My abstract algebra exercises

Evgeny Markin

2023

Contents

Part I

Preliminaries

Chapter 1

Relations and Functions

Chapter 2

The Integers and Modular Arithmetic

Part II

Groups

Chapter 3

Introduction to Groups

3.1 An Important Example

3.1.1

In S_4, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. Calculate $\sigma\tau$, $\tau\sigma$ and σ^{-1}.

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

$$\tau\sigma = \begin{pmatrix} l1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

3.1.2

In S_5, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$ calculate $\sigma\tau\sigma$, $\sigma\sigma\tau$, σ^{-1}.

$$\sigma\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

$$\sigma\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$$

3.1.3

How mamy permutations are there in S_n? In S_5, how many permutations α satisfy $\alpha(2) = 2$?

We can follow that there are $n!$ permutations total, and if we've got a restriction $\alpha(2) = 2$, then we've got $(n-1)!$ permutation. For the case S_5 it means that there are $4! = 24$ such permutations.

3.1.4

Let H be the set of all permutations $\alpha \in S_5$ satisfying $\alpha(2) = 2$. Which of the properties of closure, associativity, identit, inverses does H enjoy under composition?

All of them

3.1.5

Consider the set of all functions from 6 to 6. Which of the ...

Everything other then inverse

3.1.6

Let G be the set of all ...

All of them

3.2 Groups

3.2.1

Give group tables for following additive grops: Z_3, $Z_3 \times Z_2$

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

last one is ommited

3.2.2

Give group tables for the following groups: $U(12), S_3$

We follow that $U(12) = \{1, 5, 7, 11\}$. THus

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

One of the programs in progs folder produces desired table for S_3 (and can produce one for any S_n for that matter).

3.2.3

Show that $G \times H$ is abelian iff G and H are both abelian

Was proven in dummit and foote, check 1.1.29

Rest of the exercises in this section were either already proven in D&F, are trivial, or could be solved at a later time if I encounter some gaps in the theory.

3.3

3.4

3.5

3.6 Cyclic Groups

3.6.1

Let $G = \langle a \rangle$ be a cyclic group of order 12. List every subgroup of G. List every group of Z_{12}

12's divisors are $\{1, 2, 3, 4, 6, 12\}$, therefore subgroups of G are $\langle a^i \rangle$ for $i \in \{0, 1, 2, 3, 4, 6\}$

Since Z_{12} is cyclic, we follow that $\langle [0, 1, 2, 3, 4, 6] \rangle$ are the subgroups of Z_{12}.

3.6.2

Let $G = \langle a \rangle$ be a cyclic group of order 120. List all of the groups of order 120. List all of the elements of order 12 in G.

Divisors of 120 are $\{1, 2, 3, 4, 5, 6, 8, 10, 12, 24, 60, 120\}$, thus we can state that subgroups of a cyclic group are a to powers of those numbers

According to the theorems, there should be $\phi(12) = 4$ elements of order 12. All of them lie in a subgroup $\langle a^{120/12} \rangle = \langle a^{10} \rangle$ and are in form $(a^{10})^k$ where $k \in 1, 5, 7, 11$.

How many element of order 12 are there in a cyclic group of order 1200?

Also 4.

3.6.3

Let p be a prime and n a positive integer. Show that $\phi(p^n) = p^n - p^{n-1}$

If $j \in Z_+$ is such that $j = pi$ for some $i \in Z_+$, then we follow that $(p^n, j) = p$, therefore they are not relatively prime. Suppose that $(p^n, j) = 1$ for some $j \in Z_+$. Let S be a multiset of prime divisors of $p^n N$ and T be a multiset of divisors of j. Then we follow that $S \cap T = \emptyset$, since otherwise we would've had that j is a multiple of p, which is not relatively prime to p^n. Thus we follow that the set of not relatively prime numbers to p^n is equal to the set of multiples of p.

We can follow that there are pricicely p^{n-1} of multiples of p that are less or equal to p^n (don't think that we need to prove that), therefore the total amount of numbers that are less or equal to p^n, which are relatively prime to p^n is $p^n - p^{n-1}$, as desired.

3.6.4

Find all positive integers n such that $|U(n)| = 24$.

We can follow that $\phi(n)$ is an function that tends to infinity (i.e. for every $n \in Z_+$ there exists $j \in Z_+$ such that $m > n$ implies that $\phi(m) > j$) since $\phi(n)$ is larger than the number of prime numbers that is in the set $Z_+ \cap [1, n)$. Therefore we conclude that there is an upper bound for a number of numbers n such that $\phi(n) = 24$.

