

Archive of documentation for

MATH 323, Algebra 1

Bilkent University, Fall 2014, Laurence Barker

version: 17 January 2015

Source file: arch323fall14.tex

page 2: Course specification.

page 4: Homeworks and quizzes.

page 8: Midterm 1.

page 9: Solutions to Midterm 1.

page 11: Midterm 2 and Solutions.

page 13: Makeup for Midterm 2.

page 14: Final and Solutions.

MATH 323, Algebra I, Fall 2014

Course specification

Laurence Barker, Mathematics Department, Bilkent University,
version: 22 October 2014.

Course Aims: To introduce the methods and techniques of group theory, as an introduction to algebra.

Course Description: Group theory lies at the foundation of modern algebra. We shall be focusing on the theory of groups because the methods carry over to other branches of algebra.

Course Requirements: Most mathematics cannot be learned just by listening. To take in the concepts and techniques, you have to study the course notes and do some exercises yourself.

Instructor: Laurence Barker, Office SAZ 129,
e-mail: barker at fen dot bilkent dot edu dot tr.

Assistant: Hatice Mutlu.
e-mail: hatice dot mutlu at bilkent dot edu dot tr.

Course Text: D. S. Dummit, R. M. Foote, “Abstract Algebra”, 3th Edition. (Wiley, 2004).

Classes: Wednesdays 09:40 - 10:30 SA-Z03, Fridays, 10:40 - 12:30 SA-Z03.

Office Hours: Wednesdays, 08:40 - 09:30, SA-129.

Please note, Office Hours is not just for the strong students. I will have no sympathy for drowning students who do not come to me for help. Students who are having serious difficulties must come to Office Hours to discuss the mathematics. In fact, I need those students to come, so as to ensure that the classroom material does not lose touch with parts of the audience.

Syllabus:

Week number: Monday date: Subtopics. Section numbers

- 1: 15 Sept:** Background from number theory, 0.3
- 2: 22 Sept:** Examples of groups, 1.1-1.5
- 3: 29 Sept:** Homomorphisms, group actions, subgroups, 1.6, 1.7, 2.1-2.4.
- 4: 6 Oct:** The lattice of subgroups, Lagrange’s Theorem, 2.5, 3.2
- 5: 13 Oct:** Quotient groups and the isomorphism theorems, 3.1, 3.3, 3.4.
- 6: 20 Oct:** The symmetric and alternating groups, 3.5.
- 7: 27 Oct:** Review for Midterm 1. Midterm 1 on 31 October.

- 8: 3 Nov:** Permutation representations, 4.1, 4.2
- 9: 10 Nov:** Cayley's Theorem. The class equation, 4.2, 4.3
- 10: 17 Nov:** Automorphisms, statement of Sylow theorems 4.4, 4.5.
- 11: 24 Nov:** Proof of Sylow theorems, 4.5, simplicity of A_n , 4.6.
- 12: 1 Dec:** Review for Midterm 2. Midterm 2 on 5th December.
- 13: 8 Dec:** Direct products, finitely generated abelian groups 5.1, 5.2.
- 14: 15 Dec:** Recognizing direct products, 5.3
- 15: 22 Dec:** Semidirect products, 5.4
- 16: 29 Dec:** [no scheduled classes]

Assessment:

- Quizzes, Homework and Participation 15%.
- Midterm I, 25%, Friday 31 October.
- Midterm II, 25%, Friday 5th December.
- Final, 35%.

75% attendance is compulsory.

Class Announcements: All students, including any absentees from a class, will be deemed responsible for awareness of class announcements.

MATH 323, Algebra 1, Fall 2014

Homeworks, Quizzes

Laurence Barker, Mathematics Department, Bilkent University,
version: 24 December 2014.

Office Hours: Wednesdays, 08:40 - 09:30, SA 129.

Office Hours would be a good time to ask me for help with the homeworks.

The course textbook is D. S. Dummit and R. M. Foote, "Abstract Algebra", 3rd Edition (Wiley 2004). Some of the questions are taken from there. The solutions are discussed in class.

Homework 1 due Friday 26th September

1.1: Which of the following binary operations are associative?

(a) The operation $*$ on \mathbb{Z} defined by $a * b = a + b + ab$.

(b) The operation $*$ on \mathbb{Q} defined by $a * b = 2(a * b)$

(c) The operation $*$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, \alpha) * (b, \beta) = (a\beta + b\alpha, \alpha\beta)$.

1.2: Show that the multiplication operation on $\mathbb{Z}/n\mathbb{Z}$ given by $[a]_n \cdot [b]_n = [ab]_n$ is well-defined.

1.3: For the following a and b express the greatest common divisor (a, b) in the form $(a, b) = xa + yb$ where x and y are integers.

(i) $a = 20$ and $b = 13$.

(ii) $a = 69$ and $b = 372$.

1.4: Let G be a group such that every non-identity element has order 2. Show that G is abelian.

Quiz 1: *Wednesday 24 September.* Find the orders and the inverses of all 12 elements of the group $\mathbb{Z}/12\mathbb{Z}$.

Solution 1: The elements 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 have orders 1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, 12 and inverses 0, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1, respectively.

