 6)$

$|\alpha| = \operatorname{lcm}(|(1\ 3\ 5\ 2)|, |(4,7,6)|$

$= \operatorname{lcm}(4,3) = 12$

Alternatively: brute force:

$\alpha^0, \alpha, \alpha^2, \alpha^3, \alpha^4, --, \alpha^{11}, \alpha^{12}$

1C. Disjoint cycle forms in S_7:

	lc	order
(ab) : 2	2	2
(abc): 3	3	3
(abcd): 4	4	4
(abcde): 5	5	5
(abcdef): 6	6	6
(abcdefg): 7	7	7
(ab)(cd): 2+2	4	
(ab)(cde): 2+3	6	
(ab)(cdef): 2+4	4	
(ab)(cdefg): 2+5	10	10
(abc)(def): 3+3	3	
(abc)(defg): 3+4	12	12
(ab)(cd)(ef): 2+2+2	2	
(ab)(cd)(efg): 2+2+3	6	

1d $\alpha \in S_7$ cannot contain a cycle of length 8 and cannot be the product of cycles such that the lcm of their seperate lengths (orders) is 8.

1f $|\varepsilon|=1$, $|(12)|=2$ $|(123)|=3$ $|(1234)|=4$
$|(12345)|=5$ $|(123456)|=6$
$|(1234567)|=7$
$|(12)(34567)|=10$
$|(123)(4567)|=12$

1g. D_{360} has 720 elements, whereas S_7 has 5040 elements, hence they are not isomorphic.

2. (a) $(a\ b\ c) + (d\ e\ f) = (a+d, b+e, c+f)$

$(a\ b c) \cdot (d e\ f) = (ad, be, cf)$

(b) Units in R: $(\pm 1, \pm 1, \pm 1)$

so 8 in total

(c) S is not a subring of R because it is not closed with respect to multiplication:

$$\underset{\in S}{\underset{\downarrow}{(1,1,2)}} \cdot \underset{\in S}{\underset{\downarrow}{(1,1,2)}} = \underset{\notin S}{\underset{\downarrow}{(1,1,4)}}$$

3. (a) $\text{Stab}_G(1) = \{R_0, R_{90}, R_{180}, R_{270}\}$

rotations about the line that connects the centers of Face 1 and Face 6

$|\text{Stab}_G(1)| = 4$

(b) Rotations about the axis that connects the centers of Faces 2 & 4 yield Faces 1, 3, 5, 6

Rotation about the centers of Faces 3 and 5 yield Faces 1, 2, 4, 6

$\text{Orb}_G(1) = \{1, 2, 3, 4, 5, 6\}$

& $|\text{Orb}_G(1)| = 6$

(c) Orbit - Stabaliser theorem:

$$|G| = |\mathrm{Stab}_G(1)| \cdot |\mathrm{Orb}_G(1)| = 4 \cdot 6 = 24$$

(d) $S = \{(c_1 c_2 c_3 c_4 c_5 c_6) \mid c_i \in \{r, y, b\},\ c_{i_1} = r,\ c_{i_2} = y,\ c_{i_3} = b\}$

Number of elements can be determined as follows:

$$S_{2b} = \{(c_1, \dots, c_6) \mid c_i \in \{r, y\}\} \setminus \{(rrrrrr), (yyyyyy)\}$$

$$|S_{2b}| = 2^6 - 2$$

likewise $|S_{2y}| = 2^6 - 2$ $|S_{2r}| = 2^6 - 2$

$S_3 = \{(c_1 - - c_6) \mid c_i \in \{r, y, b\}\}$ $|S_3| = 3^6$

$$S = S_3 \setminus (S_{2b} \cup S_{2y} \cup S_{2r} \cup \{(r \cdots r), (y \sim y), (b - - b)\}$$

