

My abstract algebra exercises

Evgeny (Gene) Markin

2024

Contents

1	A Potpourri of Preliminary Topics	4
2	Groups - Part 1	5
2.1	Introduction to Groups	5
2.1.1	5
2.1.2	5
2.1.3	5
2.1.4	6
2.2	Abstract Groups	6
2.2.1	6
2.2.2	7
2.2.3	9
2.2.4	9
2.2.5	11
2.3	Interesting Examples of Groups	11
2.3.1	12
2.3.2	13
2.3.3	13
2.3.4	13
2.3.5	13
2.3.6	14
2.3.7	14
2.3.8	15
2.3.9	16
2.3.10	16
2.3.11	17
2.4	Group Homomorphism	17
2.4.1	17
2.4.2	18
2.4.3	18

2.4.4	18
2.4.5	19
2.4.6	20
2.5 Subgroups, Cosets, and Lagrange's Theorem	20
2.5.1	20
2.5.2	21
2.5.3	22
2.5.4	22
2.5.5	23
2.5.6	24
2.5.7	25
2.5.8	25
2.5.9	26
2.5.10	26
2.5.11	28
2.5.12	29
2.5.13	30
2.5.14	30
2.5.15	32
2.6 Products of groups	32
2.6.1	32
2.6.2	33
3 Rings - Part 1	34
3.1 Abstract Rings and Ring Homomorphisms	34
3.1.1	34
3.1.2	35
3.2 Interesting Examples of Rings	37
3.2.1	37
3.2.2	37
3.2.3	39
3.2.4	40

Preface

This is another yet another attempt at making any progress with abstract algebra, this time with 'Abstract Algebra: An Integrated Approach' by Joseph H. Silverman. I really hope that it works out this time.

So far, it's been most pleasurable journey. This book embodies all the things, that I like in the mathematics books: lots of rigor and a bit of lightheartedness, that really lights it up.

After some time with this book my opinion changed a bit in a worse direction due to an increasing number of typos that I have to deal with. \subseteq and \subset are often mixed up, I've encountered an exercise (2.30(c)), whose whole text is one big typo, and some others. On a brighter note, nothing seems to be as messed up as an unprovable exercise from the Lovett's book, and every typo is kinda handled by the context.

Also, the exercise numbering in this book is a tad bit messed up: it enumerates all the exercises for a given chapter in one sequence without splitting on the section of a chapter. I don't bother translating them to the normal format, and by extension some references in the text of the exercise is a bit messed up.

Some of the notation migrated from my previous endeavours in the maths. Notably for permutation groups I often use a cyclic representation, where I do not skip identities. Some of the notation comes from the book, notable examples of this notation are:

$\langle g \rangle$ - a cyclic group that is generated by g

also it is not explicitly defined, but \cong is presumed to mean isomorphism

I might mix up isometry and isomorphy here and there, but it's pretty clear from context what exactly do I mean.

Chapter 1

A Potpourri of Preliminary Topics

All of the topics, discussed in this chapter I know already; skip

Chapter 2

Groups - Part 1

Notes

I'm gonna use the symbol $*$ as the generic group function and e as an identity until stated otherwise since it's most convenient to me. Sometimes I'll omit $*$ whenever it's clear what's going on. Also, sometimes I omit parenthesis, but given that we've got associativity, we can omit them without problems. For rigorousness' sake, I'll define it to mean left-associative (i.e. $a * b * c = (a * b) * c$).

2.1 Introduction to Groups

2.1.1

By substituting shapes for numbers we get a trivial exercise

2.1.2

Let n be a positive integer, and let S_n be the group of permutations of the set $\{1, 2, \dots, n\}$ as described in Example 2.19. Prove that S_n is a finite group, and give a formula for the order of S_n .

From the combinatorics we know that the number of permutations is exactly the factorial of the cardinality of the underlying set.

2.1.3

(a) Let S be a finite set, and let $\phi : S \rightarrow S$ be a function. Prove that the injectivity, surjectivity, and bijectivity of this function are equivalent

I'm pretty sure that we've proven that rigorously in the set theory course. If not, then the proof comes from contradiction and the cardinality of the codomain of, which proves

that injectivity and surjectivity are equivalent, and bijectivity comes from definition.

(b) Give an example of an infinite set S and a function $\phi : S \rightarrow S$ such that ϕ is injective but not surjective

We can let $S = \omega$, $\phi(x) = 2x$, which gives us range of even numbers.

(c) Give an example of an infinite set S and a function $\phi : S \rightarrow S$ such that ϕ is surjective but not bijective

We can set $S = \omega$ and

$$\phi(x) = \begin{cases} x = 0 \rightarrow 1 \\ x - 1 \text{ otherwise} \end{cases}$$

2.1.4

This one involves drawing and is pretty trivial; skip

2.2 Abstract Groups

2.2.1

Let G be a group. In this exercise you will prove the remaining parts of Proposition 2.9. Be sure to justify each step using the group axioms or by reference to a previously proven fact

(a) G has exactly one identity element.

Suppose that e_1 and e_2 both satisfy identity axiom. We follow that both of them are in G and thus

$$e_1 = e_1 e_2 = e_2 e_1 = e_2$$

which comes directly from the Identity Axiom.

(b) $g, h \in G \Rightarrow (g * h)^{-1} = h^{-1} g^{-1}$

We follow that

$$(g * h)^{-1} (g * h) = e$$

by definition of identity. Thus

$$(g * h)^{-1} (g * h) * h^{-1} = e h^{-1}$$

$$(g * h)^{-1} (g * h) * h^{-1} g^{-1} = e h^{-1} g^{-1}$$

by the fact that $*$ is a binary function. Thus

$$(g * h)^{-1} g * (h * h^{-1}) * g^{-1} = e h^{-1} g^{-1}$$

$$(g * h)^{-1} g * g^{-1} = e h^{-1} g^{-1}$$

$$(g * h)^{-1} (g * g^{-1}) = e h^{-1} g^{-1}$$

$$(g * h)^{-1} = eh^{-1}g^{-1}$$

by associative laws, and then we've got that

$$(g * h)^{-1} = h^{-1}g^{-1}$$

by the identity axiom, as desired

$$(c) \ g \in G \Rightarrow (g^{-1})^{-1} = g$$

We follow that

$$(g^{-1})^{-1} * (g^{-1}) = e$$

by the inverse axiom. Thus

$$(g^{-1})^{-1} * (g^{-1}) * g = e * g$$

$$(g^{-1})^{-1} * (g^{-1}) * g = g$$

by identity and properties of functions. Thus

$$(g^{-1})^{-1} * ((g^{-1}) * g) = g$$

$$(g^{-1})^{-1} * e = g$$

$$(g^{-1})^{-1} = g$$

by associativity and so on, as desired.

2.2.2

Let G be a group, let $g, h \in G$, and suppose that g has order n and that h has order m .

(a) If G is an abelian group and if $\gcd(m, n) = 1$, prove that the order of gh is mn .

Firstly, I want to follow a couple of things:

If order of g is m , and order of g^{-1} is not $n < m$, then

$$e = e * e = g^m(g^{-1})^n = g^{m-n} = e$$

which is a contradiction. Similar case holds for $n > m$. Thus if order of g is n , then order of g^{-1} is also n .

We also follow that if g has finite order n , then $(g^k)^n = (g^n)^k = e$, and thus g^k has finite order for any $k \in \mathbb{Z}$. Moreover, since $(g^k)^n = e$ we follow that g^k 's order divides n .

We also follow that if g has finite order n , then

$$g * g^{n-1} = e$$

$$g^{n-1} = g^{-1}$$

Now back to our exercise. We follow that

$$(gh)^{mn} = g^{mn}h^{mn} = (g^n)^m(h^m)^n = e^m e^n = e$$

where we can split it this way since G is abelian. Thus we follow that order of gh is finite and divides mn .

Suppose that the order of gh is k . We follow that $k \leq mn$ since it divides mn .

$$(gh)^k = e$$

thus

$$(gh)^k = g^k h^k = e$$

if $g^k \neq e$, then we follow that $h^k = (g^k)^{-1} \neq e$, thus $h^k = (g^{-1})^k = (g^{n-1})^k$. Thus we follow that h^k is a multiple of g , and thus its order divides order of g m . Since h^k is both multiple of g and h , we follow that its order divides both m and n , and since $\gcd(m, n) = 1$, we follow that its order is 1. Thus $h^k = e$, which is a contradiction.

Thus we conclude that $g^k = e$. For h^k we've got a similar case. Thus we follow that k divides both m and n , and thus it's either 1 or mn . If $k = 1$, then we follow that $g = h^{-1}$, and thus $\gcd(m, n) = 1$ implies that the order of both g and h cannot be anything other than 1, and thus $k = mn = 1$. If $k \neq 1$, then we follow that $k = mn$, as desired.

(b) Give an example showing that (a) need not be true of we allow $\gcd(m, n) > 1$

We can have some group where order of g is $n > 1$ (for example $g = 1$ in $G = \mathbb{Z}/5$) and set $h = g^{-1}$, for which we'll have that order of gh is 1.

(c) Give an example of a nonabelian group showing that (a) need not be true even if we retain the requirement that $\gcd(m, n) = 1$.

A dihedral group of a triangle with $g = r$ and $h = f$ will do. We'll have that order of rf is 2:

$$(rf)^2 = (rf)(rf) = f^{-1} r r f = e$$

with order of g being 2 and order of h being 3

(d) Again assume that G is an abelian group, and let $l = mn/\gcd(m, n)$ (i.e. $l = \text{lcm}(m, n)$). Prove that G has an element of order l .

