Archive of documentation for

MATH 323, Algebra 1

Bilkent University, Fall 2016, Laurence Barker

version: 16 January 2017

Source file: arch323fall16.tex

Course specification

MATH 323, Algebra I, Fall 2016

Laurence Barker, Bilkent University. Version: 20 October 2016

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: Serious mathematics cannot be learned just by listening in class and copying homeworks. To take in the concepts and techniques, you have to take notes in class, study the notes, and do plenty of exercises on your own.

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

Course Texts:

Primary: D. S. Dummit, R. M. Foote, "Abstract Algebra", 3th Edition. (Wiley, 2004).

Secondary: Walter Ledermann, Alan Jeffrey Weir, "Introduction to Group Theory", 2nd edition, (Longman, 1996).

Secondary: P. BḂhattacharya, S. K. Jain, S. R. Nagpaul, "Basic Abstract Algebra", 2nd edition, (Cambridge University Press, 1994).

Classes: Room SAZ 20, Tuesdays, 15:40 - 16:30, Fridays, 13:40 - 15:30.

Office Hours: Tuesdays, 16:40 - 17:30. Sometimes in the classroom SAZ 20, sometimes in my office, SA-129, choice made at end of Tuesday class according to demand.

If you are having difficulty with the course, then you must come to see me. One major cause of difficulty is having done insufficient work earlier in then semester, then finding that one cannot understand anything much. That is perfectly normal, not a crime. Seeking help and trying to catch up is better than just accepting defeat.

Syllabus:

Week number: Monday date: Subtopics. Section numbers

1: 19 Sep: (Friday 23rd is first day of classes.) Some historical comments. Definition of a group. Some examples. **1.1, 1.2, 1.3**.

2: 26 Sep: Classifying groups of small order, unsystematically. Group isomorphism **1.6**.

3: 3 Oct: Euclidian algorithm, Chinese Remainder Theorem, Euclidian algorithm. Subgroups **2.1**. The subgroups of a cyclic group. **2.3, 2.4**.

4: 10 Oct: Only for abelian groups: Lagrange's Theorem **3.1**. Homomorphisms and quotient groups for abelian groups, **3.2**.

5: 17 Oct: Only for abelian groups: The Three Isomorphism Theorems **3.3**, the Direct Product Recognition Theorem **5.4**, Sylow's Theorem **4.5.**

6: 24 Oct: (Friday 28, no classes.) For arbitrary groups: Lagrange's Theorem, classification of groups of order up to 11, **3.1**.

7: 31 Oct: For arbitrary groups: The Three Isomorphism Theorems **3.3**, the Direct Product Recognition Theorem **5.4**.

8: 7 Nov: Review and Midterm 1 on Friday 11 November.

9: 14 Nov: Permutation Sets, Platonic solids, Orbit Stabilizer Equation, **4.1**

10: 21 Nov: Conjugacy classes, centralizers, normalizers **2.2**. The class equation and the groups $\mathrm{Inn}(G) \cong G/Z(G)$ and $\mathrm{Out}(G) \cong \mathrm{Aut}(G)/\mathrm{Inn}(G)$, **4.3, 4.4**.

11: 28 Nov: Finite p-groups, **6.1**. Two proofs of Sylow's Theorem and applications **4.5**.

12: 5 Dec: The symmetric and alternating groups. The simplicity of most of the alternating groups, **4.6**.

13: 12 Dec: Review and Midterm 2 on Friday 9th December.

14: 19 Dec: Structure Theorem for Finite Abelian groups, **5.1, 5.2:**

15: 26 Dec: (Friday 30 is last day of classes.) Holder-Jordan Theorem. Discussion of simple finite groups, **3.4**.

Assessment:

- Quizzes, Homework and Participation 15%.
- Midterm I, 25%, Friday 11th November.
- Midterm II, 25%, Friday 9th December.
- Final, 35%.

75% attendance is compulsory. Attendance will be assessed through quiz returns.

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

Homeworks and Quizzes

MATH 323, *Algebra 1*, Fall 2016

Laurence Barker, Mathematics Department, Bilkent University,
version: 27 December 2016

Office Hours: Tuesdays, 16:40 - 17:30 following the one-hour class. Usually in the classroom, otherwise in my office, room SA-129 (in the same building as the classroom). For all students, flying easily, struggling desperately or anywhere in-between, this is the time and place to discuss algebra, talk about coursework, or ask me for help with the homeworks.

Homework 1 due Friday 14 October.

Reminder 1: For a positive integer n, we define the **cyclic group** of order n to be the group $C_n = \{1, a, a^2, ..., a^{n-1}\}$ where $a^n = 1$. Writing $\mathbb{Z}/n$ to denote the ring of modulo n integers, we let $(\mathbb{Z}/n)^\times$ denote the group of invertible elements of $\mathbb{Z}/n$. In class, we observed that

$$(\mathbb{Z}/8)^\times = \{1, 3, 5, 7\} \cong V_4 \cong C_2 \times C_2 \; , \qquad (\mathbb{Z}/9)^\times = \{1, 2, 4, 5, 7, 8\} \cong C_6 \cong C_2 \times C_3 \; .$$

Reminder 2: In class, we found that, up to isomorphism, the groups of order 5 are C_1, C_2, C_3, C_4, V_4, C_5. We have also found two groups with order 6, namely C_6 and S_3. Later, we will prove that there are no other groups with order 6.