Brute-force shows that those numbers are

$$35, 39, 45, 52, 56, 70, 72, 78, 84, 90$$

Can't come up with a better answer than that, but I'm sure that it's there.

3.6.5

Let G be a nonabelian group. If H and K are cyclic subgroups of G, does it follow that $H \cap K$ is also a cyclyc subgroup? Prove that it does, or provide a counterexample.

We follow that every subgroup has an identity in it, thus $e \in H \cap K$. Suppose that $j \in H \cap K$. We follow that $j \in H \wedge j \in K$. Since H and K are both subgroups, we follow that $j^{-1} \in H \wedge j^{-1} \in K$. Thus $j^{-1} \in H \cap K$. Therefore $H \cap K$ is closed under inverses. We can follow also by the same logic that $j, l \in H \cap K$ implies that $jl \in H \cap K$. Therefore we can conclude that $H \cap K$ is a subgroup.

We can follow that if $H \cap K = \{e\}$, then it's cyclic. We can follow that $H \cap K$ can be not only a trivial subgroup by setting $H = K$. Suppose that $H \cap K \neq \{e\}$. By the fact that both H and K are cyclic we follow that $H \cap K = \{a^i : i \in \text{ some subset of } Z_+\}$. Since $H \cap K \neq \{e\}$, we follow that there exists an element $a \in G$ and two sets $H', K' \in \mathcal{P}(Z_+)$ such that $H = \{a^i : i \in H'\}$ and $K = \{a^i : i \in K'\}$. Since both H and K are cyclic we follow that both H' and K' are the sets of multiples of some number. Thus $H' \cap K'$ is a set of multiples of some number as well (proof ommited). Thus we follow that $H \cap K = \{a^i : i \in H' \cap K'\}$ is a cyclic group as well.

3.6.6

Let $G = \langle a \rangle$ be an infinite cyclic. If m and n are positive integers, find a generator for $\langle a^m \rangle \cap \langle a^n \rangle$.

We can follow pretty easily that $\langle a^m \rangle \cap \langle a^n \rangle = \langle a^{lcm(m,n)} \rangle$

3.6.7

Let n be a positive integer and let T be the set of positive integers that divide n. Show that $\sum_{k \in T} \phi(k) = n$.

For 12 we've got

$$T = \{1, 2, 3, 4, 6, 12\}$$
$$\phi(1) = 1$$
$$\phi(2) = 1$$
$$\phi(3) = 2$$
$$\phi(4) = 2$$
$$\phi(6) = 2$$
$$\phi(12) = 4$$

and we follow that result works.

3.7 Cosets and Lagrange's Theorem

3.7.1

For each group G and subgroup H, find all the left cosets and right cosets of H in G.

1. $G = Z, H = 4Z$.

We follow thaht $0 + H = 4Z = H$, $1 + H = \{1 + x : x \in Z\}$, and so on for $3 + H$. Since the group is abelian, we follow that right cosets are the same.

3.7.2

Let G be a group whose order is the product of two (not necessarily distinct) primes. Show that every proper subgroup of G is cyclic

We follow that order of any given proper subgroup is equal to one of those primes, or 1. This implies that this subgroup is cyclic, as desired.

3.7.3

Let G be a group of order p^n for some prime p and positive integer n. Show that G has an element of order p.

We follow that any proper subgroup is some power of p. By induction we can conclude that such an element exists.

3.7.4

Let G be a group having a subgroup H of order 28 and a subgroup K of order 65. Show that $H \cap K = \{e\}$.

We follow that

$$28 = 2 * 2 * 7$$

$$65 = 13 * 5$$

since they don't have no commot prime multiples, we follow that $H \cap K$'s only order as a subgroup of both can be only 1. Since every group has an identity, we conclude the desired result.

3.7.5

blah blah blah

$$lcm(1, 2, ..., 10)$$

Chapter 4

Factor Groups and Homomorphisms

4.1 Normal Subgroups

4.1.1

Is each of the following sets a normal subgroup of $GL_2(R)$?

1. $H = \{A \in GL_2(R) : \det(A) \in Q\}$

We can follow that this thing is a subgroup by the properties of determinants of compositions of matrices and the fact that $Q \setminus \{0\}$ is closed under multiplication.

We follow that for all $a \in GL_2(R)$ and $h \in H$ we've got that

$$\det(a^{-1} * h * a) = \det(a^{-1}) * \det(h) * \det(a) = \det(a^{-1}) * \det(a) * \det(h) = \det(I) * \det(h) = \det(h)$$

and thus we follow that sH is a normal subgroup by one of the equivalencees in of the normal group.

2. the set of diagonal matrices in $GL_2(R)$.