We follow that n divides order of g^m . We also follow that m divides order of h^n . Since $l = \text{lcm}(m, n)$ is divided by both m and n we follow that $g^m h^n$'s order divides l .

If there's $k \leq \text{lcm}(m, n)$ such that

$$(g^m h^n)^k = e$$

then we follow that

$$g^{mk} h^{nk} = e$$

Here we're gonna employ a more generalized version of an argument in part (a): If $g^{mk} \neq e$, then $k < \text{lcm}(m, n)$, thus h^{nk} 's order is a multiple of both m and n . h^{nk} cannot be 1, and its order must be then $\text{lcm}(m, n)$ or 1, and it can be neither, thus we've got a contradiction. Thus we conclude that $g^{mk} = h^{nk} = 1$, which implies that k divides both m and n , which implies that $k = \text{lcm}(m, n)$, as desired.

2.2.3

Definition 2.6 says that a group is a set G with a composition law satisfying three axioms. In particular, it says that there's an identity element $e \in G$ that works on both sides and that every element $g \in G$ has an inverse that works on both sides. Suppose that we weaken the requirements to specify that the identity and inverse work only on one side. In other words, we suppose that G is a set with a composition law satisfying the following weaker axioms:

(a) (*Right-Identity Axiom*) *There is an element $e \in G$ so that $g * e = g$ for all $g \in G$*

(b) (*Right-Inverse Axiom*) *For all $g \in G$ there is an element $h \in G$ so that $g * h = e$*

(c) (*Associative Law*) *$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ for all $g_1, g_2, g_3 \in G$.*

Prove that G is a group.

We're gonna start with establishing the inverse axiom for G , as suggested in the hint to the exercise. Suppose that for $g \in G$ there's $h \in G$ such that

$$g * h = e$$

we also follow that for h there's an element k such that $h * k = e$ by the same axiom. We thus follow that

$$h * g = h * g * e = h * g * h * k = h * (g * h) * k = h * e * k = (h * e) * k = h * k = e$$

where we use justification of

$$a \rightarrow (h * k = e) \rightarrow c \rightarrow b \rightarrow c \rightarrow a \rightarrow (h * k = e)$$

in our equalities (given axioms are presented by letters). Thus we've got that $h * g = e = g * h$ (i.e. normal inverse axiom)

Now suppose that $g \in G$. We follow that

$$e * g = g * g^{-1} * g = g * (g^{-1} * g) = g * e = g$$

which practically establishes the Identity axiom. The associative law is unchanged from the standard definition of the group, and thus we're following that G is indeed a group, as desired.

2.2.4

There are other sorts of algebraic structures that are similar to groups in that they are sets S that have a composition law

$$S \times S \rightarrow S, (s_1, s_2) \rightarrow s_1 * s_2$$

but they have fewer or different axioms than a group. In this exercise we explore two of these structures.

The set S with its composition law is a monoid if it has an identity element $e \in S$ and satisfies the associative law, but elements are not required to have inverses.

The set S with its composition law is a semigroup if its composition law is associative, but it need not have an identity element or inverses.

i.e. monoid satisfies associative and identity, semigroup satisfies associative, and group satisfies all of them. Hence we've got nested classes of structures:

semigroup \subseteq monoid \subseteq group

For each of the following sets S and composition laws $$ determine if $(S, *)$ is a group, a monoid, or a semigroup.*

(a) *The set of natural numbers $N = \{1, 2, 3, \dots\}$ with the composition law being addition.*

I usually do include 0 into the set of naturals, but in this particular case it seems that we don't do it.

In this particular case we follow that N has associativity with $+$, rigorous proof of which comes from the construction of the naturals. In the course of the set theory I've gone through that proof, but I'm pretty sure that it's not required here.

If we don't include 0 into N , then we don't have an identity in N , which can be proven by defining order $>$ on N and proceeding from there (which was also handled in the course on set theory). Hence it is only a semigroup. If we include it, however, then we get an identity, and thus this set becomes a monoid.

We can also state that it's not got identities.

(b) *The set of extended natural numbers $N_0 = \{0, 1, 2, 3, \dots\}$ with the composition law being addition.*

handled in part (a)

(c) $(\mathbb{Z}, +)$

We can follow that it's a superset of N , which gets its inverses ($a^{-1} = -a$) and hence becomes a full-blown group.

(d) $(N, *)$

We follow that it's associative, has the identity 1, and hence is at least a monoid. It's not got multiplicative inverses (because that would be \mathbb{Q}_+), and hence is not a group.

(e) $(N_0, *)$

Same as previous, 0 does not change associativity and identities. Is not a group for the same reason as the previous case.

(f) $(\mathbb{Z}, *)$

Same as previous for the same reason.

(g) *The set of integers \mathbb{Z} with the composition law $m * n = \max\{m, n\}$*

If there's $m \in \mathbb{Z}$, then there's $n_0, n_1 \in \mathbb{Z}$ such that

$$n_0 < m < n_1$$

and hence

$$n_0 * m = n_0, n_1 * m = m$$

and hence we follow that there's no identity.

We follow that

$$(n * m) * k = \max\{\max\{n, m\}, k\} = \max\{n, m, k\} = \max\{n, \max\{m, k\}\} = n * (m * k)$$

hence we've got associativity. Thus the given structure is a semigroup.

(h) *The set of naturals N with the composition law $m * n = \max\{m, n\}$*

It's got associativity and hence this thing is a semigroup. We can follow that $1 \leq m$ for all $m \in N$, and thus $\max\{1, m\} = m$. Thus we follow that we also have a monoid. Inverses are not present, and thus it's not a group.

(i) *The set of naturals N with the composition law $m * n = \min\{m, n\}$*

We've got associativity. If $m \in N$, then there's $n \in N$ such that $n > m$, and thus $\min\{m, n\} = m$, which means that there's no identity, and hence this thing is only a semigroup.

(j) *The set of naturals N with the composition law $m * n = mn^2$*

We follow that

$$(m * n) * k = (mn^2) * k = mn^2k^2$$

$$m * (n * k) = m * nk^2 = mn^2k^4$$

setting m, n, k to primes we can follow that $(m * n) * k \neq m * (n * k)$, which implies that this thing is neither a group, a monoid, nor a semigroup.

2.2.5

Look up magmas, Moufang loops, quandles, and matroids

Magma is just a set with a binary function. There are some discussions about closure, but as long as the thing provided with a set is a binary function, it's a magma.

TODO: look up the rest

2.3 Interesting Examples of Groups

Notes

Although I'm pretty sure that the collection of groups is a proper class (i.e. not a set), I don't have a proof for that. I'll try to change it now.

Empty sets cannot be groups since they've gotta have an element (identity).

Although we can try to do something with cardinals and whatnot, we know that for any set S there's an injection to the set S^S . We then follow that there's a subset of bijections in S^S . We then follow that this subset of bijections is a group (permutations), and hence we conclude that for each set there's a group, and thus a collection of groups is a proper class, as desired.

We can also skip all this stuff, and state singleton of any set S is a trivial group under projection. Trivial group (if I'm not mistaken) is a group that's got only an identity in it.

Permutation Group practically states that a set of bijections over a set constitutes a group under composition. There are no further restrictions, which is pretty neat.

Matrix group leads us to an interesting idea, which is also bleeding into dihedral groups: as long as a subset of the set of bijections is closed under composition, includes inverses, and includes an identity, given subset is a group (associativity is a property of composition). Can we lose some restrictions though?

Suppose that there's a set of bijections over a set and it is closed under composition. If a set is finite, then we can follow that the set of pairs of bijections is larger than the set of bijections, hence there's got to be a pair

$$S \circ C = S$$

or something like that, which would imply that C is an identity. If the set is infinite, then this proof will not do. Finality of the set does not imply the existence of inverses: $\{C, e\}$ will be closed under composition, will have an identity, and will not have inverses.

Given a set of nonzero naturals N , for each $n \in N$ we can have $S_n : \omega \rightarrow \omega$

$$S_n(x) = x + n$$

For each $n, m \in N$ we've got that

$$(S_n \circ S_m)(x) = S_n(x + m) = x + m + n = S_{m+n}(x)$$

which gives us a set of bijections, that is closed under a composition, does not include an identity ($0 \notin N$ by our restriction), and no element has an inverse.

Thus we conclude that if a set of bijections is finite and is a singleton, then it's a group. If it's not a singleton and is finite, then it's a monoid (i.e. associativity and identity). If it's not finite, then it's just a semigroup (i.e. associativity exclusively).

We can't have a group of functions, where the set is not a singleton and domain and range of the function are distinct, since two functions are supposed to compose. We can't have non-bijections be present, since we've got to have both left-hand side and right-hand side inverses of any given element.

2.3.1

Let G be a finite cyclic group of order n , and let g be a generator of G . Prove that g^k is a generator of G if and only if $\gcd(k, n) = 1$.

Suppose that g^k is a generator of G . If $k = 1$, then we follow that $\gcd(k, n) = \gcd(1, n) = 1$, thus assume that $k \neq 1$.

We follow that there's $m \in \omega$ such that $m \neq 0$ and

$$(g^k)^m = g^{km} = g$$

thus

$$g^{km-1} = e$$

and hence we follow that $km - 1$ is multiple of order of G . Thus there exists $j \in Z$ such that $km - 1 = jn$. Thus $km - jn = 1$, which implies that $\gcd(k, n) = 1$, as desired.