Quiz 2: *Wednesday 1 October.* Show that the group isomorphism relation \cong is an equivalence relation.

Solution 2: Let F, G, H be groups. The identity function on F is an isomorphism $F \rightarrow F$, so $F \cong F$ and \cong is reflexive. Suppose that $F \cong G$. Let $\theta : F \rightarrow G$ be an isomorphism. For $g_1, g_2 \in G$, writing $g_1 = \theta(f_1)$ and $g_2 = \theta(f_2)$, then

$$\theta^{-1}(g_1 g_2) = \theta^{-1}(\theta(f_1 f_2)) = f_1 f_2 = \theta^{-1}(g_1) \theta^{-1}(g_2).$$

So $\theta^{-1} : G \rightarrow F$ is an isomorphism. In particular, $G \cong F$. We have shown that \cong is symmetric.

Suppose that $F \cong G$ and $G \cong H$. Let $\theta : F \rightarrow G$ and $\phi : G \rightarrow H$ be isomorphisms. For $f_1, f_2 \in F$, we have

$$\phi(\theta(f_1 f_2)) = \phi(\theta(f_1)\theta(f_2)) = \phi(\theta(f_1))\phi(\theta(f_2)).$$

So $\phi \circ \theta : F \rightarrow H$ is an isomorphism. In particular, $F \cong H$. We have shown that \cong is transitive.

Quiz 3: *Wednesday 15 October.* Consider the group $D_{10} = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}$. How many subgroups does D_{10} have? Draw a diagram of the subgroup lattice.

Solution 3: In the problem solved immediate before the quiz, it was shown that all the elements of the form $a^i b$ have order 2 and the other four non-identity elements have order 5. By Lagrange's Theorem, all the proper subgroups of D_{10} are cyclic. So the subgroups are: D_{10} , $\langle a \rangle$, $\langle b \rangle$, $\langle ab \rangle$, $\langle a^2 b \rangle$, $\langle a^3 b \rangle$, $\langle a^4 b \rangle$, $\{1\}$. In particular, there are 8 subgroups. [Diagram of subgroup lattice omitted.]

Homework 2 due Friday 17th October

2.1: Let G and H be groups. Show that $G \times H \cong H \times G$.

2.2: Show that $S_4 \not\cong D_{24}$.

2.3: Let k be a positive integer and put $n = 2k$. Let a and b be elements of D_{2n} such that $a^n = b^2 = 1$ and $ba = a^{-1}b$. Show that if $k \geq 2$ then $Z(D_{2n}) = \{1, a^k\}$. Evaluate $Z(D_4)$.

2.4: Find the order of the element $(1, 2)(3, 4, 5)(6, 7, 8, 9, 10)$ of S_{10} .

Solution 2.1: There is an isomorphism $G \times H \ni (g, h) \leftrightarrow (h, g) \in H \times G$.

Solution 2.2: The group D_{24} has an element with order 12, but the maximum order of an element of S_4 is 4.

Solution 2.3: Write $Z = Z(D_{2n})$. Let i be an integer. Then $(a^i b)a(a^i b)^{-1} = a^{-1}$, so $a^i b \notin Z$. We have $ba^i b^{-1} = a^{-1}$, so $a^i \in Z$ if and only if i is divisible by k . Therefore $Z = \{1, a^k\}$. We have $D_4 = \{1, a, b, ab\}$ with $a^2 = b^2 = (ab)^2 = 1$. Therefore $D_4 \cong V_4$, which is abelian. In particular, $Z(D_4) = D_4$.

Solution 2.4: Let $g = (1, 2)(3, 4, 5)(6, 7, 8, 9, 10)$. Since $(1, 2)$ and $(3, 4, 5)$ and $(6, 7, 8, 9, 10)$ mutually commute, $g^n = (1, 2)^n(3, 4, 5)^n(6, 7, 8, 9, 10)^n$ for any integer n . By considering the actions on $\{1, 2\}$ and $\{3, 4, 5\}$ and $\{6, 7, 8, 9, 10\}$, we see that $g^n = 1$ if and only if n is divisible by 2 and 3 and 5. In other words, the order of g is 30.

Homework 3 due Friday 28th November

3.1: *Exercise 4.1.1 page 116:* Let G be a group acting on a set A . Let $a, b \in A$ and $g \in G$ such that $b = ga$. Show that $G_b = gG_a g^{-1}$. Deduce that, if G acts transitively on A , then the kernel of the action is $\bigcap_{g \in G} gG_a g^{-1}$.

3.2: *Exercise 4.1.3 page 116:* Let A be a set and let G be an abelian subgroup of $\text{Sym}(A)$ such that G acts transitively on A . Show that $ga \neq a$ for all $g \in G - \{1\}$ and $a \in A$. Deduce that $|G| = |A|$.

3.3: *Exercise 4.3.13 page 130:* Find, up to isomorphism, all the finite groups that have exactly 2 conjugacy classes.

3.4: *Exercise 4.3.25 page 131:* Let G be the group of invertible 2×2 matrices over \mathbb{C} . Consider the subgroup

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{C}, ac \neq 0 \right\}.$$

Show that every element of G is conjugate to some element of H . (You may assume standard results from linear algebra.)

