Archive for MATH 323, Algebra 1, Fall 2020

Bilkent University, Laurence Barker, 24 January 2021.

Source file: arch323fall20.tex

MATH 323, Algebra I, Fall 2020

Course specification

Laurence Barker, Bilkent University. Version: 21 December 2020.

Course Aims: To introduce some methods and techniques of algebra, focusing on group theory

Course Description: We shall mainly be concentrating on group theory, a subject area that lies at the foundation of modern algebra. We shall also be touching on some ring theory.

Course Requirements: The course takes place under exceptional conditions, which create adversity but which, to some extent, might also be used to advantage. It has always been the case that, to do well, students must be prepared to think for themselves. No teacher can simply inject skill and knowledge into a passive student who does only what is explicitly demanded. This semester, since much of your study is likely to be in seclusion, you may have the opportinuty to work without distraction (even a teacher is ultimately a distraction) and to fully take possession of the material you are required to learn.

A very good way of mastering the material is to do exercises. Learning, in mathematics, usually happens when you succeed with a problem that you could not immediately see how to do. So, if you give up as soon as you get stuck, then it will be impossible to learn very much.

You may sometimes find, when stuck on a difficult exercise, that there is something important you have not yet fully assimilated. You will not learn it just by reading or listening, following paths laid out by others. You will have to find you own way though the material. When you are unsure or confused about a basic notion, you must be willing to take the time to think it through until you have got it.

If you do not like a proof that you have read, then do not worry about how to imitate the person who wrote it. A better response is to compose, yourself, a proof that you find satisfactory. Then, in the short run, you might loose a few marks here and there but, in the long run, your independent judgement will make you a stronger mathematician.

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

Assistant, for homework grading: Demir Eken.
e-mail: demir dot eken at ug nokta bilkent dot edu nokta tr.

Course Texts: The primary course text is:

Thomas W. Judson, *Abstract Algebra*, 2020 edition.

To download a free copy of it, search for "Judson Abstract Algebra". The website is abstract.ups.edu, supported by University of Puget Sound.

A secondary text, also very thorough, is:

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

Course Documentation: On my homepage, see the files of **course notes** on selected topics, the file on **homeworks and solutions**.

Syllabus: The information on STARS is broadly correct. Note that, in view of exceptional health considerations this semester, some the information on STARS cannot be promptly updated to reflect modifications to course procedures associated with changes of university and national procedures.

A detailed syllabus is as follows. The format is *Week number: Monday date: Subtopics.*

1: 14 Sep: Review of equivalence relations, partial orderings, Euclidian algorithm, modular arithmetic.

2: 21 Sep: Abelian groups. Cyclic groups. Unit groups in modular arithmetic. Chinese Remainder Theorem.

3: 28 Sep: Abelian cases of Lagrange's Theorem, the Three Isomorphism Theorems, Sylow's Theorem.

4: 5 Oct: Abstract groups. Subgroups and cosets. Lagrange's Theorem.

5: 12 Oct: Conjugacy classes of elements and of subgroups. Centralizers and normalizers. The class formula.

6: 19 Oct: Quotient groups. The Three isomorphism Theorems.

7: 26 Oct: Direct Product Recognition Theorem. Symmetric groups.

8: 2 Nov: Cycle notation. Integer partitions and conjugacy.

9: 9 Nov: *Midterm Week.*

10: 16 Nov: Alternating groups and their conjugacy classes. Simplicity of the alternating groups of degree at least 5.

11: 23 Nov: Permutation groups. Orbit-Stablizer Equation. Symmetries of regular polyhedra.

12: 30 Nov: Finite p-groups. Cauchy's Theorem on existence of p-elements.

13: 7 Dec: Sylow's Theorem and applications.

14: 14 Dec: Finitely generated abelian groups.

15: 21 Dec: Zassenhaus' Butterfly Lemma. Jordan–Holder Theorem.

FZ Criterion: Very low homework and midterm marks, dependent on assignment difficulty.

Assessment:

- Homework, 30%,
- Midterm, 30%,
- Final, 40%.

75% attendance is compulsory. Attendance will be assessed through electronic records. Exceptions will be made only for students with documentary evidence of health excemptions or course clashes.

MATH 323, Algebra I, Fall 2020
Homeworks and Solutions

Laurence Barker, Bilkent University. Version: 17 December 2020.

Bear in mind that there are often many very good ways of responding to an exercise. The responses below are inevitably in my style, but you will develop a style of your own. What matters is whether or not your solutions are correct, succinct, and easily comprehensible to others in the class.

To be easily comprehensible, though, your style must conform to certain rules. Two important rules are as follows:

Rule 1: You should write in complete sentences, because otherwise the meaning will be ambiguous. "Prime p" has no meaning. "So p is prime" and "Let p be a prime" do have meanings, different meanings.

Rule 2: You should define all the symbols you introduce. "So p is prime" means nothing if the reader has not been told what p is.