Every implication in the forward direction is pretty much a biconditional (not exactly though, we need to add some quantifiers to the mix), so it works in the reverse direction as well.

Also, we haven't gone into a proof that $\gcd(m, n) = l$ if and only if l is the lowest positive number such that there exist $i, j \in Z$ such that

$$mi + jn = l$$

but we've essentially proven the result for $\gcd(m, n) = 1$ in 1.35

2.3.2

Skip

2.3.3

Prove that the Dihedral group D_n , as described in Example 2.22, has exactly $2n$ elements

We can follow that there are n vertices, and each of them gotta go to one of the other n spaces. There are n ways to put the first vertex into any of those places. Whenever we put the first vertex n into some place, there are 2 places where the second vertex can go, so now we're down to $2n$ possible positions. Whenever we put the second vertex down, positions of the rest are determined, and hence we can follow that there are total of $2n$ possible positions, as desired.

2.3.4

(a) Let Q^ be the set of non-zero rational numbers, with the group law being multiplication. Prove that Q^* is a group.*

We follow that $1 * q = q$, and hence we've got an identity. If $q \in Q^* \Rightarrow q \neq 0 \wedge q \in Q$, then we follow that $1/q$ exists, and thus there's q^{-1} such that $qq^{-1} = 1$. Multiplication's associativity does not require a proof (or can be provided, but in this course it is assumed), and thus we conclude that Q^* is a group (moreover, an abelian group), as desired.

the rest is skipped

2.3.5

(b) Let p be a prime number. Prove that the set of non-zero elements of Z/pZ is a group using multiplication as the group law

We follow that for each $i \in \mathbb{Z}/p\mathbb{Z}$, $i * 1 = i$, and thus i is our identity. Associativity of multiplication under \mathbb{Z} implies our associativity.

From group theory we know that there's x such that $ax \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$. We then follow that for any given $i \in \mathbb{Z}/p\mathbb{Z}$ we've got that $\gcd(i, p) = 1$ since p is prime, and thus there's $a \in \mathbb{Z}/p\mathbb{Z}$ such that $a * i = 1$. Thus we've got the inverse, and $\mathbb{Z}/p\mathbb{Z}$ is a group under multiplication, as desired.

We can probably also prove the other direction if we want. If p is not 1 and is not a prime, then there's a divisor q of p in $\mathbb{Z}/p\mathbb{Z}$, which implies that only multiple of q is its multiple, or 0, which implies that it's got no inverse and hence $\mathbb{Z}/p\mathbb{Z}$ is not a group, as desired. If p is not a prime, however, then we've got that $\mathbb{Z}/p\mathbb{Z}$ is a trivial group. We can probably reword this thing so it becomes a theorem, but I'm too lazy to do this.

(c) Heck, I've proven this already and I didn't even read this section

(d) blah blah blah

Got pretty much the same proof as part (a). The only thing of note is that we've got new notation:

$$(\mathbb{Z}/p\mathbb{Z})^*$$

which is a group under multiplication of numbers relatively prime to p .

2.3.6

Let C be the set of complex numbers, that is, the (... a crude definition of complex numbers)

(a) We make C into ...

It's a group under addition, yes. Proof is trivial

(b) $C^* = C \setminus \{0\}$ is a group under multiplication.

Yes it is. Multiplicative inverse is kinda whacky in complex numbers, let me find it:

$$\frac{1}{a+bi} = \frac{(a-bi)}{(a+bi)(a-bi)} = \frac{(a-bi)}{a^2-b^2i^2} = \frac{(a-bi)}{a^2-b^2*(-1)} = \frac{(a-bi)}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

which I would never ever find on my own, if I wouldn't start a complex analysis course at some time in the past (probably should look into it not, this thing looks pretty fun)

2.3.7

(a) Let

$$GL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, ad - bc \neq 0 \right\}$$

be the indicated set of 2-by-2 matrices, with composition law being matrix multiplication. Prove that $GL_2(R)$ is a group.

It's a set of bijections, that is closed under composition (see linear algebra course), each element is invertible by the restriction, and has identity, thus it's a group. We can also

scale this thing to complex numbers, and we can also increase dimensions of the underlying sets and substitute restriction from the determinant-based to just being invertible (which are equivalent).

(b) Let

$$SL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, ad - bc = 1 \right\}$$

be the indicated set of 2-by-2 matrices, with composition law being matrix multiplication. Prove that $SL_2(R)$ is a group.

Same logic as before. We can scale with determinants here as well.

This group does not include all the isometries though, which is kinda interesting. Some isometries (e.g. 1, -1 on diagonal) will not be included here. TODO: research this thing a bit more

(c) ...

Pretty much is solved by my discussion in previous points. A thing to remember though:

General linear group is a set of invertible linear functions.

Special linear group is a set of matrices with 1 for the determinant.

2.3.8

Let $GL_2(R)$ be the general linear group. Prove or disprove that each of the following subsets of $GL_2(R)$ is a group. In the case of non-groups, indicate which of the group conditions fail.

(a)

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, ad - bc = 2 \right\}$$

Not a group, identity is not in there, and composition is not closed ($|AB| = |A||B| = 2 * 2 = 4$)

(b)

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, ad - bc \in \{1, -1\} \right\}$$

Is a group, pretty sure that those describe the isometries.

(c)

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, c = 0 \right\}$$

Is a set of upper-triangulars, which are closed under composition, and contain the identity. Inverses of upper-triangular are also upper-triangular, thus we've got a group.

(d)

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, d = 0 \right\}$$

Does not contain the identity, and inverses arent present

(e)

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, a = d = 1, c = 0 \right\}$$

Pretty sure that this once is a group as well.

2.3.9

Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of quaternions. We claimed that the group law for Q is determined by

$$i^2 = j^2 = k^2 = ijk = -1$$

Use these formulas to prove following formulas, which completely determine the group operations on Q :

We firstly follow that $(-1)^{-1} = -1$. Thus

$$i * i = -1$$

$$(i * i)^{-1} = (-1)^{-1}$$

$$i^{-1} * i^{-1} = -1$$

$$i^{-1} = -1 * i$$

$$i^{-1} = -i$$

where the last part comes from the note that -1 commutes with everything. We can follow that $k^{-1} = -k$ and $j^{-1} = -j$ by the same logic.

We follow now that

$$i * j = i * j * 1 = i * j * (k * -k) = (i * j * k) * -k = -1 * -k = k$$

$$j * k = 1 * j * k = (-i * i) * j * k = -i * -1 = i$$

$$k * i = 1 * k * i = -j * j * k * i = -j * (j * k) * i = -j * i * i = -j * -1 = j$$

we then follow that

$$-k = k^{-1} = (i * j)^{-1} = -j * -i = j * i$$

and so on for all the inverses.

2.3.10

Skip

2.3.11

Practically continue with the functions in the notes. Part (a) is handled

(b) If X is a finite set with n elements, Prove that \mathcal{E}_X is a finite monoid and compute how many elements it has.

We follow that the number of functions is n^n , the rest is handled in the notes

(c) If $|X| \geq 3$, prove that \mathcal{E}_X is not commutative, i.e. show that there are elements $\phi, \psi \in \mathcal{E}_X$ satisfying $\phi \circ \psi \neq \psi \circ \phi$.

We can map a portion of this set to 1, 2, 3, and then get functions

$$\phi(x) = \begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 2 \\ 3 \rightarrow 2 \end{cases}$$

$$\psi(x) = \begin{cases} 1 \rightarrow 3 \\ 2 \rightarrow 3 \\ 3 \rightarrow 3 \end{cases}$$

which will suffice.

2.4 Group Homomorphism**2.4.1**

Recall that two groups G_1, G_2 are said to be isomorphic if there is a bijective homomorphism

$$\phi : G_1 \rightarrow G_2$$

The fact that ϕ is bijective means that the inverse map $\phi^{-1} : G_2 \rightarrow G_1$ exists. Prove that ϕ^{-1} is a homomorphism from G_2 to G_1 .

We essentially need to prove that

$$\phi^{-1}(h_1 * h_2) = \phi^{-1}(h_1) * \phi^{-1}(h_2)$$

for all $h_1, h_2 \in G_2$.

ϕ is a bijection, and thus for $h_1, h_2 \in G_2$ there are $g_1, g_2 \in G_1$ such that $\phi(g_1) = h_1, \phi(g_2) = h_2$. By the fact that ϕ is a bijection we also follow that $g_1 = \phi^{-1}(h_1), g_2 = \phi^{-1}(h_2)$. Thus we've got that

$$\phi^{-1}(h_1 * h_2) = \phi^{-1}(\phi(g_1) * \phi(g_2)) = \phi^{-1}(\phi(g_1 * g_2)) = g_1 * g_2 = \phi^{-1}(h_1) * \phi^{-1}(h_2)$$

as desired

2.4.2

Let G be a group, and consider the function

$$\phi : G \rightarrow G, \phi(g) = g^{-1}$$

(a) Prove that $\phi(\phi(g)) = g$ for all $g \in G$

$$\phi(\phi(g)) = \phi(g^{-1}) = (g^{-1})^{-1} = g$$

(b) Prove that ϕ is a bijection.

We follow that for each $g \in G$ there's $g^{-1} \in G$, thus $\phi(g^{-1}) = g$, which implies that the range of ϕ is G .

We follow that if $g_1 \neg g_2$, then $g_1^{-1} \neq g_2^{-1}$, and thus ϕ is injective.

(c) Prove that ϕ is a group homomorphism if and only if G is an abelian group.