1.1: Up to isomorphism, express the groups $(\mathbb{Z}/15)^\times$ and $(\mathbb{Z}/16)^\times$ and $(\mathbb{Z}/17)^\times$ as direct products of cyclic groups.

1.2: Prove the following group-theoretic version of the Chinese Remainder Theorem: given coprime positive integers m and n, then

$$C_{mn} \cong C_m \times C_n \; .$$

1.3: Find, up to isomorphism, all the groups with order 7 or 8 or 9. (Hint: use Lagrange's Theorem.)

Homework 2 due Friday 28 October.

1.1: Find:
(a) the inverse of 3 in $(\mathbb{Z}/7)^\times$,
(b) the inverse of 7 in $(\mathbb{Z}/31)^\times$,
(c) the inverse of 31 in $(\mathbb{Z}/127)^\times$.

2.2: Prove the following converse to the abelian case of Lagrange's Theorem: given a finite abelian group A and a divisor m of $|A|$, then A has a subgroup B with order $|B| = m$.

2.3: Consider the group $\mathbb{Q}$ under addition. For each positive integer n,
(a) How many elements of order n are there in $\mathbb{Q}$?
(b) How many elements of order n are there in the quotient group $\mathbb{Q}/\mathbb{Z}$?
(c) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order.

Homework 3 due Tuesday 6th December.

3.1: Let G be a group and X a G-set. Define a relation $=_G$ on X such that, given $x, y \in X$, then $x =_G y$ provided $x = gy$. Show that $=_G$ is an equivalence relation.

3.2: Find the group of rotational symmetries and the group of rigid symmetries of the cube and the octahedron.

3.3: Find those two symmetry groups for the dodecahedron and the icosahedron.

Quizzes

1: 7 Oct. Show that any group homomorphism preserves identity elements and inverses.

2: 4 Nov. For $H \leq G \trianglerighteq K$, show that $K \trianglelefteq HK \leq G$.

3: 25 Nov. Give a geometric description, in terms of the regular tetrahedron, of a set of size 3 that is naturally permuted by the S_3 quotient of the group of rigid symmetries S_4.

4: 20 Dec. Show that every element of S_n can be expressed as a product of at most $n-1$ transpositions.

5: 23 Dec. How many conjugacy classes does S_6 have?

Revision Questions for Final, which are not to be marked.

0: Let G be a simple group with order 660. How many Sylow 11-subgroups does G have?

To do the Final in the file arch323fall14.pdf, the following information will be helpful: given a subset S of a group G, we define the **subgroup generated by** S, denoted $\langle S \rangle$, to be the smallest subgroup of G such that $S \subseteq \langle S \rangle$. When $\langle S \rangle = G$, we call S a **generating set** for G. When G has a finite generating set, we say that G is **finitely generated**. (The additive group of real numbers $(\mathbb{R}, +)$ is an example of an abelian group that is not finitely generated.)

Also recall, a group C is said to be **cyclic** provided C has a generating set with size 1. The infinite cyclic group C_∞ is unique up to isomorphism. The additive group $(\mathbb{Z}, +)$ is an isomorphic copy of C_∞.

Structure Theorem for Finitely Generated Abelian Groups: *Let A be a finitely generated abelian group. Then $A \cong C_{q_1} \times ... \times C_{q_s}$ where each q_i is either ∞ or a power of a prime. Furthermore, the direct product decomposition is unique in that, if $A \cong C_{r_1} \times ... \times C_{r_t}$, then $s = t$ and there is a permutation $\sigma \in S_s$ such that each $r_i = q_{\sigma(i)}$.*

MATH 323: Algebra I. Midterm 1. LJB, 11 November 2016, 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.

Remember to justify your answers, except in any cases where your answers are obvious.

1: 25 marks. (a) Find the inverse of 5 in the multiplicative group of units $(\mathbb{Z}/127)^\times$.

(b) Find the orders of the elements 2 and 19 in $(\mathbb{Z}/127)^\times$.

(c) How many elements of order 2 are there in $(\mathbb{Z}/127)^\times$?

(d) What are the prime numbers p such that $(\mathbb{Z}/127)^\times$ has an element of order p?

(e) Find the inverse of 2234 in $(\mathbb{Z}/8191)^\times$.

2: 32 marks. Which of the following statements hold for all subgroups B of all finite abelian groups A? (In each case, give a proof or a counter-example.)

(a) If A is cyclic, then B and A/B are cyclic.

(b) If B and A/B are cyclic, then A is cyclic.

(c) If A has a subgroup of order 127, then B or A/B has a subgroup of order 127.

(d) If B or A/B has a subgroup of order 127, then A has a subgroup of order 127.

3: 21 marks. Let G be a finite group with normal subgroups H and K. Let $\theta : G \to G/H \times G/K$ be the function such that $\theta(g) = (gH, gK)$ for each $g \in G$.

(a) Show that θ is a group homomorphism.

(b) Show that, if the positive integers $|G|/|H|$ and $|G|/|K|$ are coprime, then θ is surjective.

(c) In the case where θ is surjective, express $|H \cap K|$ in terms of $|G|$ and $|H|$ and $|K|$.