Another tip, not crucial but good style, is always to begin a sentence with a word, not a mathematical expression. That facilitates smooth reading, because it makes it easier for the reader to see immediately where the beginnings of sentences are. Instead of "$x-2x+1=0$. $x=1$." you can write "We have $x^2-2x+1=0$. So $x=1$." Not only is that more readable, it is also more clear, because it avoids the misinterpretation "We have $x^2-2x+1=0$. Suppose $x=1$".

Homeworks

Homework 1

This homework is to be submitted to Moodle by Tuesday, 13 October, by 12:00 noon.

Recall, in a deductive mathematical argument, we arrive at a conclusion by a sequence of steps, each step being obvious. Of course, if something is already obvious, then there is no need to break it down into further steps. In fact, if an assertion is obvious, then proof of it is neither necessary nor even possible.

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

Exercise 1.A: Which of the following abelian groups are cyclic? (In all five cases, the answers are not obvious. So you will have to give a justifications.) $(\mathbb{Z}/9)^\times$, $(\mathbb{Z}/10)^\times$, $(\mathbb{Z}/20)^\times$, $(\mathbb{Z}/27)^\times$, $(\mathbb{Z}/1000)^\times$.

Recall, one definition of Euler's totient function $\phi : \mathbb{N} - \{0\} \leftarrow \mathbb{N} - \{0\}$ is by the formula $\phi(n) = |(\mathbb{Z}/n)^\times|$. You may use that definition in the next exercise. We mention that another formula is $\phi(n) = n \prod_p (1 - 1/p)$ where p runs over the prime divisors of n. Of course, that characterization, too, can be taken as the definition.

Exercise 1.B: Using Lagrange's Theorem, prove the following. (Proofs by other means will not be accepted.)
(1) Fermat's Little Theorem: Given a prime p and an integer x, then $x^p \equiv_p x$.
(2) Euler's Little Theorem: Given a positive integer n and an integer a coprime to n, then $a^{\phi(n)} \equiv_n 1$.

For an abelian group A, an isomorphism $A \leftarrow A$ is called an **automorphism** of A. We write $\mathrm{Aut}(A)$ for the set of automorphisms of A.

Exercise 1.C: Show that, given a positive integer n, then $(\mathrm{Aut}(\mathbb{Z}/n), \circ)$ is an abelian group, where $\circ$ indicates the usual composition of functions.

Exercise 1.D: What is the size of the set $\mathrm{Aut}((\mathbb{Z}/8)^\times)$?

Exercise 1.E: Show that $(\mathrm{Aut}((\mathbb{Z}/8)^\times, \circ)$ is not an abelian group.

Exercise 1.F: Let m and n be positive integers. Let $\theta : \mathbb{Z}/m \times \mathbb{Z}/n \leftarrow \mathbb{Z}/mn$ be the homomorphism given by the formula in the Chinese Remainder Theorem. (The same argument as before confirms that θ is indeed a homomorphism.) Evaluate $|\ker(\theta)|$ and $|\mathrm{im}(\theta)|$ in terms of m and n.

Exercise 1.G: Which of the following assertions are true for all positive integers m and n? (In each case, give a proof or a counter-example.)
(a) If $\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn$, then m and n are coprime.
(b) If m and n are coprime, then $(\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times \cong (\mathbb{Z}/mn)^\times$.
(c) If $(\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times \cong (\mathbb{Z}/mn)^\times$, then m and n are coprime.

Homework 2

This homework is to be submitted to Moodle by Wednesday 4 November, by 12:00 noon.

Exercise 2.A: Find all the subgroups of the infinite cyclic group C_∞. (You may assume the result in the notes asserting that every subgroup of a cyclic group is cyclic.)

Exercise 2.B: Let H be a subgroup of a group G. Show that H has only finitely many left cosets in G if and only if H has only finitely many right cosets in G. Also show that, when those equivalent conditions hold, the number of left cosets is equal to the number of right cosets.

Exercise 2.C: Let G be a finite group and $H \leq G$ such that $|G : H| = 2$. Show that $H \trianglelefteq G$.

Exercise 2.D: Recall, as an abuse of notation, the trivial subgroup $\{1_G\}$ of a group G is often written as 1.

Direct Product Recognition Theorem: *Let H and K be normal subgroups of a group G. Suppose that $H \cap K = 1$. Show that $HK \cong H \times K$.*

A more general theorem, concerning the scenario of the Second Isomorphism Theorem in the case where $H \cap K = 1$, will be discussed later.

Exercise 2.E: Prove:

Theorem: *Let $\theta : F \leftarrow G$ be a homomorphism. Then the condition $A = \theta(B)$ characterizes a bijectiive correspondence $A \leftrightarrow B$ between:*
(a) *The subgroups $A \leq \mathrm{im}(\theta)$,*
(b) *Those subgroups $B \leq G$ such that $\ker(\theta) \leq B$.*

Exercise 2.F: Let G be a finite group and A, B, C strict subgroups of G such that $G = A \cup B \cup C$. Show that A, B, C all have index 2.

Homework 3

This homework is to be submitted to Moodle by Thursday 10 December, by 12:00 noon.

Do the Practise Midterm below. I suggest you do it once as a closed-book two-hour exam, and then to do it again, consulting your notes when necessary and taking as much time as you like. Then submit just the second version to Moodle for marking.