Solution 3.1: Given $h \in G$ then the condition $h \in G_b$ is equivalent to the condition $hga = ga$, in other words, $g^{-1}hg \in G_a$. The first part is established. The rider holds because, assuming that G acts transitively, then the kernel of the action is the intersection of the stabilizers gG_ag^{-1} of the elements ga .

Solution 3.2: By the previous question, the kernel of the action of G on A is $1 = \bigcup_g gG_ag^{-1}$ for any $a \in A$. But A is abelian, so $gG_ag^{-1} = G_a$ for all a and G . Therefore $G_a = 1$, in other words, $ga \neq a$ when $g \neq 1$. By the Orbit-Stabilizer Equation, $|G| = |A|$.

Solution 3.3: Recall that, given a group G and letting g_1, \dots, g_k be representatives of the conjugacy classes of G , we have $1 = 1/|C_G(g_1)| + \dots + 1/|C_G(g_k)|$.

Plainly, the group C_2 has exactly 2 conjugacy classes. We shall show that, for every group G with exactly 2 conjugacy classes, $G \cong C_2$. Let $a \in G - \{1\}$. Then $1 = 1/|G| + 1/|C_G(a)|$. But $|G| \geq 2 \leq |C_G(a)|$. The only solution is $|G| = 2 = |C_G(a)|$. In particular, $G \cong C_2$.

Solution 3.4: The required conclusion is equivalent to the assertion that every 2×2 matrix over \mathbb{C} has an eigenvector over \mathbb{C} .

Quiz 4: *Wednesday 26 November.* Find the conjugacy classes of the group

$$D_{10} = \langle a, b : a^5 = b^2 = 1, bab^{-1} = a^{-1} \rangle = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}.$$

Solution 4: Noting that $aba^{-1} = a^2b$, we see that the conjugacy classes are

$$\{1\}, \quad \{a, a^4\}, \quad \{a^2, a^3\}, \quad \{b, ab, a^2b, a^3b, a^4b\}.$$

Quiz 5: *Friday 12 December.* Find the order of the group $\text{GL}_2(5)$.

Solution 5: Let $\{e, f\}$ be an ordered basis for the field $\mathbb{Z}/5\mathbb{Z}$. Each element $g \in \text{GL}_2(5)$ is determined by the elements $g(e)$ and $g(f)$. To choose g , there are $5^2 - 1$ choices for $g(e)$, then $5^2 - 5$ choices for $g(f)$. So the number of choices for g is $(5^2 - 1)(5^2 - 5) = 24 \cdot 20 = 480$.

Homework 4 to be discussed on Friday 26th December.

4.1: Classify, up to isomorphism, the groups with order 12.

4.2: Classify, up to isomorphism, the abelian groups with order 128.

4.3: Let $K \trianglelefteq G$ and let P be a Sylow p -subgroup of K . Show that $G = N_G(P)K$. (The idea, here, is called the **Frattini argument**.)

4.4: Let G be a finite non-trivial p -group.

(a) Show that $1 < Z(G)$.

(b) Show that there exists a strict normal subgroup $N \triangleleft G$ such that G/N is abelian.

Solution 4.1: We claim that, for a group G with order 12, there are exactly 5 possible isomorphism classes, namely

$$C_{12} \cong C_4 \times C_3, \quad V_4 \times C_3 \cong C_2 \times C_6, \quad C_4 \rtimes C_3, \quad V_4 \rtimes C_3 \cong D_{12}, \quad C_3 \rtimes V_4 \cong A_4$$

where all the semidirect products are the unique non-trivial semidirect products of the specified form. The case where G is abelian follows immediately from the Structure Theorem for Finite Abelian Groups. Let P and Q be, respectively, a Sylow 2-subgroup and a Sylow 3-subgroup of G . Note that $P \cong C_4$ or $P \cong V_4$. Also, $Q \cong C_3$. Let a be a generator of Q .

Suppose that G is non-abelian and $Q \triangleleft G$. By the Semidirect Product Recognition Theorem, $G \cong P \rtimes Q$. The only non-trivial automorphism of Q is $a \mapsto a^{-1}$. If $P \cong C_4$, say $P = \langle w \rangle$, then the only way of constructing a non-trivial semidirect product is to impose the relation $w a = a^{-1} w$. If $P \cong V_4$ then there are 3 choices of non-trivial automorphism $P \rightarrow \text{Aut}(Q)$, but all of them yield the same group up to isomorphism, $P \rtimes Q \cong D_{12}$.

Suppose that Q is not normal. Then, by Sylow's Theorem, the number of Sylow 3-subgroups of G must be 4. So the number of elements of G with order 3 is 8. There are only 4 other elements of G , so $P \triangleleft G$. Since $\text{Aut}(C_4) \cong C_2$, which has no elements with order 3, we must have $P \cong V_4$. The only non-trivial way in which a can act on the non-trivial elements of P is as a 3-cycle. Therefore, $G \cong A_4$.