Forward direction: We know that ϕ is bijective, and thus for all $h_1, h_2 \in G$ there are $g_1, g_2 \in G$ such that $\phi(g_1) = h_1, \phi(g_2) = h_2$. If G is a group homomorphism, then we follow that

$$h_1 * h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = h_2 * h_1$$

thus the group is abelian.

Reverse direction:

Let us keep assumptions about our variables. If G is abelian, then we follow that

$$h_2 * h_1 = g_2^{-1}g_1^{-1} = (g_1g_2)^{-1} = \phi(g_1g_2)$$

$$h_1 * h_2 = g_1^{-1}g_2^{-1} = \phi(g_1) * \phi(g_2)$$

Since G is abelian we follow that $h_1h_2 = h_2h_1$, and thus we can equate given equalities to get the desired result.

2.4.3

Skip

2.4.4

Let G_1 and G_2 be groups, and suppose that $\phi : G_1 \rightarrow G_2$ is an isomorphism

(a) Prove that if G_1 is finite, then G_2 is also finite, and that they satisfy $|G_1| =_c |G_2|$

Isomorphism is a bijection, thus sets have equal cardinality.

(b) Suppose that G_1 is abelian. Prove that G_2 is abelian

Let $g_1, g_2 \in G_2$. Since ϕ is a bijection we follow that there are $h_1, h_2 \in G_1$ such that $\phi(h_1) = g_1$ and $\phi(h_2) = g_2$. We follow that

$$g_1g_2 = \phi(h_1)\phi(h_2) = \phi(h_1h_2) = \phi(h_2h_1) = \phi(h_2)\phi(h_1) = g_2g_1$$

as desired.

The solution for the rest of this exercise practically copies the structure of part (a)

2.4.5

In this exercise, C_n is a cyclic group of order n , D_n is the n th dihedral group, and S_n is the n th symmetric group.

(a) Prove that C_2 and S_2 are isomorphic.

We follow that both C_2 and S_2 have 2 and $2! = 2$ elements respectively. Non-identity elements can interact with identity in a predictable way, or with themselves, where they've got an order of 2. This pretty much concludes the proof.

(b) Prove that D_3 is isomorphic to S_3 .

We know that D_3 is a subgroup (although we haven't defined at this point what a subgroup is, it doesn't take a genius to guess) of S_3 , with the same cardinality.

(c) Let $m \geq 3$. Prove that for every n , the groups C_m and S_n are not isomorphic.

If $m \neq n!$, then we follow that groups have different cardinalities, thus there's no bijection between the two, and thus no isomorphisms.

If $m = n!$, then we follow that since $m \geq 3$ that $n \geq 3$ as well. We follow that there are elements of S_n that map $(1, 2, 3)$ to $(1, 3, 2)$ and $(2, 1, 3)$ and the rest to identity. Composition of those elements is not commutative ($(2, 3, 1)$ and $(3, 1, 2)$ in forward and reverse respectively), and thus S_n is not abelian. C_n on the other hand is commutative, and thus we follow that they aren't isomorphic. This also proves that S_n is non-abelian for any $n \geq 3$.

(d) Prove that for every $n \geq 4$ the groups D_n and S_n aren't isomorphic

They don't have the same cardinalities.

(e) More generally, let $m \geq 4$, and let $n \geq 4$. Prove that the groups D_m and S_n aren't isomorphic.

We once again look at the case when $2m = n!$. We probably want to find some irregularities with orders of the elements here. We follow that if m is odd, then there is only 1 element of order 2 (f). If m is even, then we've got 3 such elements ($f, r^{m/2}, fr^{m/2}$). For S_n for $n \geq 4$ we follow that there are at least 6 of them (bijections that swap elements, there are $C(4, 2) = 6$ of them at least).

(f) The cyclic group C_8 , the dihedral group D_4 , and the quaternion group Q are non-abelian groups of order 8. Prove that they aren't isomorphic.

First of all, C_8 is abelian (as is any cyclic group for that matter). If we ignore that, then we can follow that there is one element of order 4 (2) in C_8 , and there are 6 ($\pm i, \pm j, \pm k$) in Q . There are 3 elements of order 2 in D_4 , but only one in C_8 . Q has 1 element of order 2.

2.4.6

Skip

2.5 Subgroups, Cosets, and Lagrange's Theorem

Notes

Important definition from the exercises: Let G be a group, and let $S \subseteq G$ be a subset of G . The subgroup of G generated by S , which we denote by $\langle S \rangle$, is the intersection of all of the subgroups of G that contains S ; i.e.

$$\langle S \rangle = \bigcap_{S \subseteq H \subseteq G: H \text{ is a subgroup of } G} H$$

Exercise proves that $\langle S \rangle$ is essentially a subgroup, where every element is a multiple of some combination (i.e. ordered list in non-abelian and multiset in abelian) of elements of S or their inverses, and also the smallest subgroup, that contains the entirety of S .

Another important definition is the definition of centralizer. The centralizer of the subset $(Z_G(S))$ is the most general of them, they are provided below

We also follow that if H_1, H_2 are subgroups of G , then $H_1 \cap H_2$ is a subgroup of G , which is sort of trivial to prove. Important to note that union of two subgroups is not necessarily a group.

2.5.1

Let G be a group and let $g \in G$ be an element of order n , and let $k \geq 1$.

(a) Prove that g^k has order $n/\gcd(n, k)$.

We follow that g is a generator for a cyclic group, in which multiples of g^k comprises a subgroup. Since g has order n we follow that $\langle g \rangle$ is a cyclic group of order n .

We know that $\gcd(n, k)$ is the lowest number that is a positive sum of multiples of n and k respectively. Thus there are integers a, v such that

$$an + vk = \gcd(n, k)$$

We then follow that

$$(g^n)^a * (g^k)^v = g^{\gcd(n, k)}$$

order of g is n and thus

$$(g^n)^a * (g^k)^v = (e)^a * (g^k)^v = e * (g^k)^v = (g^k)^v = g^{\gcd(n, k)}$$

We thus follow that multiples of $g^{\gcd(n, k)}$ are in cyclic subgroup of g^k . There are exactly $n/\gcd(n, k)$ such elements.

Suppose that v is not a multiple of $\gcd(n, k)$ and suppose that there's $j \in Z_+$ such that $(g^k)^j = g^{k*j} = g^v$. Since v is not a multiple of $\gcd(n, k)$, it is not a multiple of k . Thus we follow that $k * j > n$. We thus conclude that there's a maximal $h \in Z_+$ such that

$$kj - hn = v$$

$$kj + (-h)n = v$$

thus we conclude that v is a multiple of $\gcd(n, k)$, which is a contradiction.

(b) Use (a) to give a quick proof of Exercise 2.10, which says that $G = \langle g \rangle$ is a cyclic group of order n , then g^k generates G if and only if $\gcd(n, k) = 1$

We follow that if g^k generates G , then $|\langle g^k \rangle| = n/\gcd(n, k) = n$. Thus $\gcd(n, k) = 1$. Reverse case is pretty much the same.

2.5.2

Let G be a cyclic group of order n , and let $d \geq 1$ be an integer.

(a) Prove that every subgroup of G is cyclic.

Since G is cyclic we follow that there's $g \in G$ that generates G .

Suppose that H is a subgroup of G . If $g \in H$, then $G = H$, and thus we're done. Thus suppose that $g \notin H$. We then follow that there is a lowest possible $i \in Z_+$ such that $g^i \in H$. We follow that every multiple of i is in H . Suppose that $k \in Z_+$ is not a multiple of i and such that $g^k \in H$. We follow that $\gcd(k, i) < i$ since k is not a multiple of i . Thus we follow that there are $a, v \in Z$ such that

$$ak + vi = \gcd(k, i)$$

and thus

$$g^{ak} + g^{vi} = g^{\gcd(k, i)}$$

thus $g^{\gcd(k, i)} \in H$, which implies that i is not the lowest element of Z_+ such that $g^i \in H$, which is a contradiction. Thus we conclude that multiples of i are the only elements of H , which implies that H is cyclic, as desired.

Important note: this argument also works for groups G , and so we can follow that any subgroup of any cyclic group is cyclic.

(b) If d divides n , prove that G has a unique subgroup of order d .

Let H_1 and H_2 be two subgroups of order d . We follow that for both of there are least elements i_1, i_2 of Z_+ such that $g^{i_1} \in H_1$ $g^{i_2} \in H_2$. Suppose that $i_1 \neq i_2$ and assume that $i_1 < i_2$. Previous arguments in (a) imply that g^{i_1} and g^{i_2} generate H_1 and H_2 . We know also that H_1 is comprised entirely of powers of g^{i_1} . If $\gcd(i_1, d) \neq i$, we follow that $\gcd(i_1, d) < i$, and thus there are $a, v \in Z$ such that

$$(g^{i_1})^a * (g^d)^v = g^{\gcd(i_1, d)}$$

$$\begin{aligned}(g^{i_1})^a * (e)^v &= g^{gcd(i_1, d)} \\ (g^{i_1})^a &= g^{gcd(i_1, d)}\end{aligned}$$

We thus follow that $g^{gcd(i_1, d)} \in H_1$, and thus i_1 is not the lowest positive integer such that $g^{i_1} \in H$, which is a contradiction. We thus conclude that $gcd(i_1, d) = i_1$, and thus $i_1 | d$. This implies that $|H_1| = |\langle g^{i_1} \rangle| = d/i_1$. Thus if $i_1 \neq i_2$ we follow that $|H_1| \neq |H_2|$, which is a contradiction. Thus we conclude that $i_1 = i_2$, and thus $H_1 = H_2$, as desired.