MATH 323: Algebra I. Practice Midterm.

LJB, Fall 2020, Bilkent University.

Time allowed: two 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: 10 marks. For the dihedral group $D_{10} = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}$, find all the conjugacy classes.

2: 30 marks. Let p be an odd prime number.
(a) Let G be a group with order $2p$. Let a and b be elements of G with order 2. Show that ab does not have order 2.
(b) How many isomorphism classes of groups with order $2p$ are there? For each of the isomorphism classes, give an example of a group belonging to that isomorphism class.

3: 30 marks. For the symmetric group S_6:
(a) How many conjugacy classes are there?
(b) How many of those conjugacy classes $[g]_{S_6}$ does the element g have order 2?
(c) For each of the conjugacy classes $[g]_{S_6}$ where g has order 2, find the size $|[g]_{S_6}|$.

4: 30 marks. Let G be a group.
(a) Let E and F be normal subgroups of G such that G/E and G/F are abelian. Let $\theta : G \to G/E \times G/F$ be the group homomorphism such that $\theta(g) = (gE, gF)$ for each $g \in G$. By applying the First Isomorphism Theorem to θ, show that $G/(E \cap F)$ is abelian. (No marks will be awarded for proof by a different method.)
(b) Must there exist a normal subgroup $K \trianglelefteq G$ with the following property: given $L \trianglelefteq G$, then G/L is abelian if and only if $K \leq L$?

Solutions

Solutions 1

Solution 1.A: The abelian group $(\mathbb{Z}/9)^\times$ is cyclic. To see this, first note that

$$(\mathbb{Z}/9)^\times = \{[1], [2], [4], [5], [7], [8]\} .$$

The powers of [2] are, in order, [1], [2], [4], [8], [7], [5]. So [2] is a generator for $(\mathbb{Z}/9)^\times$.

Alternatively, $(\mathbb{Z}/9)^\times$ is an abelian group with order 6. Up to isomorphism, the only abelian group with order 6 is C_6, which is cyclic.

The abelian group $(\mathbb{Z}/10)^\times$ is cyclic. Indeed, $(\mathbb{Z}/10)^\times = \{[1], [3], [7], [9]\}$, which has generator [3].

The abelian group $(\mathbb{Z}/20)^\times$ is not cyclic, since the elements [9], [11], [19] all have order 2.

The abelian group $(\mathbb{Z}/27)^\times$ is cyclic. To prove this, first note that $|(\mathbb{Z}/27)^\times| = 18$. Modulo 27, we have $[2]^2 = [4]$, so $[2]^4 = [4]^2 = [16]$, so $[2]^8 = [16]^2 = [256] = [13]$. Hence, $[2]^9 = [26]$. Since $[2]^2 \neq [1]$ and $[2]^9 \neq [1]$, Lagrange's Theorem implies that [2] has order 18. We have shown that $(\mathbb{Z}/27)^\times$ is cyclic with generator [2].

The abelian group $(\mathbb{Z}/20)^\times$ is not cyclic, since [499], [501], [999] all have order 2.

Solution 1.B: Part (1). This is trivial when p divides x. When p does not divide x, Lagrange's Theorem implies that the order of the element $[x] \in (\mathbb{Z}/p)^\times$ divides the integer $|(\mathbb{Z}/p)^\times| = p = 1$. Hence, $[x]^{p-1} = [1]$.

Part (2). By Lagrange's Theorem, the order of $[a] \in (\mathbb{Z}/n)^\times$ divides the integer $|(\mathbb{Z}/n)^\times| = \phi(n)$, hence $[a]^{\phi(n)} = [1]$.

Solution 1.C: An element $[a] \in \mathbb{Z}/n$ is a generator if and only if $[a]$ has order n, in other words, $[a] \in (\mathbb{Z}/n)^\times$. Supposing that condition holds, then there is an automorphism θ_a of $\mathbb{Z}/n$ such that $\theta_a[x] = [ax]$ for all $x \in \mathbb{Z}/n$. Any $\theta \in \mathrm{Aut}(\mathbb{Z}/n)$ has that form, indeed, $\theta = \theta_a$ where $\theta[1] = [a]$.

Now let $\theta, \theta' \in \mathrm{Aut}(\mathbb{Z}/n)$. Let $a, b \in (\mathbb{Z}/n)^\times$ such that $\theta = \theta_a$ and $\theta' = \theta_b$. For all x, we have $\theta(\theta'[x]) = [abx] = [bax] = \theta'(\theta[x])$. So $\theta_\circ\theta' = \theta'_\circ\theta$.

Solution 1.D: We have $|(\mathbb{Z}/8)^\times| = \phi(8) = 8 - 4 = 4$.

Alternatively, $(\mathbb{Z}/8)^\times = \{[1], [3], [5], [7]\}$ which evidently has order 4.

Solution 1.E: The elements of $(\mathbb{Z}/8)^\times$ are the modulo 8 congruence classes [1], [3], [5], [7]. There are automorphisms θ and θ' given by the following table. The table also shows the values of $\theta_\circ\theta'$ and $\theta'_\circ\theta$.