We can follow that the thing is a subgroup my matrix identities and whatnot (identity is diagonal, inverse of diagonal is diagonal and composition of diagonal is diagonal; for justification GOTO linear algebra course, chapter 6 or 7) We can't follow that it's a normal group though, since we can set

$$a = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

which gives us that $a^{-1} ha$ is not in H (details are ommited put can be supplimented easily if you feel that you don't have nothing to do).

4.1.2

Find every normal subgroup of S_3.

We follow that S_3 is itself a normal subgroup. Every sugroup of index 2 is normal, thus we follow that in this case that means that every subgroup of size 3 is normal. Every subgroup of length 1 must contain the identity, and thus we follow that the only subgroup of size 1 is the one that contains identity. Therefore by Lagrange's theorem we follow that the only subgroups left are the ones that have size 2. Let U be a subgroup of length 2. We follow that it must contain the identity, and thus they have the form

$$U = \{e, s\}$$

where $s \in S_3 \setminus \{e\}$. There are 5 such elements, and thus we can check them by hand.

Since U has to be a subgroup, we follow that $s \in S_3$ must be such that $s = s^{-1}$. Thus our search is limited to cycles

$$(2,3), (1,2), (1,3)$$

We follow that

$$(1,2)^{-1} \circ (2,3) \circ (1,2) = (1,2) \circ (2,3) \circ (1,2) = (1,3)$$

$$(2,3)^{-1} \circ (1,2) \circ (2,3) = (2,3) \circ (1,2) \circ (2,3) = (1,3)$$

$$(2,3)^{-1} \circ (1,3) \circ (2,3) = (2,3) \circ (1,3) \circ (2,3) = (1,2)$$

thus we follow that none of those are normal. Therefore we conclude that the only normal subgroups of S_3 are the ones with size $6, 3$ and 1.

4.1.3

If N is a normal subgroup of G, and $|N| = 2$, show that $N \leq Z(G)$

We follow that

$$(\forall a \in G)(\forall h \in H)(a^{-1} ha \in H)$$

since $|H| = 2$, we follow that $H = \{e, b\}$ for some $a \in G \setminus \{e\}$. Let $x \in H$. If $x = e$, then we follow that $x \in Z(G)$. If $x = b$, then we follow that

$$a^{-1} ba \in H \Leftrightarrow a^{-1} ba = e \vee a^{-1} ba = b \Leftrightarrow ba = ae \vee ba = ab$$

Since $b \neq e$, we follow that $ba \neq a = ae$, thus we follow that for all $a \in G$ we've got that $ba = ab$. Thus we follow that $x \in Z(G)$. Therefore we follow that $H \subseteq Z(G)$, and thus $H \leq Z(G)$, since the operation is the same, as desired.

4.1.4

Let N be a normal subgroup of G. Let H be the set of all elements h of G such that $hn = nh$ for all $n \in N$. Show that H is a normal subgroup of G.

Proof that H is a subgroup is trivial and therefore ommited.

Let $a \in G$. We follow that for all $n \in N$, $a^{-1}na \in N$. Since N is normal in G, we follow that $N = a^{-1}Na$. Thus for given $a \in G$ and $n \in N$ there exists $n' \in N$ such that $n = a^{-1}n'a$. Thus $an = n'a$.

We want to show that if $h \in H$, then $a^{-1}ha \in H$. We follow that $a^{-1}ha \in H$ if and only if for all $n \in N$ we've got that

$$n(a^{-1}ha) = (a^{-1}ha)n$$
$$(a^{-1}ha) = n^{-1}(a^{-1}ha)n$$
$$(a^{-1}ha) = (an)^{-1}h(an)$$
$$(a^{-1}ha) = (n'a)^{-1}h(n'a)$$
$$(a^{-1}ha) = a^{-1}n'^{-1}hn'a$$
$$(a^{-1}ha) = a^{-1}n'^{-1}n'ha$$
$$(a^{-1}ha) = a^{-1}eha$$
$$a^{-1}ha = a^{-1}ha$$

as desired.

4.1.5

Show that the intersection of two normal subgroups of G is also a normal subgroup. Then extend this to show that if N_i is a normal subgroup of G for every i in some set T, then $\bigcap_{i\in T} N_i$ is a normal subgroup of G.

I think that I've shown earlier (maybe in another document) that $\bigcap_{i\in T} N_i$ is a subgroup. If not, then showing that is pretty trivial.