4: 22 marks. Let G be a finite group. We say that G is **perfect** provided every abelian quotient group of G is trivial. Show that G has a perfect normal subgroup N such that every perfect normal subgroup of G is contained in N.

Midterm 1 Solutions

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

1: Part (a). We have $127 = 25.5 + 2$ and $5 = 2.2 + 1$, hence

$$1 = 5 - 2.2 = 5 - 2(127 - 25.5) = 51.5 - 2.127 \ .$$

Therefore, in this group of units, $5^{-1} = 51$.

Part (b). For $1 \leq n \leq 6$, we have $2 \leq 2^n \leq 64$, perforce, $2^n \not\equiv 1$ modulo 127. But $2^7 = 128 \equiv 1$. So the order of 2 is 7.

We have $3.127 = 381$ and $19^2 = 361 = 381 - 20$ and $19.20 = 380 = 381 - 1$. Therefore $19^3 \equiv 1$ and 19 has order 3.

Part (c). We shall show that there is exactly 1 element of order 2. Let x be an integer such that $x^2 \equiv 1$ modulo 127. Then 127 divides the integer $x^2 - 1 = (x+1)(x-1)$. Since 127 is prime, it divides $x + 1$ or $x - 1$. In other words, $x \equiv 1$ or $x \equiv -1$. In the former case, x has order 1. Therefore the congruence class of $-1 \equiv 126$ is the unique element with order 2.

Part (d). The set of such p is $\{2, 3, 7\}$. Indeed, in parts (b) and (c) we saw that the elements 126, 19, 2 have orders 2, 3, 7, respectively. On the other hand, $|(\mathbb{Z}/127)^\times| = 126 = 2.3.3.7$, whereupon Lagrange's Theorem informs us that no element of the group has order divisible by a prime distinct from 2, 3, 7.

Part (e). We have $8191 = 4.2234 - 745$ and $2234 = 3.745 - 1$, hence

$$1 = 3.745 - 2234 = 3(4.2234 - 8191) - 2234 = 11.2234 - 3.8191 \ .$$

Therefore, $2234^{-1} = 11$.

Comment: Of course, part (e) can also be done using only positive remainders, exactly as in lectures, starting with $8191 = 3.2234 + 1489$. That variant takes a bit longer.

2: Part (a). The statement is true. Letting a be a generator of A, then aB is a generator of A/B and, in particular, A/B is cyclic. Let n be the order of A, and let m be the smallest positive integer such that $a^m \in B$. The greatest common divisor h of n and m has the form $h = xn + ym$ for some integers x and y. Therefore $a^h \in B$. The minimality of m now implies that $m = h$, in other words, m divides n. It is now easy to see that B is the cyclic subgroup generated by a^m.

Part (b). False. The case where $A = V_4$ and $1 < B < A$ is a counter-example.

Part (c). True. Since 127 is prime, the given assumtion implies that A has an element x with order 127. If the cyclic subgroup $X = \langle x \rangle$ is not contained in B, then $X \cap B = 1$ and the Second Isomorphism Theorem yields $X \cong XB/B \leq A/B$.

Part (d). True. One case being trivial, we may assume that A/B has a subgroup of order 127. Since 127 is prime, there exists an element $y \in A$ such that the element $yB \in A/B$ has order 127. The element $y \in A$ has order divisible by 127. So some power of y has order 127.

3: Part (a). We have $\theta(f)\theta(g) = (fH, fK)(gH, gK) = (fgH, fgK) = \theta(fg)$ for all $f, g \in G$.

Part (b). Since the kernel of θ is $H \cap K$, the First Isomorphism Theorem implies that $|\theta(G)| = |G|/|H \cap K|$, which is divisible by both $|G|/|H|$ and $|G|/|K|$. By the coprimality hypothesis, $|\theta(G)| = |G/H|.|G/K| = |G/H \times G/K|$.

Part (c). Supposing that θ is surjective then, applying the First Isomorphism Theorem as in part (b), we deduce that $|G : H \cap K| = |G : H||G : K|$. Therefore $|H \cap K| = |H||K|/|G|$.

4: Let $\mathcal{S}$ be the class of finite groups F for which there exist normal subgroups N_0, ..., N_r of G such that $1 = N_0 \trianglelefteq ... \trianglelefteq N_r = F$ and each N_i/N_{i-1} is abelian. It is not hard to see that $\mathcal{S}$ is closed under subgroups, quotient groups and direct products. We mean to say, given F and F' in $\mathcal{S}$, then every subgroup of F is in $\mathcal{S}$, every quotient group of F is in $\mathcal{S}$ and the direct product $F \times F'$ belong to $\mathcal{S}$. It follows that, given normal subgroups H and K of G such that G/H and G/K belong to $\mathcal{S}$, then every subgroup of $G/H \times G/K$ belongs to $\mathcal{S}$. Applying the First Isomorphism Theorem to the group homomorphism θ in Question 3, we deduce that $G/(H \cap K)$ belongs to $\mathcal{S}$. Therefore, G has a unique normal subgroup N that is minimal subject to G/N being in $\mathcal{S}$. In fact, given a normal subgroup N' of G, then G/N' is in $\mathcal{S}$ if and only if $N \leq N'$.