	[1]	[3]	[5]	[7]
θ	[1]	[5]	[3]	[7]
θ'	[1]	[3]	[7]	[5]
$\theta_\circ\theta'$	[1]	[5]	[7]	[3]
$\theta'_\circ\theta$	[1]	[7]	[3]	[5]

Evidently, $\theta_\circ\theta' \neq \theta_\circ\theta'$.

Solution 1.F: Given $x \in \mathbb{Z}$, then the congruence class $[x]_{mn} \in \mathbb{Z}/mn$ belongs to the kernel of θ if and only if m and n both divide x, in other words, $\mathrm{lcm}(m, n)$ divides x. So

$$|\ker(\theta)| = mn/\mathrm{lcm}(m, n) = \gcd(m, n) .$$

It follows that $|\mathrm{im}(\theta)| = \dfrac{|\mathbb{Z}/mn|}{\gcd(m,n)} = \dfrac{mn}{\gcd(m,n)} = \mathrm{lcm}(m,n)$.

Solution 1.G: Condition (a) is false. The case $m = n = 2$ is a counter-example. Indeed, every element of $\mathbb{Z}/2 \times \mathbb{Z}/2$ has order 1 or 2, whereas $\mathbb{Z}/4$ has an element with order 4.

Condition (b) holds. Indeed, now assuming that m and n are coprime, then the version of the Chinese Remainder Theorem in the notes tells us, in particular, that there exists a bijection $\theta : \mathbb{Z}/m \times \mathbb{Z}/n \leftarrow \mathbb{Z}/mn$ given by $([x]_m, [x]_n) \leftarrow\!\shortmid [x]_{mn}$ for $x \in \mathbb{Z}$. Observe that x is coprime to mn if and only of x is coprime to both m and n. Therefore, θ restricts to a bijection $\phi : (ZZ/m)^\times \times (\mathbb{Z}/n)^\times \leftarrow (\mathbb{Z}/mn)^\times$. Given integers x and y coprime to mn, then

$$\phi([x]_{mn})\phi([y]_{mn}) = ([x]_m, [x]_n)([y]_m, [y]_n) = ([xy]_m, [xy]_n) = \phi([xy]_{mn}) = \phi([x]_{mn}[y]_{mn}) \ .$$

So ϕ is an isomorphism.

Condition (c) holds. To prove this, let m and n be positive integers such that $(\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times \cong (\mathbb{Z}/mn)$. Then $\phi(m)\phi(n) = \phi(mn)$. Let p run over those primes that divide m but not n. Let q run over those primes that divide n but not m. Let r run over those primes that divide both m and n. Define

$$P = \prod_p (1 - 1/p) \ , \qquad Q = \prod_q (1 - 1/q) \ , \qquad R = \prod_r (1 - 1/r) \ .$$

We understand a product to be 1 when the indexing set is empty. Now

$$mnPQR^2 = \phi(m)\phi(n) = \phi(mn) = mnPQR \ .$$

So $R = 1$. It follows that there are no primes satisfying the condition on r.

Solutions 2

Solution 2.A: Let g be a generator of C_∞. Since every subgroup of a cyclic group is cyclic, every subgroup of C_∞, every subgroup of C_∞ has the form $\langle g^m$ where $m \in \mathbb{Z}$. Given distinct integers m and n, then $\langle g^m \rangle = \langle g^n \rangle$ if and only if $m = -n$. So there is a bijective correspondence between the natural numbers m and the subgroups M of C_∞ such that $m \leftrightarrow M$ if and only if $\langle g^m \rangle = M$.

Solution 2.B: Given $f, g \in G$, then $fH = gH$ if and only if $Hf^{-1} = Hg^{-1}$. So there exists a well-defined bijective correspondence $gH \leftrightarrow Hg^{-1}$ between the left cosets of H in G and the right cosets of H in G. □

Solution 2.C: Given $g \in G - H$, then $gH = G - H = Hg$. So the left cosets of H in G coincide with the right cosets of H in G. □

Solution 2.D: The Direct Product Recognition Theorem now appears as Theorem 5.11 in the notes.

Solution 2.E: We first show that θ is injective. Let B and B' be subgroups of G such that $B \geq \ker(\theta) \leq B'$ and $\theta(B) = \theta(B')$. Then, for each $b \in B$, there exists $b' \in B$ satisfying $\theta(b) = \theta(b')$. So $b = b'k$ for some $k \in \ker(\theta)$. Then $k \in B'$, hence $b'k \in B'$. But b is an arbitrary element of B. Therefore, $B \leq B'$. A similar argument shows that $B \geq B'$. Thus, $B = B'$. The injectivity is established.