We firsly state here explicitly that T is nonempty, otherwise $\bigcap$ is not defined. Let $x \in \bigcap_{i\in T} N_i$. This means that

$$(\forall i \in T)(x \in N_i)$$

Since N_i is normal for every $i \in T$, we follow that for all $a \in G$ we've got that $a^{-1}xa \in N_i$. Thus

$$(\forall a \in G)(\forall i \in T)(a^{-1}xa \in N_i)$$

which is equivalent to

$$(\forall a \in G)(a^{-1}xa \in \bigcap_{i\in T} N_i)$$

thus we conclude that if $x \in \bigcap_{i\in T} N_i$, then $a^{-1}xa \in \bigcap_{i\in T} N_i$. Therefore for all $x \in \bigcap_{i\in T} N_i$ and all $a \in G$ we've got that $a^{-1}xa \in \bigcap_{i\in T} N_i$. Therefore $\bigcap_{i\in T} N_i$ is normal.

4.1.6

Let $N_1 \leq N_2 \leq N_3 \leq \ldots$ be normal subgroups of G. Show that $\bigcup_{i=1}^{\infty} N_i$ is a normal subgroup of G.

This exexrcise is pretty much the same as the previous one, except that we might have to use a different quantifier.

4.1.7

Let G be a group having exactly one subgroup H of order n. Show that H is normal in G.

Suppose that H is not normal. Then we follow that $a^{-1}Ha \neq H$. Since $a^{-1}Ha$ is a subgorup with $|a^{-1}Ha| = |H| = n$. Thus we follow that there are at least two disctinct groups of order n, which is a contradiction.

4.1.8

Let $G = H \times K$. If N and L are normal subgroups of H and K respectively, show that $N \times L$ is a normal subgroup of G. Is every normal subgroup of G of this form?

Let $a \in G$ be arbitrary. We follow that $a = \langle h', k' \rangle$ for some $h' \in H, k' \in K$. We follow that $a^{-1} = \langle h'^{-1}, k'^{-1} \rangle$. Let $\langle n, l \rangle \in N \times L$ be also arbitrary. We follow that $h'^{-1}nh' \in N$ and $k'^{-1}lk' \in L$, and thus $\langle h'^{-1}nh', k'^{-1}lk' \rangle \in N \times L$. Therefore we follow that $N \times L$ is normal, as desired.

Rule of the thumb is that if someone asks you an open question in a math book, then the answer is no, therefore we want to find a contradiction. Let $H = K = Z_2$. Let $U = \{\langle 1, 1 \rangle, \langle 0, 0 \rangle\}$. We followw that since $|U| = 2$, index of U is 2, and thus it is normal.

4.1.9

Suppose that H is a subgroup of G and $a^{-1}b^{-1}ab \in H$ for all $a, b \in G$. Show that H is normal.

Let $c \in G$ and $h \in H$ be arbitrary. We follow that $h, h^{-1} \in G$ by the fact that H is a subgroup. Thus

$$c^{-1}(h^{-1})^{-1}c(h^{-1}) \in H$$

by property of H. Thus

$$c^{-1}hc(h^{-1}) \in H$$

Since $h \in H$, we follow that

$$c^{-1}hc(h^{-1})h \in H$$

thus

$$c^{-1}hc \in H$$

thus H is normal, as desired.

4.1.10

Let H and K be subgroups of G. Show that HK is a subgroup if and only if $HK = KH$.

Assume that HK is a subgroup. We follow that since $e \in K$ that $he = h \in HK$ for all $h \in H$. Thus $H \leq HK$. We also follow by the same logic that $K \leq HK$. Let $j \in KH$. We follow that $j = k'h'$ for some $h' \in H$ and $k' \in K$. Since $H \leq HK$ and $K \leq HK$, we follow that $k' \in HK$ and $h' \in HK$, thus $k'h' \in HK$. Thus $KH \subseteq HK$.

Let $hk \in HK$. We follow that $(hk)^{-1} \in HK$. Thus there exist $h' \in H$ and $k' \in K$ such that $h'k' = (hk)^{-1}$. Thus $hk = (h'k')^{-1} = k'^{-1}h'^{-1}$. Since $k' \in K$ and $h' \in H$, we follow that $k'^{-1} \in K$ and $h'^{-1} \in H$, and thus $k'^{-1}h'^{-1} \in KH$. Thus $hk = k'^{-1}h'^{-1} \in KH$. Therefore $HK \subseteq KH$, as desired.

Suppose that $HK = KH$. Since $e \in H$ and $e \in K$ we follow that $e \in HK$. Let $hk \in HK$. We follow that $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Thus $(hk)^{-1} \in HK$. Let $a, b \in HK$. We follow that $a = hk$ and $b = h'k'$ for somce $h, h' \in H$ and $k, k' \in K$. Thus

$$ab = hkh'k' = h(kh')k'$$

since $h \in HK$, $k \in HK$ and $kh' \in KH = HK$, we conclude that $ab \in HK$. Thus HK is a subgroup.