Let M be the unique normal subgroup of N that is minimal subject to N/M being in $\mathcal{S}$. Given $g \in G$, then ${}^gN = N$ and $N/{}^gM$ is in $\mathcal{S}$. By the uniqueness of M, we have ${}^gM = M$. in other words, $M \trianglelefteq G$. But G/M is in $\mathcal{S}$. By the definition of N, we have $M = N$. We have shown that N is perfect.

For any $L \trianglelefteq G$, the Second Isomorphism Theorem implies that $L/(L \cap N) \cong LN/N$. But LN/N belongs to $\mathcal{S}$. So, if L is perfect, then $L \cap N = L$, in other words, $L \leq N$. □

Comment: The groups in $\mathcal{S}$ are called the **solvable finite groups**. The name derives from the following. Any polynomial equation over $\mathbb{Q}$ is associated with a finite group, called the Galois group, which expresses the symmetries of the equation. The Galois group is solvable if and only if the solutions to the equation can be expressed in terms of $\mathbb{Q}$, addition, subtraction, multiplication, division, square roots, cube roots and higher such roots.

MATH 323: Algebra I. Midterm 1 Makeup.

LJB, 27 December 2016, 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.

Remember to justify your answers, except in any cases where your answers are obvious.

Notation: for a positive integer n, we let $\mathbb{Z}/n$ denote the integers modulo n. We let $(\mathbb{Z}/n)^\times$ denote those elements $[x]$ of $\mathbb{Z}/n$ such that x is coprime to n.

1:30 marks. You may assume that 1093 is prime. Let $A = (\mathbb{Z}/1093)^\times$.

(a) Find the inverse of 31 in A.

(b) Let $x_1 = 1$ and $x_{n+1} = 3x_n + 1$ for all positive integers n. Find n such that $1093 = x_n$. Hence find the order of 3 in A.

(c) Let k be a positive integer and p a prime such that $p = y_m$ for some m, where $y_1 = 1$ and $y_{n+1} = ky_n + 1$. Show that $k \in A$ and find the order of k in A.

2: 20 marks. Let p be a prime. As a set, let $H_p = \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p$. Let $*$ be the binary operation on H_p given by

$$(x_1, y_1, z_1) * (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2 + x_1 z_2, z_1 + z_2) \ .$$

(a) Show that H_p, equipped with the binary operation $*$, is a group.
(b) For which primes p does there exist a finite non-abelian group P such that $g^p = 1$ for all $g \in P$?

3: 30 marks. For finite groups $A \leq B \trianglerighteq C$ such that $AC = B$ and $A \cap C = 1$, we say that A **has a normal complement** in B, and we call C a **normal complement** of A in C. Let G be a finite group such that every subgroup of G has a normal complement in G.

(a) Show that, given subgroups $I \leq H \leq G$, then I has a normal complement in H.
(b) Show that G is abelian.
(c) Give an example of a finite abelian group E and a subgroup $F \leq E$ such that F does not have a normal complement in E.

4: 20 marks. A finite group H is said to be **supersolvable** provided there exists a chain of subgroups $1 = H_n \leq ... \leq H_1 \leq H_0 = H$ such that $H_i \trianglelefteq H$ and H_{i-1}/H_i is cyclic for all $1 \leq i \leq n$. Show that, for any finite group G, there exists a normal subgroup $K \trianglelefteq G$ with the property that, for any normal subgroup $J \trianglelefteq G$, the quotient group G/J is supersolvable if and only if $K \leq J$.

Midterm 1 Makeup Concise Solutions

1: We have $1093 = 35.31 + 8$ and $31 = 4.8 - 1$, yielding $1 = 4.1093 - 141.31$. So $31^{-1} = 962$. Part (b) has answer 7 as a special case of part (c), where $p = k^m + k^{m-1} ... + k + 1$ and answer is $m + 1$ because gives $p(k - 1) = k^{m+1} - 1$ while $k^m < p$.

2: Part (a) can be done routinely. For part (b), it is easy to show that, given a group G with $g^2 = 1$ for all $g \in G$, then G is abelian. On the other hand,

$$(x, y, z)^n = (nx, ny + n(n - 1)xz/2, nz)$$

in the non-abelian group H_p whence, if p is odd, then $(x, y, z)^p = (0, 0, 0)$. Therefore P as specified exists if and only if p is odd.

Comment: In pure mathematics, H_p is called the extraspecial group of order p^3 and exponent p. In applied, it is called the Heisenberg–Weil group of order p^3 and exponent p. One quick way of seeing part (a) immediately is via the matrix representation

$$(x, y, z) \leftrightarrow \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}.$$

3: Part (a). Let J be a normal complement of I in G. Let $K = J \cap H$. Plainly, $K \trianglelefteq H$ and $K \cap I = 1$. Any element of H can be written as ji with $j \in J$ and $i \in I$. But $j = (ji)i^{-1} \in H$, hence $j \in K$ and $H = KI$.

Part (b). We shall prove, by induction on $|G|$, that G is a product of cyclic groups of prime order. Let g be an element of prime order in G. Choose a normal complement $G_\bigstar$ of $\langle g \rangle$ in G. Choose a normal complement P of $G_\bigstar$ in G. By the Direct Product Recognition Theorem, $G \cong G_\bigstar \times P$. Therefore $P \cong G/G_\bigstar \cong \langle g \rangle$, which is cyclic of prime order. Applying the inductive hypothesis to $G_\bigstar$ yields the required conclusion.