It remains only to show that θ is surjective. Let $A \leq \mathrm{im}(\theta)$. Define $B = \{b \in G : \theta(b) \in A$. For all $b, b' \in B$, we have $\theta(bb') = \theta(b)\theta(b') \in A$. and $\theta(b^{-1}) = \theta(b)^{-1} \in A$. So $B \leq G$. Plainly, $\theta(B) = A$. The surjectivity is now established, as required. $\square$

Solution 2.F: Write $|G| = n$. We may assume that $|B| \leq |A| \geq |C|$. We have

$$n \leq |A \cup B \cup C| + |A \cap B \cap C| \ .$$

But $|A \cap B \cap C| \geq 1$. So $|A| > n/3$. By Lagrange's Theorem, $|A| = n/2$. It follows that $A \lhd G$. If $B \leq A$, then $G = A \cap C$, hence $n = |A| + |C| - |A \cap C|$, which is impossible, because $|C| \leq n/2$ and $|A \cap C| \geq 1$. Therefore, $AB = G$. By the Second Isomorphism Theorem

$$B/(A \cap B) \cong AB/A = G/A \cong C_2 \ .$$

Hence $2|A \cap B| = |B| = |A \cap B| + |B - A|$. So $|B - A| = |A \cap B|$. Similarly, $|C - A| = |A \cap C|$. But $|B - A| + |C - A| \geq |G - A| = |A| = n/2$. By interchanging B and C if necessary, we may assume that $|B - A| \geq |C - A|$. Hence $|B - A| \geq n/4$. We deduce that $|B| \geq n/2$. By Lagrange's Theorem, $|B| = n/2$. So $|B - A| = n/4$. Therefore, $|C - A| \geq n/4$. Repeating an argument above, we deduce that $|C| = n/2$. $\square$

Solutions 3

These are the solutions to the Practice Midterm.

Solution 3.1: We shall show that the conjugacy classes are $\{1\}$ and $\{a, a^4\}$ and $\{a^2, a^3\}$ and $\{b, ab, a^2b, a^3b, a^4b\}$. The relations are $a^5 = b^2 = 1$ and $bab^{-1} = a^{-1}$. Bearing in mind that $b = b^{-1}$, we obtain $ba = a^{-1}b$ and $ab = ba^{-1}$. So $aba^{-1} = ba^{-2} = a^2b$ and, more generally, $a^nba^{-n} = a^{2n}b$. So $a^{3n}ba^{-3n} = a^nb$. So the conjugacy class of b is as specified.

We have $(a^nb)a(a^nb)^{-1} = a^2$. So the conjugacy class for a is as specified, and similarly for that of a^2.

Solution 3.2: Part (a). We may assume that $a \neq b$. For a contradiction, suppose that ab has order 2. Then $ab = ababba = ba$. So $\{1, a, b, ab\}$ is a subgroup of G isomorphic to V_4. That contradicts Lagrange's Theorem.

Part (b). Let G be a group with order 2. By part (a) together with Lagrange's Theorem, some non-identity element y of G must have order p or $2p$. Replacing y with y^2 if necessary, we may assume that y has order p. The cyclic group $\langle y \rangle$ has index 2, so $\langle y \rangle \lhd G$. Let $x \in G - \langle y \rangle$. Then $x^2 \in \langle y \rangle$. So x has order $2p$ or 2. If x has order $2p$, then $G = \langle x \rangle \cong C_{2p}$.

Now suppose x has order 2. Write $xyx^{-1} = y^r$. Then $y = x^2yx^{-2} = y^{r^2}$. So $r^2 \equiv 1$ modulo p, that is to say, $r \equiv \pm 1$. If $r \equiv 1$ then, again, $G \cong C_2 \times C_p \cong C_{2p}$, while if $r \equiv -1$, then $G \cong D_{2p}$.

In conclusion, there are exactly 2 isomorphism classes of groups with order $2p$, namely the cyclic group C_{2p} and the dihedral group $D - 2p$.

Solution 3.3: Part (a). The integer partitions of 6 are:

$$1+1+1+1+1+1\ , \quad 2+1+1+1+1\ , \quad 2+2+1+1\ , \quad 2+2+2\ ,$$

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

So S_6 has exactly 11 conjugacy classes.

Part (b). For the conjugacy classes of elements with order 2, the corresponding partition has first term 2. So there are exactly 3 such conjugacy classes.

Part (c). Let $\Omega = \{1, ..., 6\}$. The sizes are as follows. For $2 + 1 + 1 + 1 + 1$, we have

$$|[(1, 2)]_{S_6}| = 6.5/2 = 15 \ .$$

For $2 + 2 + 1 + 1$, we have

$$|[(1, 2)(3, 4)]_{S_6}| = 3(6.5/2) = 45$$

because, to choose g in that class, there are $6.5/2$ choices for the 2 elements of Ω fixed by g, then 3 choices for gw, where w is one of the other elements of Ω. For $2 + 2 + 2$, we have

$$|[(1, 2)(3, 4)(5, 6)]_{S_6}| = 5.3 = 15$$

because, for $w_1 \in \Omega$, there are 5 choices for gw_1 and then, for $w_2 \in \Omega - \{w_1, gw_1\}$, there are 3 choices for gw_2, whereupon g is determined.

Solution 3.4: Part (a). The subgroup $\mathrm{im}(\theta) \leq G/E \times G/F$ is abelian. By the First Isomorphism Theorem, $G/\ker(\theta) \cong \mathrm{im}(\theta)$. Since $\ker(\theta) = E \cap F$, the required conclusion follows.