Solution 4.2: By the Structure Theorem for Finite Abelian Groups, any abelian group with order 128 is isomorphic to $(\mathbb{Z}/2^{n_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/2^{n_r}\mathbb{Z})$ for some positive integers n_1, \dots, n_r such that $n_1 + \dots + n_r = 7$. The form is unique upon imposing the condition $n_1 \geq \dots \geq n_r$. So the number of isomorphism classes is equal to the number of partitions of 7. We have

$$\begin{aligned} 7 &= 6+1 = 5+2 = 5+1+1 = 4+3 = 4+2+1 = 4+1+1+1 = 3+3+1 = 3+2+2 = 3+2+1+1 \\ &= 3+1+1+1+1 = 2+2+2+1 = 2+2+1+1+1 = 2+1+1+1+1+1 = 1+1+1+1+1+1+1. \end{aligned}$$

Evidently, the number of isomorphism classes is 15.

Solution 4.3: Given $g \in G$ then, by the uniqueness clause of Sylow's Theorem, there exists $k \in K$ such that ${}^g P = {}^k P$. We have $k^{-1} g \in N_G(P)$, hence $g \in KN_G(P) = N_G(P)K$.

Solution 4.4: Part (a). By the Orbit-Stabilizer Equation, every conjugacy class has order a power of p . But $|G|$ is divisible by p . So the number of singleton conjugacy classes is divisible by p . The union of the singleton conjugacy classes is $Z(G)$. We have shown that $|Z(G)|$ is divisible by p .

Part (b). If G is abelian, then the required conclusion is trivial. Suppose that G is not abelian. Invoking part (a) then, by an inductive argument on $|G|$, the quotient $G/Z(G)$ has a strict normal subgroup L such that $(G/Z(G))/L$ is abelian. Letting $H = \{h \in G : hZ(G) \in L\}$, then $H \triangleleft G$. Also, $H/Z(G) = L$ and, by the Third Isomorphism Theorem, $G/H \cong (G/Z(G))/L$.

Time allowed: 110 minutes. Please put your name on EVERY sheet of your manuscript. The use of telephones, calculators or other electronic devices is prohibited. The use of very faint pencils is prohibited too. You may take the question sheet home.

1: 20 points. Write down the orders and inverses of each of the 16 elements of the group $\mathbb{Z}/16\mathbb{Z}$. (No proofs are required. Just state the answers.)

2: The number $257 = 2^8 + 1$ is prime. Consider the multiplicative group

$$(\mathbb{Z}/257\mathbb{Z})^\times = \{[1], [2], \dots, [255], [256]\}.$$

(a), 10 points. Using the Euclidian algorithm, find the inverse of $[19]$ in $(\mathbb{Z}/257\mathbb{Z})^\times$.

(b), 5 points. You may assume that $19^{128} \equiv -1$ modulo 257. What is the order of the element $[19]$ of $(\mathbb{Z}/257\mathbb{Z})^\times$? (Do not forget to justify your answer.)

3: Let G be a finite group with subgroups H and K such that $|G|/|K| = 2$ and H is not contained in K .

(a), 10 points. Show that K is a normal subgroup of G .

(b), 10 points. Show that $H/(H \cap K) \cong C_2$.

4: The dihedral group with order 10 is the group $D_{10} = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}$ with $a^5 = b^2 = 1$ and $ba = a^{-1}b$.

(a), 10 points. Find all the subgroups of D_{10} .

(b), 5 points. Using Lagrange's theorem, explain why your list of subgroups is complete.

(c), 10 points. Draw a diagram of the subgroup lattice of D_{10} .

5: A group F is said to be **metabelian** provided F has an abelian normal subgroup A such that F/A is abelian.

(a), 10 points. Show that any subgroup of a metabelian group is metabelian.

(b), 10 points. Let $H \trianglelefteq G \triangleright K$ be groups such that G/H and G/K are metabelian. Show that $G/(H \cap K)$ is metabelian.

Bonus Question: 10 points. (This question is very hard. You are advised not to spend time on it unless you have finished the questions above.) Let G be a finite group, let p be the smallest prime number dividing $|G|$, and let $H \leq G$ such that $|G|/|H| = p$. Show that H is a normal subgroup of G . (Hint: Consider the action of G on the set of left cosets of H in G . Construct a group homomorphism from G to the symmetric group S_p .)

Midterm 1 Solutions, version 10 November 2014

There is no such thing as a “model solution”. Often, there are many good ways of deducing a given conclusion.

1: The orders and inverses of each element $x \in \mathbb{Z}/16/\mathbb{Z}$ are as shown in the table.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
order of x	1	16	8	16	4	16	8	16	2	16	8	16	4	16	8	16
inverse of x	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

2: We have $257 = 13 \cdot 19 + 10$ and $19 = 1 \cdot 10 + 9$ and $10 = 1 \cdot 9 + 1$. Now

$$1 = 10 - 9 = 10 - (19 - 10) = 2 \cdot 10 - 19 = 2 \cdot (247 - 13 \cdot 19) - 19 = 2 \cdot 257 - 27 \cdot 19 .$$

So $[19]^{-1} = [-27] = [230]$.