Part (c). Take $E = C_{p^2}$ and let F be the unique proper subgroup of E.

4: It is not hard to show that, given finite supersolvable groups A and B, then $A \times B$ is supersolvable, moreover, every subgroup of A and every quotient group of A is supersolvable. By considering the canonical group homomorphism $G \to G/I \times G/J$, we see that, given $I \trianglelefteq G \trianglerighteq J$ with G/I and G/J supersolvable, then $G/(I \cap J)$ is supersolvable. Therefore, with respect to inclusion, there is a unique minimal $K \trianglelefteq G$ such that G/K is supersolvable.

MATH 323: Algebra I. Midterm 2. LJB, 9 December 2016, Bilkent University.

Time allowed: 105 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: 14 marks. Give an example of a group G and subgroups $H \leq G \geq K$ such that $|H| = |K|$ and H is not isomorphic to K. (Make sure it is clear why, in your example, H and K are not isomorphic to each other.)

2: 30 marks. Let G be the group with order 21 such that G has generators a and b satisfying $a^7 = b^3 = 1$ and $bab^{-1} = a^2$. Find the conjugacy classes of G. For each conjugacy class $[g]$, evaluate $|C_G(g)|$.

3: 32 marks. Let G be a finite group, let X be a transitive G-set, and let $x \in X$.
(a) Consider the stabilizer $G_x = \{g \in G : gx = x\}$. Show that G_x is a subgroup of G.
(b) State the Orbit-Stabilizer Equation relating $|G|$ and $|G_x|$.
(c) Show that, given $g, h \in G$, then $gx = hx$ if and only if we have an equality of left cosets $gG_x = hG_x$.
(d) Using part (c), prove the Orbit-Stabilizer Equation.

4: 24 marks. A **24-cell** is a 4-dimensional convex polytope, in other words, it is like a Platonic solid but it is realized in 4-dimensional Euclidian space $\mathbb{R}^4$. A point x in $\mathbb{R}^4$ has the form $x = (x_1, x_2, x_3, x_4)$ where $x_1, x_2, x_3, x_4 \in \mathbb{R}$. The distance between two points $x, y \in \mathbb{R}^4$ is

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2 + (x_4 - y_4)^2}\ .$$

A **rotation** in $\mathbb{R}^4$ is a distance-preserving function $g : \mathbb{R}^4 \to \mathbb{R}^4$ such that, in a physically intuitive sense, g can be effected by continuous movement. (More precisely but harder to understand: for each $t \in [0,1]$, there is a distance-preserving function g_t such that, for each $x \in \mathbb{R}^4$, the function $t \mapsto g_t(x)$ is continuous and $g_0(x) = x$ and $g_1(x) = g(x)$). The 24-cell has 24 vertices. The vertices can be expressed as coordinate vectors in two ways:

• we can take the vertices to be the 8 points $(\pm 1, 0, 0, 0)$, $(0, \pm 1, 0, 0)$, $(0, 0, \pm 1, 0)$, $(0, 0, 0, \pm 1)$ together with the 16 points $(\pm 1/2, \pm 1/2, \pm 1/2, \pm 1/2)$,
• alternatively, we can take the vertices to be the points z such that exactly two of z_1, z_2, z_3, z_4 belong to $\{\pm 1\}$ and the other two are 0. For instance, three of the 24 points are $(1, 1, 0, 0)$ and $(1, 0, -1, 0)$ and $(0, -1, 0, -1)$.

Let G be the group of rotational symmetries of the 24-cell. Let x be a vertex and ϵ an edge of the 24-cell.
(a) Evaluate $|G_x|$, hence evaluate $|G|$.
(b) Two vertices x and y have an edge between them if and only if x and y are distinct and the distance $d(x,y)$ is as small as possible. Without using part (a), determine the number of edges, evaluate $|G_\epsilon|$, hence check your evaluation of $|G|$.
(c) What is the isomorphism class of G_x?
(d) Let g be an element of G_x with order 3. What is the size of the conjugacy class $[g]_G$ of g in G?
(e) Show that there is a unique element $f \in G$ such that f has order 2 and $fg = gf$.
(f) What is the isomorphism class of G_ϵ? (Hint: part (e) might be useful.)

Midterm 2 Solutions

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

1: The smallest example is $(G, H, K) = (D_8, C_4, V_4)$. Of course, $C_4 \not\cong V_4$ by considering orders of group elements.

2: We shall show that the conjugacy classes of G are

$$\{1\} \ , \qquad \{a, a^2, a^4\} \ , \qquad \{a^3, a^5, a^6\} \ , \qquad \{a^i b : i \in \mathbb{Z}\} \ , \qquad \{a^i b^2 : i \in \mathbb{Z}\} \ .$$

Conjugating a by b and b^2, we see that $\{a, a^2, a^4\} \subseteq [a]$. On the other hand, $\langle a \rangle \leq C_G(a)$. But $|[a]||C_G(a)| = |G| = 21$. So $|[a]| = 3$ and $|C_G(a)| = 7$. We have shown that $[a] = \{a, a^2, a^4\}$. Similarly, $[a^{-1}] = \{a^{-1}, a^{-2}, a^{-4}\} = \{a^3, a^5, a^6\}$. Since $\langle b \rangle \leq C_G(b) < G$, Lagrange's Theorem gives $|C_G(b)| = 3$, hence $|[b]| = 7$. By considering the quotient group $G/\langle a \rangle \cong C_3$, we see that all the conjugates of b belong to the coset $\langle a \rangle b$. Therefore $[b] = \langle a \rangle b$ and similarly for b^2.