Part (b). Yes. Let $\mathcal{K}$ be the set consisiting of the normal subgroups $N \trianglelefteq G$ such that G/N is abelian. Let $\phi : G \to \prod_N G/N$ such that the N-coordinate of $\phi(g)$ is gN. Arguing as in part (a), $G/\ker(\phi)$ is abelian. But $\ker(\phi) = K$. It is now clear that K has the specified property.

Alternative for part (b): Let K be the subgroup of G generated by the elements having the form $xyx^{-1}y^{-1}$ with $x, y \in G$. Given $L \trianglelefteq G$, then G/L is abelian if and only if $(xL)(yL)(xL)^{-1}(yL)^{-1} = L$ in G/L. That is equivalent to the condition that $K \trianglelefteq L$.

MATH 323: Algebra I. Midterm. LJB, 19 December 2020, Bilkent University.

Time allowed: 2 hours. Please write legibly and put your name on every sheet of your script.

1: 25 marks. Let F be a group with order 21 and elements a and b such that $a^7 = b^3 = 1$ and $bab^{-1} = a^2$.

(a) Find all the conjugacy classes of F.

(b) For each conjugacy class $[f]_F$, evaluate $|[f]_F|$ and $|C_F(f)|$. (The centralizer of f is $C_F(f) = \{x \in F : xf = fx\}$.)

2: 25 marks. In the symmetric group S_7:

(a) How many conjugacy classes of elements with order 3 are there?

(b) How many elements with order 3 are there?

(c) How many subgroups with order 3 are there?

(d) How many subgroups with order 9 are there?

3: 25 marks. Let U be a group and $V \leq U$.

(a) Show that $C_U(V) \trianglelefteq N_U(V)$. (The normalizer of V in U is $N_U(V) = \{u \in U : {}^uV = V\}$.)

(b) Show that $V/Z(V)$ is isomorphic to a subgroup of $N_U(V)/C_U(V)$. (The centre of V is $Z(V) = \{v \in V : \forall x \in V, vx = xv\}$.)

(c) Give an example where $V/Z(V)$ is not isomorphic to $N_U(V)/C_U(V)$.

4: 25 marks. Let G be a a group, and let $\mathcal{X}$ be the set of normal subgroups $H \trianglelefteq G$ such that the quotient group G/H is finite.

(a) Show that, given $H, I \in \mathcal{X}$, then $H \cap I \in \mathcal{X}$.

(b) Let L be the intersection of all the groups in $\mathcal{X}$. Show that $L \in \mathcal{X}$ if and only if $\mathcal{X}$ is finite.

(c) Give an example where the equivalent conditions in part (b) fail.

Solutions to MATH 323 Midterm, 19 December 2020.

Solution 1: Part (a). We shall show that the conjugacy classes are

$$\{1\}, \quad \{a, a^2, a^4\}, \quad \{a^3, a^5, a^6\}, \quad \{a^s b : s \in \mathbb{Z}/7\}, \quad \{a^s b^2 : s \in \mathbb{Z}/7\}.$$

Since $ba = a^2 b$, every element of F can be expressed in the form $a^s b^t$ for integers s and t. So the conjugates of a all have the form $b^t a b^{-t}$. Since $b^2 a b^{-2} = a^4$, we have $[a]_F = \{a, a^2, a^4\}$. Similarly, $[a^3]_F = \{a^3, a^5, a^6\}$.

We have $a^{-1}ba = a^{-1}a^2 b = ab$. So $a^{-s}ba^s = a^s b$. So the conjugates of b are the elements having the form $a^s b$. Also, $a^{-r}b^2 a^r = (a^{-r}ba^r)^2 = (a^r b)^2 = a^{3r}b^2$ for all $r \in \mathbb{Z}/7$. Letting r runs over all the elements of $\mathbb{Z}/7$, then $3r$ runs over all the elements of $\mathbb{Z}/7$, so the conjugates of b^2 are precisely the elements having the form $a^2 b^2$.

Part (b). Using the equality $|[f]_F|.|C_F(f)| = |F| = 21$, we obtain the following table for the sizes of the conjuacy classes and the orders of the centralizers.

f	1	a	a^3	b	b^2
$\lvert[f]_F\rvert$	1	3	3	7	7
$\lvert C_F(f)\rvert$	21	7	7	3	3

Comment: Alternatively, for the last part, we can find the orders of the centralizers as follows: since none of the non-identity elements is central in F, Lagrange's Theorem implies that $|C_F(f)| = |\langle f \rangle|$ for all $f \in F - \{1\}$.

Solution 2: Part (a). The conjugacy classes of elements with order 3 correspond to those integer partitions such that some term is 3 and every term is 3 or 1. Those partitions are $3+1+1+1+1$ and $3+3+1$. So there are exactly 2 of those conjuacy classes.