3: Part (a). Let $g \in G$. If $g \in K$ then $gK = K = Kg$. If $g \notin K$ then $gK = G - K = Kg$.

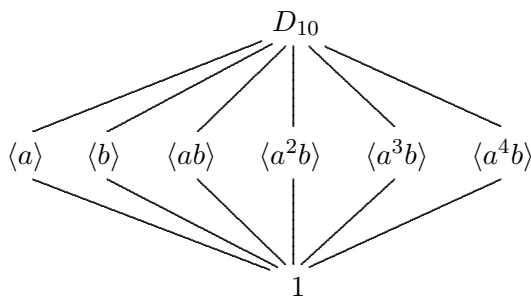
Part (b). We have $K < HK \leq G$. The integer $|G|/|HK|$ is smaller than $|G|/|K|$ and divides $|G|/|K|$. But $|G|/|K| = 2$. So $HK = G$. The group $HK/K = G/K$, being of order 2, must be isomorphic to C_2 . The Second Isomorphism Theorem says that $H/(K \cap H) \cong HK/K$.

4: Part (a). The subgroups of D_{10} are:

$$1 = \{1\}, \quad \langle a \rangle \cong C_5, \quad \langle b \rangle \cong C_2, \quad \langle ab \rangle \cong C_2, \quad \langle a^2b \rangle \cong C_2, \quad \langle a^3b \rangle \cong C_2, \quad \langle a^4b \rangle \cong C_2, \quad D_{10} .$$

Part (b). Plainly, the elements a, a^2, a^3, a^4 are of order 5. It is easy to see that all elements having the form $a^i b$ are of order 2. By Lagrange’s Theorem, every proper subgroup of D_{10} has order 2 or 5. Since 2 and 5 are prime, every proper subgroup must be cyclic. Noting that $\langle a \rangle = \langle a^2 \rangle = \langle a^3 \rangle = \langle a^4 \rangle = \{1, a, a^2, a^3, a^4\}$, it is clear that we have listed all the cyclic subgroups of G .

Part (c). The subgroup lattice of D_{10} is as shown.



5: Part (a). Let F and A be as specified and let $H \leq F$. Define $B = H \cap A$. Then B is abelian because it is a subgroup of the abelian group A . Also, H/B is abelian because F/A is abelian and, by the Second Isomorphism Theorem, $H/B \cong HA/A \leq F/A$. We have shown that H is metabelian.

Part (b). It is easy to see that the direct product of two metabelian groups is metabelian. Consider the homomorphism $\theta : G \rightarrow G/H \times G/K$ such that $\theta(g) = (gH, gK)$ for $g \in G$. The kernel of θ is $H \cap K$. Hence, via the First Isomorphism Theorem, $G/(H \cap K)$ is isomorphic to

a subgroup of the metabelian group $G/H \times G/K$. The required conclusion now follows from part (a).

Bonus Question: *Proof 1:* Enumerate the left cosets of H in G as a_1H, \dots, a_pH . Let $\theta : G \rightarrow S_p$ be the function $g \mapsto \sigma_g$ where $ga_iH = a_{\sigma_g(i)}H$ for each integer $1 \leq i \leq p$. Given $f, g \in G$, then $a_{\sigma_{fg}(i)}H = fga_iH = fa_{\sigma_g(i)}H = a_{\sigma_f(\sigma_g(i))}H$. So $\sigma_{fg} = \sigma_f \circ \sigma_g$, in other words, θ is a homomorphism. Let $K = \ker(\theta)$. The integers $|G|$ and $|S_p| = p!$ are divisible by the order of the group $G/K \cong \text{Im}(\theta)$. Hence, thanks to the hypothesis on p , we have $|G|/|K| \in \{1, p\}$. But $K \leq H < G$, so $|G|/|K| = p$. Therefore $|K| = |H|$. We have shown that the normal subgroup K coincides with H . \square

The ideas in the latest proof will be easier to follow and will seem more natural when we have spent more time on the notion of a permutation set. Let us present the same proof again, but in a smoother way which makes use of that notion.

Proof 2: Let \mathcal{R} be the set of left cosets of H in G . We allow G to act on \mathcal{R} such that an element $g \in G$ sends a coset aH to the coset gaH . The action is represented by a homomorphism $\theta : G \rightarrow \text{Sym}(\mathcal{R})$ where $\text{Sym}(\mathcal{R})$ is the group of permutations of \mathcal{R} . Let $K = \ker(\theta)$. Obviously, $|G : K|$ divides $|G|$. By the First Isomorphism Theorem, $|G : K|$ divides the integer $p! = |\text{Sym}(\mathcal{R})|$. Since p is the smallest prime divisor of $|G|$ and $K \leq H < G$, we have $|G : K| = p = |G : H|$. Therefore $K = H$. \square

Time allowed: 110 minutes. Please put your name on EVERY sheet of your manuscript. The use of telephones, calculators or other electronic devices is prohibited. The use of very faint pencils is prohibited too. You may take the question sheet home.

1: 20 points. How many conjugacy classes are there in the group D_8 (the dihedral group with order 8)?