Comment: This question can also be done just as quickly by just calculating the conjugacy classes of a and b directly, without using any theorems, then appealing to similarity for the other elements of G. The above solution illustrates a technique involving the Orbit-Stabilizer Equation. The technique becomes more useful for larger given groups, at least as a check.

3: Part (a). Let $g, h \in G_x$. Then $ghx = gx = x$ and $g^{-1}x = g^{-1}gx = x$, hence $gh \in G \ni g^{-1}$.

Part (b). We have $|G| = |X|.|G_x|$.

Part (c). The condition $gx = hx$ can be expressed as $h^{-1}gx = x$, in other words, $h^{-1}g \in G_x$, which is equivalent to $gG_x = hG_x$.

Part (d). Given $g \in G$ and $y \in X$ then, by part (c), $gx = y$ if and only if every element of gG_x sends x to y. Since X is transitive, that condition describes a bijective correspondence $gG_x \leftrightarrow y$ between the left cosets $gG_x \subseteq G$ and the elements $y \in X$. Therefore, $|X|$ is the number of left cosets gG_x. The required equality follows, because all of those left cosets have size $|G_x|$.

Comment: If we, or the reader, were not aware that all the cosets gG_x have the same size, then we could argue as in the proof of Lagrange's Theorem, directly showing that, for each y, the number of group elements sending x to y coincides with the number of group elements sending x to x.

The above argument also shows that, putting $H = G_x$, then X is a copy of the G-set of left cosets $G/H = \{aH : a \in G\}$, with each group element $g \in G$ sending aH to gaH. Moreover, we can construct the G-set G/H for any subgroup $H \leq G$. Replacing X with G/H, the argument in part (d) and the previous paragraph becomes exactly the proof we gave for Lagrange's Theorem. Thus, in essence, the Orbit-Stabilizer Equation and Lagrange's Theorem are two different ways of expressing the same underlying content.

4: Parts (a) and (c). The 8 neighbouring vertices $(1, \pm 1, \pm 1, \pm 1)$ of $(1, 0, 0, 0)$ comprise a cube whose group of rotations can be identified with G_x. So $G_x \cong S_4$ and $|G_x| = 24$. Since there are 24 vertices, $|G| = 24|G_x| = 576$.

Part (b). Since each vertex has 8 edges, while each edge has 2 vertices, the number of edges is $4.24 = 96$. Without loss of generality, the edge ϵ has vertices $x = (1, 1, 0, 0)$ and

$y = (1,0,1,0)$. Regarding G_x as the rotation group of the cube C of nearest neighbours of x, also noting that y is a vertex of C, observe that the stabilizer of y in G_x is $G_x \cap G_y$. Dividing by the number of vertices of C, we have $|G_x \cap G_y| = |G_x|/8 = 3$. The vertices x and y are interchanged by the rotation that fixes $(0,1,1,0)$ and rotates C through half a revolution about the mid-point of ϵ. Therefore $|G_\epsilon| = 2|G_x \cap G_y| = 6$. We recover the equality $|G| = 96|G_\epsilon| = 576$.

Part (d). The group S_4 has exactly 8 elements of order 3, and they are mutually conjugate. The elements of G with order 3 fixing x and y also fix $(-1,-1,0,0)$, $(-1,0,-1,0)$, $(0,1,-1,0)$, $(0,-1,1,0)$ but cannot fix any other vertices because they cannot fix a 3-dimensional subspace. Therefore, each vertex of G is fixed by 8 conjugates of g, while each conjugate of g fixes 6 vertices. So the numbers 24.8 and $6|[g]_G|$ are both equal to the number of pairs (g', z) such that g' is a conjugate of g fixing vertex z. Therefore $|[g]_G| = 32$.

Part (e). A group element of order 2 is called an **involution**. Let f be the involution in G sending each vertex (t,u,v,w) to its opposite vertex $(-t,-u,-v,-w)$. Then $f \in Z(G)$ and, in particular, $fg = gf$. By part (d), $|C_G(g)| = |G|/32 = 18$. The group Z generated by f is a normal subgroup of $C_G(g)$, and $|C_G(g)/Z| = 9$, which is odd. By Lagrange's Theorem, $C_G(g)/\langle f \rangle$ has no involution. Therefore f is the unique involution on $C_G(g)$.

Part (f). By part (b), $G_\epsilon \cong C_6$ or $G_\epsilon \cong S_3$. We may assume that $g \in G_\epsilon$. Plainly, $f \notin G_\epsilon$. Hence, via part (e), no involution in G_ϵ commutes with g. Therefore, $G_\epsilon \cong S_3$.