(c) If d does not divide n , prove that G does not have a subgroup of order d .

We follow that number of cosets of G of order d is a natural number, and thus Lagrange's Theorem implies that order of any subgroup of G divides n , as desired.

2.5.3

Let G be a group, and let $H \subseteq G$. Prove that H is a subgroup if and only if it has the following properties:

- (1) $H \neq \emptyset$
- (2) For every $h_1, h_2 \in H$, $h_1 * h_2^{-1} \in H$

Forward direction is covered by axioms.

Suppose that $H \neq \emptyset$ and for every $h_1, h_2 \in H$, $h_1 * h_2^{-1} \in H$. We follow that there's $h \in H$, and thus $h * h^{-1} = e \in H$. Thus we follow the identity axiom.

Suppose that $k \in H$. We follow that $k \in H$ and $e \in H$, thus $e * k^{-1} = k^{-1} \in H$. Thus we follow the inverse axiom.

Let $h_1, h_2 \in H$. We follow that $h_2^{-1} \in H$, and thus $h_1 * h_2^{-1} \in H$, thus giving us closure, which completes the definition of the subgroup, as desired.

2.5.4

Let G be a group, and let $H \subseteq G$ be a nonempty subset of G . Prove that H is a subgroup if and only if it has the following property:

For every $a \in H$, we have $H = \{ah : h \in H\}$

If H is a subgroup, then we follow that $a \in H$ implies that $a^{-1} \in H$, and thus for every $h \in H$ we follow that $a^{-1}h \in H$, and thus $h = e * h = aa^{-1}h \in \{ah : h \in H\}$, thus $H \subseteq \{ah : h \in H\}$. Reverse subset argument is trivial, and thus those two sets are equal, as desired.

Suppose that for every $a \in H$ we have $H = \{ah : h \in H\}$. Let $b \in H$ be an arbitrary element. We follow that $ab \in \{ah : h \in H\} = H$. We thus follow that all $H = \{ab * h : h \in H\}$. Thus there's an element k of h such that $abk = a$, which implies that $bk = e$, and thus $k = b^{-1}$. Thus we conclude that $b^{-1} \in H$. Since b is arbitrary, we conclude that H contains inverses of its elements. Since $b^{-1} \in H$, we follow that

$$H = \{ah : h \in H\}$$

and thus $ab^{-1} \in H$, which implies that H is a subgroup, as desired.

2.5.5

This exercise generalizes the notion of the cyclic subgroup generated by an element of a group as described in Example 2.37. Let G be a group, and let $S \subseteq G$ be a subset of G . The subgroup of G generated by S , which we denote by $\langle S \rangle$, is the intersection of all of the subgroups of G that contains S ; i.e.

$$\langle S \rangle = \bigcap_{S \subseteq H \subseteq G: H \text{ is a subgroup of } G} H$$

We also note that the set of subgroups of G is a subset of $\mathcal{P}(G)$, and thus let us define

$$K = \{H \in \mathcal{P}(G) : H \text{ is a subgroup of } G \text{ and } S \subseteq H \subseteq G\}$$

which is a set and our original definition can be rewritten as

$$\langle S \rangle = \bigcap_{H \in K} H$$

(a) Prove that S is not an empty set.

We follow that S is a subset of G , $G \subseteq G$, and G is a subgroup of G , and thus

$$g \in K$$

Thus K is nonempty, which is also important, since there are no intersections of empty sets. We follow that every subgroup of G contains e , and thus $e \in \langle S \rangle$, as desired.

(b) Prove that $\langle S \rangle$ is a subgroup of G

Let $a, b \in \langle S \rangle$. We follow that every element of K contains a, b , and since every element of K is a subgroup that b^{-1} is also in every element of K . Thus ab^{-1} is also in every element of K , and thus $ab^{-1} \in S$, which implies that S is a subgroup, as desired.

(c) Suppose that L is a subgroup of G and that $S \subseteq L$. Prove that $\langle S \rangle \subseteq L$. (The whole text of this part of the exercise is one big typo)

We follow that $L \in K$, and thus $\langle S \rangle = \bigcap_{H \in K} H \subseteq L$ by definition.

(d) Let T be the set of inverses of the elements in S ; i.e.

$$T = \{g^{-1} : g \in S\}$$

Prove that $\langle S \rangle$ is equal to the following set of products

$$\langle S \rangle = \{e * g_1 g_2 \dots g_n : g_{1..n} \in S \cup T\}$$

(I've deviated a tad bit from the definition in the book since we gotta take care of the $S = \emptyset$ case))

We firstly follow that $S \subseteq \langle S \rangle$, and since $\langle S \rangle$ is a subgroup of G we conclude that $T \subseteq \langle S \rangle$ by definition of T . We thus follow that for any

$$q \in \{e * g_1 g_2 \dots g_n : g_{1..n} \in S \cup T\}$$

$q \in \langle S \rangle$ by closure of composition in the subgroup, thus we've got the \supseteq case.

We now follow that rhs is nonempty by definition (in case when $S = \emptyset$ we follow that $e \in rhs$). If $a, b \in rhs$, then there are finite lists l_1, l_2 over elements of $S \cup T$ such that

$$\prod l_1 = a; \prod l_2 = b$$

we thus follow that b^{-1} is also in rhs since inverses of $S \cup T$ is closed under inverses by definition, and thus we've gotta invert elements of l_2 and order them in reverse to get b^{-1} . Thus we conclude that $ab^{-1} \in rhs$ since ab^{-1} will be just a longer list of elements of $S \cup T$, and thus we follow that rhs is a subgroup of G that contains S . This implies that $\langle S \rangle \subseteq rhs$ by definition, which in tandem with previous paragraph gives us the desired equality.

2.5.6

Let G be a finite group, let $m \geq 1$ be an integer, and let

$$G[m] = \{g \in G : g^m = e\}$$

be the set of elements of G whose order divides m .

(a) If G is an abelian group, prove that $G[m]$ is a subgroup of G .

We follow that $e^m = e$, thus $e \in G[m]$, and thus $G[m] \neq \emptyset$.

We follow that if $b \in G$, then $b^m = e$, thus $(b^{-1})^m = e$, and thus $b^{-1} \in G[m]$. Let $a, b \in G[m]$. We follow that $(ab^{-1})^m = a^m b^{-m} = e * e = e$ where we can use the first equality due to the fact that G is abelian, which implies that $ab^{-1} \in G[m]$, which implies that $G[m]$ is a subgroup, as desired.

(b) Give an example of non-abelian group and $m \geq 1$ such that $G[m]$ is not a subgroup of G .

We are aware of several non-abelian groups: permutation group, special linear group, and dihedral group.

Let us look at D_3 and get all orders of that group:

$$|e| = 1$$

$$|r| = 3$$

$$|r^2| = 3$$

$$|s| = 2$$

$$|sr| = 2$$

$$|sr^2| = 2$$

We thus follow that $D_3[2] = \{e, s, sr, sr^2\}$. We then follow that $|ssr| = |r| = 3$, and thus we conclude that this set is not closed under composition, and thus it is not a group, as desired.

2.5.7

Skip

2.5.8

Let G be a group, let $A, B \subseteq G$ be subgroups of G , and let ϕ be the map

$$\phi : A \times B \rightarrow G, \phi(a, b) = ab$$

(a) Prove that $A \cap B = \{e\}$ if and only if the map ϕ is an injection

Suppose that $A \cap B = \{e\}$. Let $a_1, a_2 \in A$, $b_1, b_2 \in B$, and suppose that

$$\phi(a_1, b_1) = \phi(a_2, b_2)$$

we follow that

$$a_1 b_1 = a_2 b_2$$

$$a_1 = a_2 b_2 b_1^{-1}$$

$$a_2^{-1} a_1 = b_2 b_1^{-1}$$

We follow that $a_2^{-1} a_1 \in A$ and $b_2 b_1^{-1} \in B$, and since they are equal we conclude that

$$a_2^{-1} a_1 = b_2 b_1^{-1} = e$$

which implies that $a_1 = a_2$ and $b_1 = b_2$, which in turn implies that ϕ is an injection, as desired.

Now suppose that ϕ is an injection. Suppose that there's $q \in A \cap B$ such that $q \neq e$. Intersection of any two subgroups is a subgroup, and thus $q^{-1} \in A \cap B$. And since $q \neq e$ we follow that $q^{-1} \neq e$. Thus we follow that $\phi(e, e) = e * e = e = qq^{-1} = \phi(q, q^{-1})$ while $\langle e, e \rangle \neq \langle q, q^{-1} \rangle$, which implies that ϕ is not an injection, which is a contradiction.

(b) We can turn $A \times B$ into a group by using the group operation

$$\langle a_1, b_1 \rangle * \langle a_2, b_2 \rangle = \langle a_1 * a_2, b_1 * b_2 \rangle$$

Prove that ϕ is a homeomorphism of groups if and only if element of A commutes with every element of B .

Suppose that ϕ is a homeomorphism. This implies that

$$\phi(\langle a_1, b_1 \rangle * \langle a_2, b_2 \rangle) = \phi(\langle a_1, b_1 \rangle) * \phi(\langle a_2, b_2 \rangle) = a_1 b_1 a_2 b_2$$

it also implies that

$$\phi(\langle a_1, b_1 \rangle * \langle a_2, b_2 \rangle) = \phi(\langle a_1, b_1 \rangle * \langle a_2, b_2 \rangle) = \phi(\langle a_1 * a_2, b_1 * b_2 \rangle) = a_1 a_2 b_1 b_2$$

thus

$$a_1 a_2 b_1 b_2 = a_1 b_1 a_2 b_2$$

for all $a_1 a_2 \in A, b_1, b_2 \in B$. By setting $a_1 = b_2 = e$ we get the desired implication.