2: 20 points. How many conjugacy classes are there in the group S_7 (the symmetric group with degree 7)? How many of those conjugacy classes are contained in the group A_7 (the alternating group with degree 7)?

3: 15 points. Let p be an odd prime. Show that the alternating group A_p has exactly 2 conjugacy classes of elements with order p .

4: Recall that, for a finite group G , a Sylow p -subgroup of G is a subgroup S of G such that $|S|$ is a power of p and $|G : S|$ is coprime to p .

(a), 10 points. State Sylow's Theorem (sometimes called Sylow's Three Theorems) about the Sylow p -subgroups of G . (Do not prove the theorem. Just state it.)

(b), 15 points. Let P be a p -subgroup of G (a subgroup of G such that $|P|$ is a power of p). Show that P is contained in a Sylow p -subgroup of G . (Hint: consider the conjugation action of P on the set of Sylow p -subgroups of G .)

5: 20 points. Show that there does not exist a simple group with order 30. (Hint: consider the number of Sylow 3-subgroups and the number of Sylow 5-subgroups.)

Bonus Question: 10 points. (This question is very hard. You are advised not to spend time on it unless you have finished the questions above.) Let p be a prime and let G be the group of invertible 3×3 matrices with entries in $\mathbb{Z}/p\mathbb{Z}$. Show that every subgroup of G with

order p^3 is isomorphic to the subgroup $\left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} : x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\}$.

Midterm 2 Solutions

There is no such thing as a "model solution". Often, there are many good ways of deducing a given conclusion.

1: Write $D_8 = \langle a, b : a^4 = b^2 = 1, bab^{-1} = a^{-1} \rangle$. Of course, $[1] = \{1\}$. It is easy to see that $Z(D_8) = \{1, a^2\}$. So $[a^2] = \{a^2\}$. Since the elements a and $a^3 = bab^{-1}$ are the only elements with order 4, we have $[a] = \{a, a^3\}$. We have $a^r b b (a^r b)^{-1} = a^{2r} b$, so $[b] = \{b, a^2 b\}$. The union of the conjugacy classes noted thus far omits only ab and $a^3 b$. Since those two elements are non-central, they must belong to the same conjugacy class. In conclusion, there are 5 conjugacy classes: $\{1\}$ and $\{a^2\}$ and $\{a, a^3\}$, and $\{b, a^2 b\}$ and $\{ab, a^3 b\}$.

More systematic alternative solution: Write $D_8 = \langle a, b \rangle$ where $a^4 = b^2 = (ab)^2 = 1$. We have $bab^{-1} = a^3$, so $[a] \supseteq \{a, a^3\}$. Also, $|C(a)| = |\langle a \rangle| = 4$, hence $|[a]| = 2$. We deduce that $[a] = \{a, a^3\}$. We have $aba^{-1} = a^2b$ and $C(b) = \{1, b, a^2, a^2b\}$, hence $[b] = \{b, a^2b\}$. Similarly, $[ab] = \{ab, a^3b\}$. Finally, $C(a^2) = D_8$, hence $[a^2] = \{a^2\}$. We have shown that $\{a, b, a^2b, a^2, 1\}$ is a set of representatives of the conjugacy classes. In particular, the number of conjugacy classes of D_8 is 5.

2: The 8 even partitions of 7 are

$$7, \quad 5+1+1, \quad 4+2+1, \quad 3+3+1, \quad 3+2+2, \\ 3+1+1+1+1, \quad 2+2+1+1+1, \quad 1+1+1+1+1+1+1.$$

The 7 odd partitions of 7 are

$$6+1, \quad 5+2, \quad 4+3, \quad 4+1+1+1, \quad 3+2+1+1, \quad 2+2+2+1, \quad 2+1+1+1+1+1.$$

So S_7 has $8+7=15$ conjugacy classes, 8 of which are contained in A_7 .

3: The elements with order p in S_p are the p -cycles. There are $(p-1)!$ of them. So, letting x be a p -cycle, $|C_{S_p}(x)| = |S_p|/(p-1)! = p$. It follows that $C_{S_p}(x) = \langle x \rangle = C_{A_p}(x)$. Therefore $|[x]_{A_p}| = |A_p|/p = |[x]_{S_p}|/2$.

4: Part (a). Let p be a prime and let G be a finite group. Write $|G| = p^a m$ where p does not divide m . Then G has a Sylow p -subgroup. The Sylow p -subgroups of G are mutually conjugate. The number of Sylow p -subgroups of G divides m and is congruent to 1 modulo p .

Part (b). Letting P act by conjugation on the set of Sylow p -subgroups of G , then the order of every orbit is a divisor of $|P|$ and is, in particular, a power of p . But the number of Sylow p -subgroups is not divisible by p . Therefore, the conjugation action of P stabilizes some Sylow p -subgroup S . In other words, $P \leq N_G(S)$. Applying the Second Isomorphism Theorem to P and S as subgroups of $N_G(S)$, we deduce that PS is a subgroup and $PS/S \cong P/(P \cap S)$. It follows that PS is a p -subgroup of G . On the other hand, by Lagrange's Theorem, $|PS| \leq |S|$. We deduce that $PS = S$, in other words, $P \leq S$.