Comment: In the question, the equivalence of the two coordinatizations of the vertices was merely stated. The two coordinatizations do describe the same polytope, indeed, there is a linear map from the first to the second such that

$$(1,0,0,0) \mapsto (1,1,0,0)/2 \; , \qquad (0,1,0,0) \mapsto (1,-1,0,0)/2 \; ,$$

$$(0,0,1,0) \mapsto (0,0,1,1)/2 \; , \qquad (0,0,0,1) \mapsto (0,0,1,-1)/2 \; .$$

Noting that vertices $(1,0,0,0)$, $(0,1,0,0)$, $(1,1,\pm1,\pm1)/2$ form an octahedron with centroid $(1,1,0,0)/2$, we see that the vertices of either one of two specified polytopes are, as vectors, double the centroids of the octahedral faces of the other specified polytome. So the 24-cell is self-dual.

MATH 323: Algebra I. Final. LJB, 6 January 2016, Bilkent University.

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.

Notation: Recall, when G is a group and H is a subgroup of G, we write $H \leq G$. When $H \leq G$ and $H \neq G$, we write $H < G$ and call H a **strict subgroup** of G.

1: 28 marks. A subgroup H of a group G is called a **maximal subgroup** provided $H < G$ and there does not exist a K such that $H < K < G$.
(a) Given an example of a finite group G such that $1 = Z(G) < G$.
(b) Let p be a prime and let P be a finite p-group such that $1 < P$. Show that $1 < Z(P)$.
(c) Give an example of a finite group G and a maximal subgroup $H < G$ such that the index $|G : H|$ is not prime.
(d) Let p and P be as in part (b). Show that every maximal subgroup of P has index p.

2: 42 marks. Recall, for a positive integer n, the shape of an element of S_n is a partition $n_1 + ... + n_r$ of n, the terms n_1, ..., n_r being positive integers such that $n_1 \geq n_2 \geq ... \geq n_r$ and $n_1 + n_2 + ... + n_r = n$.
(a) Find the shapes of all the elements of A_6.
(b) Show that, given an element $g \in A_6$ with shape $5 + 1$, then $C_{S_6}(g) \leq A_6$.
(c) Show that, given an element $g \in A_6$ with shape $3 + 3$, then $fg = gf$ for some element $f \in S_6$ with shape $2 + 2 + 2$.
(d) Show that, given an element $g \in A_6$ with shape neither $5 + 1$ nor $3 + 3$, then $fg = gf$ for some transposition f.
(e) How many conjugacy classes does A_6 have, and what are their sizes?
(f) Show that A_6 is simple. (You may use any method. You may assume that A_5 is simple.)

3: 14 marks. Let G be a simple group with order $|G| = 360$. Find the number of Sylow 5-subgroups of G.

4: 16 marks. In this question, we work through the steps of another proof of part of Sylow's Theorem. Following the steps, you are to prove that, given a prime divisor p of $|G|$, then G has a Sylow p-subgroup. That is, G has a p-subgroup S such that $|G : S|$ is coprime to p.
(a) Without using any results about the structure of finite abelian groups, show that, given a finite abelian group A and a prime divisor p of $|A|$, then A has an element with order p. (Hint: argue by induction on $|A|$.)
(b) Using part (a), prove the existence of a Sylow p-subgroup in the case where p divides $|Z(G)|$.
(c) Starting from the Orbit-Stabilizer Theorem, prove that

$$|G| = |Z(G)| + \sum_{g} |G : C_G(g)|$$

where g runs over representatives of those conjugacy classes of G that have at least 2 elements.
(d) Using part (c), prove the existence of a Sylow p-subgroup in the case where p does not divide $|Z(G)|$.

Solutions to Final exam

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

1: Part (a), $G = S_3$.

Part (b). By the Orbit-Stabilizer Equation, the order of each conjugacy class of P is a power of p. Perforce, every non-singleton conjugacy class is of order divisible by p. But the sum of the orders of the conjugacy classes is $|P|$, which is divisible by p. So $Z(P)$, being the union of the singleton conjugacy classes, has order divisible by p. Of course, $1 \in Z(P)$, hence $|Z(P)| \geq 1$. It follows that $|Z(P)| \geq p$.

Part (c). The smallest example is with $G \cong A_4$ and $H \cong C_3$. To see why H is maximal, observe that, if there were a subgroup K of order 6, then K would contain an involution and an element g with order 3, which is impossible because the conjugation action of g on the 3 involutions is transitive.

Part (d). Let Q be a maximal subgroup of P. We argue by induction on $|Q|$. The case $Q = 1$ is easy. Now assume that $1 < Q$ and that the required conclusion holds in all smaller cases. We have $Q \leq QZ(P) \leq P$. By the maximality, one of those inequalities is an equality. So $Z(P) \leq Q$ or $Q \lhd P$. Either way, in view of part (b), some non-trivial normal subgroup R of P is contained in Q. Replacing P and Q by P/R and Q/R, respectively, the required conclusion now follows from the inductive assumption.

2: Part (a). From the 11 partitions of 6, we remove those of odd parity, leaving

$$1+1+1+1+1+1\,, \qquad 2+2+1+1\,, \qquad 3+1+1+1\,, \qquad 3+3\,, \qquad 4+2\,, \qquad 5+1\,.$$

Part (b). An odd permutation of $\{1,2,3,4,5,6\}$ commuting with (12345) would fix 6 and would therefore belong to A_5, which is plainly impossible.

Part (c). The element $(123)(456)$, which has shape $3+3$, commutes with the element $(14)(25)(36)$, which has shape $2+2+2$.