(mutually disjoint sets)

$$
\begin{aligned}
|S| &= 3^6 - \left((2^6 - 2) \cdot 3 + 3\right) \\
&= 3^6 - (3 \cdot 2^6 - 3) \\
&= 3^6 - 3 \cdot 2^6 + 3 \\
&= 729 - 192 + 3 \\
&= \boxed{540}
\end{aligned}
$$

e $|R_{90}| = 4 \Rightarrow$ permutation of the form $(a)(b)(c\,d\,e\,f)$

$\Rightarrow |fix(R_{90})| = 6$

$|fix(R_{270})| = 6$

$|R_{180}| = 2 \Rightarrow$ permutation of the form $(a)(b)(cd)(ef)$

$$fix\,R_{180} = \{\underset{\binom{4}{2}\cdot 2}{rryb},\ \underset{\binom{4}{2}\cdot 2}{ryyb},\ \underset{\binom{4}{2}\cdot 2}{rybb}\}$$

$\Rightarrow |fix\,R_{180}| = \binom{4}{2}\cdot 3\cancel{2} = 36$ (see next page for alternative sol.)

$|fix\,R_{90}| + |fix\,R_{180}| + |fix\,R_{270}| = 6+36+6 = 48$

3 pairs → $3 \cdot 48 = \boxed{144}$

Alternative solution for $|\mathrm{fix}\, R_{180}|$

$$(a)(b)(c\,d)(e\,f)$$

Similar to the calculation of $|S|$, define

$$T = \{ (c_1, c_2, c_3, c_4) \mid c_i \in \{r, y, b\},\ c_i = r,\ c_{i_2} = y,\ c_{i_3} = b \}$$

T is the set of colourings of the four cycles for which all three colours are used

$$T_{2b} = \{ (c_1, c_2, c_3, c_4) \mid c_i \in \{r, y\} \} \setminus \{rrrr, yyyy\}$$

$|T_{2b}| = 2^4 - 2$, likewise $|T_{2y}| = 2^4 - 2$, $|T_{2r}| = 2^4 - 2$

$$T_3 = \{ (c_1, c_2, c_3, c_4) \mid c_i \in \{r, y, b\} \}$$

$$T = T_3 \setminus \left(T_{2b} \cup T_{2y} \cup T_{2r} \cup \{rrrr, yyyy, bbbb\} \right) \quad \text{(disjoint union)}$$

$$|T| = |T_3| - \left(|T_{2b}| + |T_{2y}| + |T_{2r}| + 3 \right)$$

$$= 3^4 - \left(3(2^4 - 2) + 3 \right) = 81 - (3.16 - 3) = 81 - 45 = 36$$

(f) Opposite edges → R_{180} , order 2

$\Rightarrow$ $(a\,b)(c\,d)(e\,f)$

$|\text{fix } R_{180}| = 6$

6 pairs → $6 . 6 = \boxed{36}$

(g) Opposite vertices:

$|R_{120}| = 3$ → $(a\,b\,c)(d\,e\,f)$

$\text{fix}(R_{120}) = \emptyset \Rightarrow |\text{fix } R_{120}| = |\text{fix } R_{240}| = 0$

h. Number of orbits:

$$\frac{1}{24}\sum_{\varphi\in G} |\mathrm{fix}(\varphi)| = \frac{1}{24}\left(540+36+144\right) = \frac{720}{24} = 30$$

4. (a) Required: $p(x)$ irreducible

$p(0) = P_0 \Rightarrow P_0 = 1$

$p(1) = 1 + P_1 + P_0 = 1 + P_1 + 1 = P_1 \Rightarrow P_1 = 1$

because deg ≤ 3

$\Rightarrow p(x) = x^3 + x + 1$

(b) $\mathbb{Z}_2[x] \big/ \langle p(x) \rangle = \{ a_2 x^2 + a_1 x + a_0 + \langle p(x) \rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_2 \}$

$|\mathbb{F}| = 2^3 = 8$

(c) $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ has 7 elements $\Rightarrow$

order is 1 or 7.