5: Suppose, for a contradiction, that there exists a simple group G with order 30. Let n_3 and n_5 be the number of Sylow 3-subgroups and the number of Sylow 5-subgroups, respectively. The conjugation action of G on the Sylow 3-subgroups of G yields a non-trivial group homomorphism $G \rightarrow S_{n_3}$. But G is simple so, by the First Isomorphism Theorem, $n_3! = |S_{n_3}| \geq |G| = 30$. So $n_3 \geq 4$. A similar argument shows that $n_5 \geq 4$. In fact, since $n_5 \equiv 1$ modulo 5, we have $n_5 \geq 6$.

Each Sylow 3-subgroup owns 2 elements with order 3. So G has $2n_3$ elements with order 3. But $n_3 \geq 4$, so G has at least 8 elements with order 3. Similarly, since each Sylow 5-subgroup owns 4 elements with order 5 and $n_5 \geq 6$, there are at least $4 \cdot 6 = 24$ elements of G with order 5. In conclusion, G has at least $8+24=32$ elements with order 3 or 5. This contradicts the hypothesis that $|G| = 30$.

LJB, 31 December 2014, Bilkent University.

Time allowed: 110 minutes. Please put your name on EVERY sheet of your manuscript. The use of telephones, calculators or other electronic devices is prohibited. The use of very faint pencils is prohibited too. You may take the question sheet home.

1: 24 marks. Let p be an odd prime. Consider the dihedral group D_{2p} with order $2p$.

- (a) How many subgroups does D_{2p} have?
- (b) How many normal subgroups does D_{2p} have?
- (c) How many conjugacy classes of elements does D_{2p} have?

2: 12 marks. Let G be a finite group with a subgroup H such that $H \cong A_5$. Let $N \trianglelefteq G$. Show that $H \leq N$ or $|N| \leq |G : H|$.

3: 24 marks. (a) State the Orbit-Stabilizer equation for a finite group G acting on a transitive G -set.

(b) Let x_1, \dots, x_k be representatives of the conjugacy classes of a finite group G . Simplify the expression $\sum_{i=1}^k 1/|C_G(x_i)|$.

(c) Classify the conjugacy classes of the group S_6 and find the sizes of each conjugacy class. Directly check your answer to part (b) in this case.

4: 20 marks. Find the conjugacy classes of the group A_6 . Hence show that A_6 is simple. (Hint: Question 2 is not needed but it may be helpful.)

5: 20 marks. Let G be a group with order $p^a m$ where p is prime and p does not divide m . Suppose that, given any two Sylow p -groups S and T of G , then $S = T$ or $S \cap T = \{1\}$. Show that the number of Sylow p -groups of G is congruent to 1 modulo p^a . (Hint: Adapt part of the proof of Sylow's Theorem.)

Time allowed: 2 hours. Please put your name on EVERY sheet of your manuscript. The use of telephones, calculators or other electronic devices is prohibited. The use of very faint pencils is prohibited too. You may take the question sheet home.

- 1: 20 marks.** (a) State the Structure Theorem for Finitely Generated Abelian Groups.
(b) Up to isomorphism, how many abelian groups are there of order $2^5 3^4 = 2592$?

2: 15 marks. Let A be an abelian group. An element $a \in A$ is called a **torsion element** provided $a^n = 1$ for some positive integer n . Let $T(A)$ be the set of torsion elements of A .

- (a) Show that $T(A)$ is a normal subgroup of A .
(b) Show that, if A is finitely generated, then $T(A)$ is finite.
(c) Give an example of an abelian group A such that $T(A)$ is infinite.

3: 30 marks. Let G be a group. Recall that we define an **automorphism** of G to be an isomorphism $G \rightarrow G$. Let $\text{Aut}(G)$ denote the group of automorphisms of G . Given $g \in G$, then the automorphism sending each element $x \in G$ to the element ${}^g x \in G$ is called an **inner automorphism** of G . Let $\text{Inn}(G)$ denote the group of inner automorphisms of G .

- (a) Show that $G/Z(G) \cong \text{Inn}(G)$.
(b) Show that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.
(c) Let $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$. Find $\text{Out}(G)$, up to isomorphism, in the case where $G = S_3$.

4: 35 marks. Let G be the group of invertible 3×3 matrices over the field $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. You may assume that the conjugacy classes of G have sizes 1, 21, 56, 42, 24, 24 and that the elements of those conjugacy classes have orders 1, 2, 3, 4, 7, 7, respectively.

- (a) Show that, for each $p \in \{2, 3, 7\}$, the group G is generated by the elements with order p .
(b) From part (a), deduce that G is simple.
(c) How many Sylow 7-subgroups does G have?
(d) How many Sylow 3-subgroups does G have?
(e) Show that, given an element $g \in G$ such that g has order 2, then $C_G(g)$ is a Sylow 2-subgroup of G .
(f) Find the Sylow 2-subgroups of G up to isomorphism.
(g) How many Sylow 2-subgroups does G have?

Solutions to Final

The following are just examples of solutions. Of course, a mathematical result may admit many different good proofs. A proof may admit many different good presentations.