Part (b). The conjugacy class corresponding to the first of those partitions has size

$$|[(1,2,3)]_{S_7}| = 2\binom{7}{3} = \frac{2.7.6.5}{3.2} = 2.7.5 = 70$$

because, to choose g in that class, there are $7.6.5/3.2$ choices for the non-singleton orbit of g, then 2 choices for how the elements of that orbit are moved. The conjugacy class corresponding to the other partition has size

$$|[(1,2,3)(4,5,6)]_{S_7}| = 70.4 = 280$$

because there are 70 choices for a first 3-cycle, say $(1,2,3)$, then 4 choices for the other non-singleton orbit, say $\{4,5,6\}$, then 2 choices for the action on $\{4,5,6\}$, but we must divide by 2 because selection of the 2 non-singleton orbits in the other order would yield the same element of S_7.

So the total number of elements with order 3 is $70 + 280 = 350$.

Part (c). Each subgroup with order 3 owns exactly 2 elements with order 3. Conversely, each element with order 3 belongs to a unique subgroup with order 3. So the number of subgroups with order 3 is $350/2 = 175$.

Part (d). The subgroups with order 9 all have the form $\langle x, y \rangle$, where x and y are commuting 3-cycles. So each subgroup with order 9 owns exactly 4 elements with shape $3+3+1$. Conversely, every element of that shape belongs to a unique subgroup with order 9. So the number of subgroups with order 9 is $280/4 = 70$.

Comment 1: An alternative for part (d): Each subgroup with order 9 owns exactly 4 elements with shape $3+1+1+1+1$. On the other hand, each element with that shape belongs to exactly 4 subgroups with order 9. So the number of such subgroups is the number of such elements, which is 70.

Comment 2: Another alternative for part (d): Using the above form for a subgroup S with order 9, the normalizer $N(S)$ is generated by a subgroup isomorphic to $S_3 \times S_3$ and an element with shape 2+2+2+1 which interchanges the two non-singleton S-orbits. So $|N_G(S)| = 6.6.2 = 6.4.3$ and the number of subgroups with order 9 must be $7.6.5.4.3.2/6.4.3 = 7.5.2 = 70$.

Solution 3: Part (a). Let $h \in C_U(V)$ and $g \in N_U(V)$. We are to show that $ghg^{-1} \in C_U(V)$. Let $v \in V$. Since $g^{-1}vg \in V$, we have $hg^{-1}vgh^{-1} = g^{-1}vg$, hence

$$ghg^{-1}v(ghg^{-1})^{-1} = ghg^{-1}vgh^{-1}g^{-1} = gg^{-1}vgg^{-1} = v \ .$$

So $ghg^{-1} \in C_U(V)$, as required.

Part (b). Let $\theta : N_U(V)/C_U(V) \leftarrow V$ be the composite of the canonical homomorphism $N_U(V)/C_U(V) \leftarrow N_U(V)$ and the inclusion $N_U(V) \leftarrow V$. That is to say, $\theta(v) = vC_U(V)$ for $v \in V$. We have $\ker(\theta) = V \cap C_U(V) = Z(V)$. So, via the First Isomorphism Theorem, $V/Z(V)$ is isomorphic to the subgroup $\mathrm{im}(\theta) \leq N_U(V)/C_U(V)$.

Part (c). An example satisfying the specified condition is the case where $U \cong S_3$ and $V \cong C_3$. In that case, $V/Z(V)$ is trivial, while $N_U(V)/C_U(V) \cong C_2$.

Solution 4: Part (a). By the Second Isomorphism Theorem, $H/(H \cap I) \cong HI/I \leq G/I$, so $|H : H \cap I| < \infty$ and $|G : H \cap I| = |G : H|.|H : H \cap I| < \infty$.

Part (b). By part (a) and an inductive argument, the intersection of finitely many groups in $\mathcal{X}$ belongs to $\mathcal{X}$. So, if $\mathcal{X}$ is finite, then $L \in \mathcal{X}$.

Conversely, suppose $L \in \mathcal{X}$. Then there is a bijective correspondence $H \leftrightarrow H/L$ between the elements $H \in \mathcal{X}$ and the normal subgroups H/L of the finite group G/L. So $\mathcal{X}$ is finite.

Part (c). The conditions in (b) fail for the infinite cyclic group $(\mathbb{Z}, +)$.

MATH 323: Algebra I. Final. LJB, 3 January 2021, Bilkent University.

Time allowed: 2 hours. Please write legibly and put your name on every sheet of your script.

1: 5 marks. Give an example of two finite groups G and H such that $|G| = |H|$ and G is not isomorphic to H. (No proof is required. It is enough just to name the groups.)

2: 25 marks. (a) Find all the conjugacy classes of the alternating group A_4.

(b) Find all the normal subgroups of A_4.

3: 30 marks. (a) State Sylow's Theorem.

(b) Let G be a finite group with order $p^a m$ where p is prime, a is a natural number and m is a positive integer not divisible by p. Suppose that, for any two distinct Sylow p-subgroups S and T of G, we have $|S \cap T| = 1$. Show that the number of Sylow p-subgroups of G is congruent to 1 modulo p^a.

(c) Give an example to show that, when we remove the assumption that each $|S \cap T| = 1$, the conclusion in part (b) can fail.