By not setting $a_1 = b_1 = e$ and running the argument for the forward implication (with possible reorder of equalities) in reverse we can also get the reverse implication, which gives us the desired result.

2.5.9

Let g be a finite group, and let $A, B \subseteq G$ be subgroup of G , and supposet that $\gcd(|A|, |B|) = 1$. Prove that $A \cap B = e$

$A \cap B$ is a subgroup of both A and B , and thus its order gotta divide orders of both A and B . Since $\gcd(|A|, |B|) = 1$ we conclude that order of $A \cap B$ is 1, which gives us the desired result.

2.5.10

Let G be a group. The center of G , denoted by $Z(G)$, is the seet of elements of G that commute with every other element; i.e.

$$Z(G) = \{g \in G : (\forall h \in G)(gh = hg)\}$$

(a) Prove thtat $Z(G)$ is a subgroup of G .

We follow that for all $h \in H$ we've got that $eh = h = he$, thus $e \in Z(G)$, and hence $Z(G) \neq \emptyset$

Let $a, b \in Z(G)$. Let $h \in G$ be arbitrary. We follow that

$$bh = hb$$

$$(bh)b^{-1} = hbb^{-1}$$

$$(bh)b^{-1} = h$$

$$b^{-1} b h b^{-1} = b^{-1} h$$

$$h b^{-1} = b^{-1} h$$

we thus follow that since h, b are arbitrary that $b \in Z(G)$ implies that $b^{-1} \in Z(G)$.

With the same assumptions we then follow that

$$(ab^{-1})h = a(b^{-1}h) = ahb^{-1} = (ah)b^{-1} = h(ab^{-1})$$

thus $ab^{-1} \in Z(G)$, and thus we conclude that $a, b \in Z(G)$ implies that $ab^{-1} \in Z(G)$, which with nonemptiness of $Z(G)$ gives us the desired result.

(b) *When does $Z(G)$ equal G ?*

The obvious case of equality comes when G is abelian. Assume that G is non-abelian. This implies that there are $a, b \in G$ such that $ab \neq ba$. We thus conclude that neither a nor b are in $Z(G)$, and thus $Z(G) \neq G$, which implies that $Z(G) = G$ if and only if G is abelian.

(c) *Compute the center of the symmetric group S_n .*

We follow that for $n \in \{1, 2\}$, S_n is abelian, and thus $Z(S_2) = S_2$. Let us enumerate elements of S_3 :

$$S_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\}$$

we follow that $Z(S_3)$ includes at least e . Something tells me that $Z(S_3)$ consists exclusively of e . Let us particularly look at the "shift" operator $(2, 3, 1)$ (the one that maps one element to the next with mapping the last element to the first). We follow that any given permutation group contains one. For $n \geq 3$ we can also find an element, that is distinct from the shift element, that swaps two elements in place (we're gonna take $(2, 1, 3)$ in this case). We follow that

$$(2, 3, 1) \circ (2, 1, 3) = (1, 3, 2)$$

$$(2, 1, 3) \circ (2, 3, 1) = (3, 2, 1)$$

thus we follow that shift operator is not in the $Z(S_3)$.

Generally let $a \in \{1, \dots, n\}$, let $q \in S_n$ be an element such that it maps a to itself, and maps $(a + 1) \bmod n$ not to itself, and let $s \in S_n$ be the shift operator. We follow that $(q \circ s)(a) = q(s(a)) = q(a + 1)$ and $s(q(a)) = s(a) = a + 1$. By definition $q(a + 1) \neq a + 1$, and thus we conclude that neither shift operator, nor the element that has partial identity are in $Z(S_n)$.

With a given example we can generalize even more to create a proof for our conjecture:

Let $n \geq 3$ and let $q \in S_n$ be such that $q \neq e$. Since $q \neq e$ we follow that there's an element $a \in \{1, \dots, n\}$ such that $q(a) \neq a$. We then follow that there exists an element $s \in S_n$ such that $s(a) = a$, and $s(q(a)) \neq q(a)$ (we can do this because there are at least 3 elements in $\{1, \dots, n\}$: we take the $q(a)$ and some element $b \in \{1, \dots, n\} \setminus \{q(a), a\}$, then map a to itself, and swap $q(a)$ and b ; the fact that there's an element that is distinct from both $q(a)$ and a is the restriction that fails for S_2). We follow that

$$(s \circ q)(a) = s(q(a)) \neq q(a) = q(s(a)) = (q \circ s)(a)$$

and thus $s \circ q \neq q \circ s$. Therefore we conclude that $q \notin Z(S_n)$. Since the only restriction on q is that $q \in S_n \setminus \{e\}$ we follow that $Z(S_n) = \{e\}$ for all $n \geq 3$, as desired.

(d) Compute the center of the dihedral group D_n .

We follow that

$$s * r \neq r * s = s * r^{n-1}$$

thus neither r nor s are in $Z(D_n)$ for $n \geq 3$. We follow that

$$sr^j * r = sr^{j+1}$$

$$rsr^j = sr^{-1}r^j = sr^{j-1}$$

thus for $n \geq 3$ we follow that $sr^{j+1} \neq sr^{j-1}$, and thus for all $j \in \{1, \dots, n-1\}$ we follow that $sr^j \notin Z(D_n)$. We also follow that

$$r^j * s = sr^{n-j}$$

$$s * r^j = sr^j$$

thus if $j \neq n/2$ we follow that $r^j \notin Z(D_n)$. Thus we follow that if n is odd that $Z(D_n) = \{e\}$. We follow that

$$r^{n/2} * sr^k = sr^{n-n/2+k} = sr^{n/2+k}$$

$$sr^k * r^{n/2} = sr^{n/2+k}$$

for all $k \in \{0, \dots, n\}$. Case with r^k for arbitrary k is trivial, and thus we conclude that if n is even that $Z(D_n) = \{e, r^{n/2}\}$, which is kinda surprising.

(e) Compute the center of the quaternion group Q .

We follow that none of the i, j, k are commuting with each other (by definition), nor do their inverses, and thus none of them are in $Z(Q)$. ± 1 on the other hand commute with everything (once again, by definition), and thus $Z(Q) = \{\pm 1\}$.

2.5.11

Let G be a group, and let $g \in G$. The centralizer of g , denoted $Z_G(g)$ is the set of elements of G that commute with g , i.e.

$$Z_G(g) = \{g' \in G : gg' = g'g\}$$

(a) Prove that $Z_G(g)$ is a subgroup of G .

The proof is pretty much the same as with centralizer of the entire group. We can also note that the definition implies that $Z(G)$ is a subgroup of $Z_G(g)$ for any given $g \in G$. Also important to note that $g \in Z_G(g)$.

(b) Compute the centralizer $Z_G(g)$ for the following groups:

(i) $G = D_4$ and $g = r$

4 is even, and thus $\{e, r^2\}$ are in $Z_G(g)$. Any rotation is also there. $sr \neq sr^3$, and thus s is not included there. $sr^j r = sr^j \neq sr^{j-1} = rsr^j$, which implies that none of the sr^j are in there

(ii) $G = D_4$ and $g = sr^j$

r and r^3 aren't in there. If $j = 2$, then s is also in there, otherwise it isn't. If $j = 2$, then $sr sr^2 = r^3$ and $sr^2 sr = r$, thus sr is not in there. sr^3 is the inverse of sr , and thus it's not in there. The rest can be handled pretty easily.

(iii) $G = GL_2(R)$ and $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$

We follow that this matrix is diagonal, and thus it commutes with other diagonal matrices. If matrix is not diagonal then

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} q & w \\ e & r \end{pmatrix} = \begin{pmatrix} qa & wa \\ ed & rd \end{pmatrix}$$

$$\begin{pmatrix} q & w \\ e & r \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} qa & wd \\ ea & rd \end{pmatrix}$$

thus we need $wa = wd$ and $ea = ed$. Therefore if $a \neq d$ we need $w = e = 0$ and this would include only include other diagonal matrices, that we've already included. If $a = d$, then any matrix will do.

(c) Prove that $Z_G(g) = G$ if and only if $g \in Z(G)$.

IF $g \in Z(G)$, then by definition every element of G commutes with G , and thus $Z_G(g) = G$.

Assume that $Z_G(g) = G$. We follow that every element of G commutes with g , and thus $g \in Z(G)$.

(d) More generally, if $S \subseteq G$ is any subset of G , then the centralizer of S is the set

$$Z_G(S) = \{g \in G : (\forall s \in S)(sg = gs)\}$$

Prove that $Z_G(S)$ is a subgroup of G

Proof is borderline identical to the case of centralizer of group/element.

2.5.12

This exercise explains when two elements of G determine the same coset of H . Let G be a group, let H be a subgroup of G , and let $g_1, g_2 \in G$. Prove that the following three statements are equivalent:

- (1) $g_1 H = g_2 H$.
- (2) There are $h \in H$ such that $g_1 = g_2 h$.
- (3) $g_2^{-1} g_1 \in H$.