Part (d). By inspection, all such g have an orbit $\{x,y\}$ in $\{1,2,3,4,5,6\}$ with size 2 or have 2 singleton orbits $\{x\}$ and $\{y\}$. Either way, the transposition (x,y) commutes with g.

Part (e). Recall, a conjugacy class of S_6 contained in A_6 either remains a single A_6-conjugacy class or else splits into 2 equally sized A_6-conjugacy classes. The former case holds if and only if an element of the class commutes with an odd permutation. So, via parts (b), (c), (d), the former case holds for the partitions 6.1 and $2.2+2.1$ and $3+3.1$ and 2.3 and $4+2$ but not for $5+1$. Therefore, A_6 has precisely $1+1+1+1+1+2 = 7$ conjugacy classes.

By straightforward enumerative methods, the S_6-conjugacy classes with shapes 6.1 and $2.2+2.1$ and $3+3.1$ and 2.3 and $4+2$ and $5+1$ have sizes 1 and 45 and 40 and 40 and 90 and 144, respectively. So the shapes and sizes of the 7 conjugacy classes of A_6 are as shown in the table.

shape of class	6.1	$2.2+2.1$	$3+3.1$	2.3	$4+2$	$5+1$	$5+1$
size of class	1	45	40	40	90	72	72

Part (f). Let K be a non-trivial normal subgroup of A_6. Then K is a union of conjugacy classes of A_6. Of course, $\{1\} \subset K$. So $|K| = 1 + k_1 + ... + k_t$ where $1 \leq t \leq 6$ and k_1, ..., k_t are taken from the numbers 40, 40, 45, 72, 72, 90 up to multiplicity. By Lagrange's Theorem, $|K|$ divides the order $|A_6| = 360 = 2^3.3^2.5$. None of the six candidate values of k_s are 1 less than a divisor of 360, so $t \geq 2$. It follows that $|K| \geq 1 + 40 + 40 = 81$ and $|A_6 : K| \leq 360/81 < 8$. Therefore $|K|$ is even and one of the k_s, without loss of generality k_1, must be $k_1 = 45$. If $t = 2$, then $|K| = 46 + m$ where $m \in \{40, 72, 90\}$. But of those possibilities contradict the condition that $|K|$ divides 360. Therefore $t \geq 3$ and $|K| \geq 1 + 45 + 40 + 40 = 126 > |A_6|/3$, in other words, either $|K| = |A_6|/2 = 180$ or else $K = A_6$. Since 45, 72, 90 are divisible by 9 and $|K|$ must also be divisble by 9, we can put $k_2 = k_3 = 40$. Hence $|K| = 126 + k_4 + ... + k_t$. But $k_4 \geq 72$, hence $|K| > 180$. We conclude that $K = A_6$, in other words, A_6 is simple.

Alternative argument for part (f): Consider a strict normal subgroup $K \lhd A_6$. We must show that $K = 1$. Understanding A_6 to act naturally on the set $I = \{1, ..., 6\}$, let B_i be the stabilizer of each $i \in I$. The groups B_1, ..., B_6 are all isomorphic to A_5 and they are all conjugate to each other. If $B_i \leq K$ for some i then, by the mutual conjugacy, $B_i \leq K$ for all i, which is impossible because the B_i together generate A_6 whereas $K < A_6$. We have shown strictness $K \cap B_i \lhd B_i$. But A_5 is simple, hence $K \cap B_i = 1$ for all i. Any non-trivial element g of K acts fixed-point-freely on I, we mean to say, $gi \neq i$ for all i. If such g exists then, by part (a), g must have shape $3+3$ or $4+2$. In the former case, since the elements of shape $3+3$ comprise a single A_6-conjugacy class, we have $(123)(456) \in K \ni (123)(654)$. Taking the product, we deduce that $(321) \in K$, which is impossible because (321) does not act fixed-point-freely. A similar argument yields a contradiction in the case where K owns an element with shape $4+2$. We conclude that no non-tivial element of K exists, in other words, $K = 1$, as required.

3: Let n be the number of Sylow 5-subgroups of G. We shall show that $n = 36$. When $G \cong A_6$, this is clear, because $36 = 144/4$, there are 144 elements with order 5, each element with order 5 belongs to a unique Sylow 5 subgroup, whereas each Sylow 5-subgroup owns exactly 4 elements with order 5.

Now let G be arbitrary. By Sylow's Theorem, $n \equiv 1$ modulo 5 and n divides $|G|/5 = 72 = 2^3 3^2$. Therefore $n \in \{1, 6, 36\}$. Since G is simple, $n \neq 1$. For a contradiction, assume that $n = 6$. Then, by considering the conjugation action of G on the Sylow 5-subgroups, we see that G can be identified with a subgroup of S_6. Also regarding A_6 as a subgroup of S_6 in the usual way, let $N = A_6 \cap G$. Since G is simple, either $N = 1$ or $N = G$. The former of those two cases is impossible because, thanks to the Second Isomorphism Theorem, G/N is isomorphic to a subgroup of $S_6/A_6 \cong C_2$. Yet the latter case is also impossible, because it implies that $G = A_6$, contradicting the assumption on n.

Comment: In fact, A_6 is the isomorphically unique simple group with order 360. But that is a deeper result and it may not be assumed.

4: This has been or will be included in my online IntroNotesGroupTheory.pdf file.