4: 20 marks. Let G be a group with order 50.

(a) Show that G cannot be simple.

(b) Find, up to isomorphism, all the simple composition factors of G.

5: 20 marks. Let $\mathbb{N}_+$ denote the set of positive integers. For each $n \in \mathbb{N}^+$ and each element g of the alternating group A_n, we can regard g as an element of the symmetric group $\mathrm{Sym}(\mathbb{N}^+)$ by letting g fix all the integers greater than n. In this way, A_n can be regarded as a subgroup of $\mathrm{Sym}(\mathbb{N}^+)$. Consider the infinite union

$$A_\infty = \bigcup_{n=1}^{\infty} A_n \ .$$

(a) Show that A_∞ is a subgroup of $\mathrm{Sym}(\mathbb{N}^+)$.

(b) Show that the group A_∞ is simple.

Solutions to MATH 323 Final, 3 January 2020.

Solution 1: The smallest example is $G = C_4$ and $H = V_4$.

Solution 2: Part (a). The conjugacy classes of S_4 that are contained in A_4 are those with the partitions $1+1+1+1$ and $2+2$ and $3+1$ of 4. They have sizes 1 and 3 and 8, respectively. The elements with shape $2+2$ are not central, so they comprise a single conjugacy class of A_4. Since 8 does not divide 12, the elements of A_4 with shape $3+1$ comprise 2 conjugacy classes of A_4, both of them with size 4. Conjugating by the elements of shape $2+2$, we see that $(1,2,3)$ has A_4-conjugates $(1,4,2)$ and $(1,3,4)$ and $(2,4,3)$. So the conjugacy classes are

$$\{1\},\ \{(1,2)(3,4)\},\ \{(1,2,3),(1,4,2),(1,3,4),(2,4,3)\},\ \{(1,3,2),(1,2,4),(1,4,3),(2,3,4)\}.$$

Part (b). Every normal subgroup is a union of conjugacy classes. So, in view of Lagrange's Theorem, the normal subgroups of A_4 are 1 and A_4 and the subgroup

$$\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \cong V_4\ .$$

Comment: Alternatively, in part (a), to avoid calculating the conjugates of a 3-cycle, we can observe that, since each conjugacy class with shape $3+1$ must intersect with every Sylow 3-subgroup, no element of that shape can be conjugate to its inverse. It follows that the conjugacy classes are $[1]_{A_4}$, $[(1,2)(3,4)]_{A_4}$, $[(1,2,3)]_{A_4}$, $[(1,3,2)]_{A_4}$.

Solution 3: Part (a). Sylow's Theorem: Let G be a finite group with order $p^a m$ as in part (b). Then the Sylow p-subgroups are mutually G-conjugate, and the number of them divides m and is congruent to 1 modulo p.

Part (b). Fix a Sylow p-subgroup S of G. Let Ω be the set consisting of all the other Sylow p-subgroups of G. We may assume that $\Omega \neq \emptyset$, because otherwise the required conclusion is trivial. Let S act on Ω by conjugation. Given $T \in \Omega$, then the stabilizer of T in S is $R = S \cap N_G(T)$. By the Second Isomorphism Theorem, $|RT|/|T| = |R|/|R \cap T|$. So $|RT|$ is a power of p. By Lagrange's Theorem, $|RT| = |T|$. On the other hand, $R \cap T \leq S \cap T$, so $|R \cap T| = 1$. Therefore $|R| = 1$. We have shown that every S-orbit of Ω has size $|S| = p^a$.

Part (c). Put $G = S_3 \times C_2$. Then the number of Sylow 2-subgroups is 3, which is not congruent to 1 modulo $p^a = 4$.

Comment: The argument in part (b) is a straightforward adaptation of part of the standard proof that the Sylow p-subgroups are mutually conjugate.

Solution 4: Part (a). By Sylow's Theorem, the number n of Sylow 5-subgroups of G divides 2 and is congruent to 1 modulo 5. So $n = 1$, and G has a unique Sylow 5-subgroup that is normal in G. Perforce, G is not simple.

Part (b). Let Q be a proper normal subgroup of the normal Sylow 5-subgroup P of G. Then $1 \lhd Q \lhd P \lhd G$ is a composition series. We have $Q/1 \cong P/Q \cong C_5$ and $G/P \cong C_2$. So the simple composition factors of G are C_5 and C_2 (with multiplicities 2 and 1, respectively).

Solution 5: Part (a). Given $a, b \in A_\infty$, then there exists n such that $a, b \in A_n$. Then $a^{-1}, ab \in A_n$, hence $a^{-1}, ab \in A_\infty$. So $A_\infty \leq \mathrm{Sym}(\mathbb{N}^+)$.

Part (b). For a contradiction, suppose there exists a proper normal subgroup H of A_∞. Then there must exist n such that $1 < H \cap A_n < A_n$. Since $1 < H \cap A_m < A_m$ for all $m \geq n$, we may assume that $n \geq 5$. The normality of H implies that $1 \lhd H \lhd A_n$. This contradicts the simplicity of A_n.