Assume that $g_1H = g_2H$. We follow that $e \in H$ and thus $g_1e \in g_2H$. Thus there's $h \in H$ such that $g_1e = g_1 = g_2h$ by definition. Thus

$$g_1 = g_2h$$

$$g_2^{-1}g_1 = h \in H$$

We can run this in reverse to establish equivalence of (2) and (3). We follow that since $g_1 = g_2h$ that $g_1H \cap g_2H \neq \emptyset$, and thus they are equal.

2.5.13

Let G be a finite group whose only subgroups are $\{e\}$ and G . Prove that either $G = \{e\}$ or else that G is a cyclic group whose order is prime.

Set with $G = \{e\}$ is trivial, thus assume that $G \neq \{e\}$. Let $q \in G \neq e$. We follow that since G is finite that q has an order, and thus its powers constitute a subgroup $\langle q \rangle$. Since order of G is a prime we follow that order of $\langle q \rangle$ divides the order of G and thus order of $\langle q \rangle$ is either 1 or order of G . Since $q \neq e$ we conclude the latter, and thus $\langle q \rangle = G$, which implies that G is cyclical, as desired.

2.5.14

Let G be a group, and let $K \subseteq H \subseteq G$ be subgroups. We may thus view K as a subgroup of G or as a subgroup of H . We also recall that the index of a subgroup is its number of distinct cosets.

(a) If G is finite, prove the Index Multiplication Rule:

$$(G : K) = (G : H)(H : K)$$

We follow that

$$|H| = |K|(H : K)$$

$$|G| = |H|(G : H)$$

and

$$|G| = |K|(G : K)$$

therefore

$$|G|/|K| = (G : K)$$

thus

$$|G| = |K|(H : K)(G : H)$$

$$|G|/|K| = (H : K)(G : H)$$

$$|G|/|K| = (G : H)(H : K)$$

$$(G : K) = (G : H)(H : K)$$

as desired.

(b) *Prove that the Index Multiplication Rule is true even if G, H, K are allowed to be infinite groups, provided that we assume that $(G : K)$ is finite*

Let Q' be the set of distinct cosets of H in G . Let W' be the set of distinct cosets of K in H . For each $q' \in Q'$ there's an element q of G such that $qH = q'$. By AoC we can define subset Q of G that correspond to Q' . For each $w' \in W'$ there's an element w of H such that $wK = w'$. By AoC we can define subset W of H that correspond to W' .

Let j be a coset of K in G . We follow that there's $g \in G$ such that $gK = j$. We follow that gH is a coset of H , and thus there's a unique $q \in Q$ such that $qH = gH$. We follow then that $g^{-1}q \in H$ (see a couple of exercises above), and thus $(g^{-1}q)K$ is a coset of K in H . Thus there's a unique $w \in W$ such that

$$wK = (g^{-1}q)K$$

thus

$$qwK = gK$$

therefore for each coset of K in G there's a pair $\langle q, w \rangle \in Q \times W$. By uniqueness of q and w in Q and W , and the fact that j is an arbitrary coset we conclude that there's an injection from a set of cosets of K in G to $Q \times W$.

Let $\langle q_1, w_1 \rangle, \langle q_2, w_2 \rangle \in Q \times W$ are such that $\langle q_1, w_1 \rangle \neq \langle q_2, w_2 \rangle$. We follow that if $q_1 \neq q_2$, and thus $q_1H \neq q_2H$ by definition. $w_1w_2 \in H$, and thus $w_1w_2H = H$. Since $K \subseteq H$ we follow that

$$q_1w_1K \subseteq q_1H$$

$$q_2w_2K \subseteq q_2H$$

and thus

$$q_1w_1K \neq q_2w_2K$$

If $q_1 = q_2$ we follow that $w_1 \neq w_2$. This implies that

$$w_1K \neq w_2K$$

and thus

$$q_1w_1K \neq q_1w_2K$$

and since $q_1 = q_2$ we follow that

$$q_1w_1K \neq q_2w_2K$$

This implies that if $\langle q_1, w_1 \rangle, \langle q_2, w_2 \rangle \in Q \times W$ then $q_1w_1K \neq q_2w_2K$, and thus we conclude that there's an injection from $Q \times W$ to a set of cosets of K . Schroder-Bernstein now implies that the set of cosets of K in G is equal to $|Q \times W|$. If the latter is finite, then we follow

that $(G : K) = |Q| * |W|$. Definition of Q and W respectively imply that $|Q| = (G : H)$ and $|W| = (H : K)$, which implies that

$$(G : K) = (G : H)(H : K)$$

as desired.

2.5.15

Let p be a prime and let $a \in Z$ be an integer satisfying $p \nmid a$. Use Exercise 2.13(b) and Lagrange's theorem to prove

Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$

We follow that if $a \nmid p$, then $a \not\equiv 0 \pmod{p}$. We thus follow that there's $r \in Z_+$ such that $r < p$ and there's an integer k such that $a = kp + r$. This implies that

$$a^n = (kp + r)^n = \sum_{i \in \{0, \dots, n\}} bc(n, i)(kp)^i r^{n-i}$$

by the binomial theorem (bc is the binomial coefficient). We then follow that the only element of the sum that does not have p as its multiple is the one where $i = 0$. Thus we follow that

$$a^n \equiv \sum_{i \in \{0, \dots, n\}} bc(n, i)(kp)^i r^{n-i} \equiv r^n \pmod{p}$$

thus we follow that the original theorem is equivalent to the statement that for all $r \in Z_+$ such that $r < p$ we've got that

$$r^{p-1} \equiv 1 \pmod{p}$$

We know that 1 is the identity in the multiplicative group $(Z/pZ)^*$. We also follow that order of $(Z/pZ)^*$ is $p - 1$. We thus follow that any cyclic subgroup of $(Z/pZ)^*$ has order that divides $p - 1$. Therefore we follow that for each provided r we've got that order of r is some divisor n of $p - 1$, and thus

$$r^{p-1} = r^{n*k} = e^k = e = 1$$

which gives us the desired result.

2.6 Products of groups

2.6.1

Let G_1, G_2, \dots, G_n be groups. Generalize definition 2.54 by explaining why

$$G_1 \times \dots \times G_n$$

with component-wise operation is a group.

We can follow this case by induction. Interesting thing is to ask that if K is an indexed set of groups, then is $\prod K$ a group?

We can follow that the product of identities is an identity. Inverses are also handled. Component-wise association gives us also association for the product group. $\prod K$ is abelian if and only if all the constructing groups are abelian.

2.6.2

Let G be a group, let A and B be subgroups of G and consider the map

$$\phi : A \times B \rightarrow G, \phi(a, b) = ab$$

(a) If G is an abelian group, prove that ϕ is a homomorphism.

Follows from the exercise that we've already finished (there we've handled the specific case that $B \subseteq Z_G(A)$)

(b) If G is an abelian group, prove that

$$\ker(\phi) = \{\langle c, c^{-1} \rangle : c \in A \cap B\}$$

We can follow that application of ϕ to the element of rhs will give us identity by definition, and thus we've got \supseteq .

If $\phi(i, j) = e$, then by definition $ij = e$, and thus $i = j^{-1}$. Thus we've got the \subseteq .

(c) Suppose that there are elements $a \in A$, $b \in B$ such that $ab \neq ba$. Prove that ϕ is not a homeomorphism

Exercise that handled this premise before concludes with biconditional, which gives us this implication

the rest of the exercises are skipped

Chapter 3

Rings - Part 1

3.1 Abstract Rings and Ring Homomorphisms

Notes

Distributive law can be generalized through application of associativity, which will give us

$$a * (b + c + d) = ab + ac + ad$$

and the same for the other direction. We can also by induction do the same with a general sum.

$$b \sum a_i = \sum ba_i$$

The idea of ring homomorphism can be summed up to preserving functions upon application of the function, and mapping identities to identities.

3.1.1

Let R be a ring, and let $a, b \in R$.

(a) Prove that

$$(-a) * (-b) = a * b$$

$$(-a) * (-b) = (0 + (-a)) * (-b) = (a + (-a) + (-a)) * (-b) = a * (-b) + (-a) * (-b) + (-a) * (-b)$$

(we've added 0 to the $-a$ and then distributed over it) thus

$$(-a) * (-b) = a * (-b) + (-a) * (-b) + (-a) * (-b)$$

and cancelation law implies that

$$0 = a * (-b) + (-a) * (-b)$$

this in turn implies that

$$(-(a * (-b))) = (-a) * (-b)$$

we can do a similar thing for $(-b)$, which will result in

$$(-((-a) * b)) = (-a) * (-b)$$

Given that everything has additive inverse, we can follow that

$$a + b = (-((-a) * b)) = -(a * (-b))$$

which will imply that

$$\begin{aligned} (-a)*(-b) &= -(a*(-b)) = -((-(-a))*(-b)) = -((-(-a))*(-b)) = -(-(-(-a))*b) = \\ &= -(-(a * b)) = a * b \end{aligned}$$

as desired.

(b) Our proof of Proposition 3.2(a) used the multiplicative identity element 1_R of R . Find a proof that works even if R does not have a multiplicative identity

We follow that for all $b \in R$

$$ab = a * (b + 0) = ab + a0$$

thus by cancelation law of the group we follow that

$$-(ab) + ab = -(ab) + ab + a0$$

$$0 = 0 + a0$$

$$0 = a0$$

as desired.

3.1.2

Let R be a commutative ring

(a) Suppose that the map

$$f : R \rightarrow R, f(a) = a^2$$

is a ring homomorphism. Prove that $1_R + 1_R = 0_R$.