1: Part (a). Every finitely generated abelian group A is isomorphic to a direct product $C^n \times C_{q_1} \times \dots \times C_{q_r}$ where q_1, \dots, q_r are prime-powers and C^n denotes the direct product of n copies of the infinite cyclic group. Furthermore, given A , then n is unique and, up to renumbering, q_1, \dots, q_r are unique.

Part (b). By part (a), the number isomorphism classes of abelian groups with order 2^5 is equal to $p(5)$, the number of partitions of 5. Noting that

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1,$$

we see that $p(5) = 7$. Similarly, noting that $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$, we see that there are $p(4) = 5$ isomorphism classes of abelian groups with order 2^4 . Any abelian group A with order $2^5 3^4$ is the direct product of its Sylow 2-subgroup and its Sylow 3-subgroup. So the number of isomorphism classes of such groups A is $7 \cdot 5 = 35$.

2: Part (a) is trivial, because A is abelian. Part (b) follows immediately from the above Structure Theorem. For part (c), one example is the direct product of infinitely many copies of G , where G is any non-trivial finite abelian group.

3: For $g \in G$, let θ_g be the inner automorphism sending $x \in G$ to $g x g^{-1}$. Part (a) follows from the First Isomorphism Theorem because the homomorphism $G \ni g \mapsto \theta_g \in \text{Aut}(G)$ has kernel $Z(G)$. Part (b) holds because, for $\phi \in \text{Aut}(G)$, then $(\phi \theta_g)(x) = \phi(g) \phi(x) \phi(g)^{-1} = (\theta_{\phi(g)} \phi)(x)$, hence $\phi \theta_g = \theta_{\phi(g)} \phi$. For part (c), write $S_3 = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$. Any automorphism ϕ of S_3 must send a to a or a^2 . Also, ϕ must send b to b or ab or $a^2 b$. The values of ϕ at the generating elements a and b determine ϕ . Therefore $|\text{Aut}(S_3)| \leq 6$. But each element of S_3 yields a unique inner automorphism of S_3 . Therefore $\text{Inn}(S_3) = \text{Aut}(S_3) \cong S_3$. We deduce that $\text{Out}(S_3)$ is trivial.

4: Let $\mathcal{C}_1, \dots, \mathcal{C}_6$ be the conjugacy classes, enumerated such that the elements have orders 1, 2, 3, 4, 7, 7, respectively. Thus, the sizes of $\mathcal{C}_1, \dots, \mathcal{C}_6$ are 1, 21, 56, 42, 24, 24, respectively. We have $|G| = 1 + 21 + 56 + 42 + 24 + 24 = 168$.

Part (a). Let G_p be the normal subgroup of G generated by the elements with order p . We have $G_7 \supseteq \mathcal{C}_1 \cup \mathcal{C}_5 \cup \mathcal{C}_6$ and, in particular, $|G_7| \geq |\mathcal{C}_1| + |\mathcal{C}_5| + |\mathcal{C}_6| = 49$. But $|G_7|$ divides 168 and $|G_7| - 49$ must be a sum of numbers in $\{|\mathcal{C}_2|, |\mathcal{C}_3|, |\mathcal{C}_4|\} = \{21, 56, 42\}$. The only possibility is $|G_7| = 168$, in other words $G_7 = G$. A similar argument shows that $G_3 = G$.

We have $G_2 \supseteq \mathcal{C}_2$. In particular, $|G_2| > 8$. Therefore $|G_2|$ is divisible by q for $q = 3$ or $q = 7$. Since $G_2 \trianglelefteq G$ and the Sylow q -subgroups of G are cyclic with order q , we deduce that G_2 contains all the Sylow q -subgroups of G . In other words $G_2 \subseteq G_q$. But we have already show that $G_q = G$. Therefore, $G_2 = G$.

Part (b). Let N be a non-trivial normal subgroup of G . Then N must own an element of prime order p . Since the subgroups of G with order p are mutually conjugate, N must contain G_p . By part (a), $N = G$.

Part (c). Counting elements with order 7, we see that there are $48/6 = 8$ Sylow 7-subgroups.

Part (d). Similarly, the number of Sylow 3-subgroups is $56/2 = 28$.

Part (e). We have $|G : C_G(g)| = |[g]_G| = 21$, so $|C_G(g)| = 8$.

Part (f). Let P be a Sylow 2-subgroup. Arguing as in part (e), we see that, given an element h of G with order 4, then $|C_G(h)| = 4$. That is to say, $C_G(h) = \langle h \rangle$. So P is non-abelian, in other words, $P \cong Q_8$ or $P \cong D_8$. If $P \cong Q_8$, then every element with order 2 must have at least 6 square roots. This is impossible, because the number of elements with order 4 is only twice the number of elements with order 2. Therefore, $P \cong D_8$.

Part (g). There is a bijective correspondence $g \leftrightarrow P$ between the elements g with order 2 and the Sylow 2-subgroups P . The bijective correspondence is characterized by the condition that $P = C_G(g)$, equivalently, $\langle g \rangle = Z(P)$. So the number of Sylow 2-subgroups is $|C_2| = 21$.