$x + \langle p(x) \rangle \neq 1 + \langle p(x) \rangle \Rightarrow$

$|x + \langle p(x) \rangle| = 7$

(d) $(x+\langle p(x)\rangle)^{-1} = a(x)+\langle p(x)\rangle$

$$\Rightarrow (x+\langle p(x)\rangle)(a(x)+\langle p(x)\rangle) \overset{?}{=} 1+\langle p(x)\rangle$$

$$a(x)=a_2x^2+a_1x+a_0$$

$$(x+\langle p(x)\rangle)(a_2x^2+a_1x+a_0+\langle p(x)\rangle) =$$

$$a_2x^3+a_1x^2+a_0x+\langle p(x)\rangle$$

$$= a_2(x+1)+a_1x^2+a_0x+\langle p(x)\rangle$$

$$= a_2x+a_2+a_1x^2+a_0x+\langle p(x)\rangle$$

$$= (a_2+a_0)x+a_1x^2+a_2+\langle p(x)\rangle \overset{?}{=} 1+\langle p(x)\rangle$$

$$\Rightarrow a_2=1 \quad a_1=0 \quad a_2+a_0=0 \Rightarrow a_0=1$$

$$\Rightarrow (x+\langle p(x)\rangle)^{-1} = x^2+1+\langle p(x)\rangle$$

Alternative method: Euclidean algorithm

$$(x+\langle p(x)\rangle)(a(x)+\langle p(x)\rangle) = 1+\langle p(x)\rangle$$

$$\Rightarrow \quad x\,.\,a(x) = 1+\langle p(x)\rangle$$

$$\Rightarrow \quad x\,.\,a(x)+p(x)\,b(x) = 1$$

$$x^3+x+1 = x\,.\,(x^2+1)+1$$

$$x\,.\,(x^2+1) = -1+\langle p(x)\rangle$$

$$= 1+\langle p(x)\rangle$$

$$\Rightarrow \quad (x+\langle p(x)\rangle)^{-1} = x^2+1+\langle p(x)\rangle$$

5a) As $n = 119$, $p = 7$ and $q = 17$.

Therefore, $r = \varphi(n) = (p-1)(q-1) = 6 \cdot 16 = 96$

We want to compute $M = C^d \pmod n$, so we need $d = e^{-1}$ (in $\mathbb{Z}_{96}$). As $e = 35$ the ext. Eucl. algorithm gives

$$\begin{bmatrix} 96 & 1 & 0 \\ 35 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 26 & 1 & -2 \\ 35 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 26 & 1 & -2 \\ 9 & -1 & 3 \end{bmatrix}$$

$$\sim \begin{bmatrix} 8 & 3 & -8 \\ 9 & -1 & 3 \end{bmatrix} \sim \begin{bmatrix} 8 & 3 & -8 \\ \boxed{1} & -4 & 11 \end{bmatrix} \sim \begin{bmatrix} 0 & 35 & -52 \\ 1 & -4 & 11 \end{bmatrix}$$

$\Rightarrow 1 = -4 \cdot 96 + 11 \cdot 35$

$\Rightarrow 35^{-1} = 11 \pmod{96}$, so $d = 11$.

As $C = 5$, we need to compute $5^{11} \pmod{119}$. To that end, note that $11 = 2^3 + 2^1 + 2^0$.

We compute mod 119:

$$5^{2^0} = 5$$
$$5^{2^1} = (5)^2 = 25$$
$$5^{2^2} = (25)^2 = 625 = 30$$
$$5^{2^3} = (30)^2 = 900 = 67$$

So, $M = C^d \pmod n = 5^{2^0} \cdot 5^{2^1} \cdot 5^{2^3} \pmod{119} =$

$5 \cdot 25 \cdot 67 \pmod{119} = 6 \cdot 67 \pmod{119}$

$= 45$ $\blacksquare$

5b) i) True. If $\gcd(M, n) > 1$ then $p \mid M$ or $q \mid M$

$$\Rightarrow p \mid C = M^e \quad (\text{or } q \mid C)$$

So, computing $\gcd(C, n)$ will yield p (or q) and this can be done efficiently. Then $r=(p-1)(q-1)$ can also be computed efficiently, as can $d = e^{-1} (\mathbb{Z}_r)$ and finally $M = C^d (\text{mod } n)$.

ii) False. Knowing that n is not prime does not help, as it does not give any information towards the prime factorization $n = p \cdot q$.