By definition of ring homeomorphism we follow that

$$1_R = f(1_R)$$

and thus we follow that

$$1_R + 1_R = f(1_R) + f(1_R) = f(1_R + 1_R) = (1_R + 1_R)^2 = (1_R + 1_R)(1_R + 1_R) =$$

$$= 1_R(1_R + 1_R) + 1_R(1_R + 1_R) = (1_R + 1_R) + (1_R + 1_R)$$

thus

$$(1_R + 1_R) = (1_R + 1_R) + (1_R + 1_R)$$

$+$ is a group, thus we're justified to use cancelation to get that

$$1_R + 1_R = 0$$

as desired

(b) Conversely, if $2 = 0$ in the ring R , prove that $f(a)^2$ is a homomorphism from R to R

We follow that

$$0^2 = 0$$

$$1^2 = 1$$

so identities are there.

One thing to point out is that R is commutative, which is used in deriviations here

$$\begin{aligned} f(a+b) &= (a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = \\ &= a^2 + ab + ab + b^2 = f(a) + ab + ab + f(b) = f(a) + f(b) + ab(1+1) = \\ &= f(a) + f(b) + *0 = f(a) + f(b) \end{aligned}$$

thus we've got the addition

$$f(a*b) = (a*b)^2 = (a*b)*(a*b) = a*b*a*b = a^2*b^2 = f(a)*f(b)$$

and multiplication, that now satisfies the definition of the homomorphism.

(c) Suppose that the map

$$f : R \rightarrow R, f(a) = a^3$$

is a ring homomorphism. Prove that $6 = 0$ in the ring R

$$\begin{aligned} f(1+1) &= (1+1)^3 = (1+1)*(1+1)*(1+1) = 8 \\ f(1+1) &= f(1) + f(1) = 1+1 = 2 \end{aligned}$$

thus

$$8 = 2$$

$$6 = 0$$

as desired. In general we follow that if $f(a) = a^n$ is a homomorphism, then $2^n - 2 = 0$

3.2 Interesting Examples of Rings

Notes

When checking for subrings, we follow that associativity of both operations and their distributivity gets grandfathered by the subset, and thus the only things that we need to check for are the identities and closures of operations

When we're using generalized rings with polynomials, it is possible that different lists of coefficients might give the same functions. This is easily observed, when we remember that there exist finite rings, and thus the space of functions from this ring to itself is finite, but the list of possible coefficients is infinite.

When we're talking about polynomial equality, we mean that they've got the same list of coefficients. This essentially means, that a polynomial is practically a list of elements of the ring, and not the function.

It's also important to remember, that coefficients of polynomials are the elements of the underlying ring, but powers are natural numbers by definition.

We can also theoretically have polynomials over polynomials, and so on, and so forth.

In the book, the ring of quaternions is defined over coefficients in R , but the subrings of R can be also used to define appropriate subrings.

Matrix ring is an important example of the fact that two non-zero elements when multiplied can produce a zero.

3.2.1

Let $m \geq 1$ be an integer, and define a map

$$\phi : Z \rightarrow Z/mZ, \phi(a) = a \pmod{m}$$

Prove that ϕ is a ring homomorphism.

We firstly follow that $\phi(0) = 0, \phi(1) = 1$ by definition, and thus identities are mapped properly. Fact that

$$a \equiv c \pmod{m}, b \equiv d \pmod{m} \Rightarrow a + b \equiv c + d \pmod{m}, a * b \equiv c * d \pmod{m}$$

implies that all the function properties are satisfied, and thus ϕ is a homeomorphism, as desired.

3.2.2

(a) Let $\alpha = 7$ and $\beta = 11$ be elements of the ring $Z/17Z$. Compute $\alpha + \beta$ and $\alpha * \beta$.

We follow that

$$7 + 11 = 18 \equiv 1 \pmod{17}$$

$$7 * 11 = 77 \equiv 9 \pmod{17}$$

(b) Let $\alpha = 2 + 4x$ and $\beta = 1 + 4x + 3x^2$ be elements of the ring $(\mathbb{Z}/7\mathbb{Z})[x]$. Compute $\alpha + \beta$ and $\alpha * \beta$.

$$(2 + 4x) + (1 + 4x + 3x^2) = 3 + x + 3x^2$$

$$(2 + 4x) * (1 + 4x + 3x^2) = (2 + 1x + 6x^2) + (4x + 2x^2 + 5x^3) = 2 + 5x + x^2 + 5x^3$$

(c) Let $\alpha = 3 + 2i$ and $\beta = 2 - 3i$ be elements of the ring $\mathbb{Z}[i]$. Compute $\alpha + \beta$ and $\alpha * \beta$.

$$3 + 2i + 2 - 3i = 5 - i$$

$$(3 + 2i) * (2 - 3i) = 6 - 9i + 4i + 6 = 12 - 5i$$

(d) Let $\alpha = 3 + 2x - x^2$ and $\beta = 2 - 3x + x^2$ be elements of the ring $\mathbb{Z}[x]$. Compute $\alpha + \beta$ and $\alpha * \beta$.

$$(3 + 2x - x^2) + (2 - 3x + x^2) = 5 - x$$

$$\begin{aligned} (3 + 2x - x^2) * (2 - 3x + x^2) &= (6 - 9x + 3x^2) + (4x - 6x^2 + 2x^3) + (-2x^2 + 3x^3 - x^4) = \\ &= 6 - 15x - 5x^2 + 5x^3 - x^4 \end{aligned}$$

(e) Let $R = \mathbb{Z}[i]$ and let $\alpha = (1 + i) + (2 - i)x - x^2$ and $\beta = (2 + i) + (1 + 3i)x$ be elements of the ring $\mathbb{Z}[x]$. Compute $\alpha + \beta$ and $\alpha * \beta$.

$$(1 + i) + (2 - i)x - x^2 + (2 + i) + (1 + 3i)x = (2 + 2i) + (3 + 2i)x - x^2$$

$$\begin{aligned} &((1 + i) + (2 - i)x - x^2) * ((2 + i) + (1 + 3i)x) = \\ &= (2 + 2i + i - 1) + (4 - 2i + 2i + 1)x + (-2 - i)x^2 + (1 + i + 3i - 3)x + (2 - i + 6i + 3)x^2 + (-1 - 3i)x^3 = \\ &= (1 + 3i) + 5x + (-2 - i)x^2 + (-2 + 4i)x + (5 + 5i)x^2 + (-1 - 3i)x^3 = \\ &= (1 + 3i) + (3 + 4i)x + (3 + 4i)x^2 + (-1 - 3i)x^3 \end{aligned}$$

(f) Let $\alpha = 1 + 2i - j + k$ and $\beta = 2 - i + 3j - k$ be elements of the ring H . Compute $\alpha + \beta$ and $\alpha * \beta$.

$$1 + 2i - j + k + 2 - i + 3j - k = 3 + i + 2j$$

$$\begin{aligned} &(1 + 2i - j + k) * (2 - i + 3j - k) = \\ &= (2 - i + 3j - k) + 2i(2 - i + 3j - k) - j(2 - i + 3j - k) + k(2 - i + 3j - k) = \\ &= (2 - i + 3j - k) + (4i + 2 + 6k + 2j) - (2j + k - 3 - i) + (2k - j - 3i + 1) = \\ &= (2 - i + 3j - k) + (2 + 4i + 2j + 6k) + (3 + i - 2j - k) + (1 - 3i - j + 2k) = \\ &= 8 + i + 2j + 6k \end{aligned}$$

3.2.3

For any integer D that is not the square root of an integer, we can form a ring

$$Z[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in Z\}$$

If $D > 0$, then $Z[\sqrt{D}]$ is a subring of R , while if $D < 0$, then in any case it is a subring of C .

(a) Let $\alpha = 2 + 3\sqrt{5}$ and let $\beta = 1 - 2\sqrt{5}$. Compute the quantities

$$a + b, a * b, a^2$$

We follow that

$$\begin{aligned} 2 + 3\sqrt{5} + 1 - 2\sqrt{5} &= 3 + \sqrt{5} \\ (2 + 3\sqrt{5}) * (1 - 2\sqrt{5}) &= 2 - 4\sqrt{5} + 3\sqrt{5} - 30 = -28 - \sqrt{5} \\ (2 + 3\sqrt{5})^2 &= 4 + 12\sqrt{5} + 45 = 49 + 12\sqrt{5} \end{aligned}$$

(b) Prove that the map

$$\phi : Z[\sqrt{D}] \rightarrow Z[\sqrt{D}], \phi(a + b\sqrt{D}) = a - b\sqrt{D}$$

is a ring homomorphism.

We follow that identities are golden.

$$\begin{aligned} \phi(a + b\sqrt{D} + c + d\sqrt{D}) &= \phi((a + c) + (b + d)\sqrt{D}) = \\ &= (a + c) - (b + d)\sqrt{D} = a - b\sqrt{D} + c - d\sqrt{D} = \phi(a + b\sqrt{D}) + \phi(c + d\sqrt{D}) \end{aligned}$$

$$\phi((a + b\sqrt{D}) * (c + d\sqrt{D})) = \phi(ac + ad\sqrt{D} + bc\sqrt{D} + bdD) = ac + bdD - ad\sqrt{D} - bc\sqrt{D}$$

$$\begin{aligned} \phi(a + b\sqrt{D}) * \phi(c + d\sqrt{D}) &= (a - b\sqrt{D}) * (c - d\sqrt{D}) = \\ &= ac + bdD - ad\sqrt{D} - bc\sqrt{D} \end{aligned}$$

thus everything checks out, as desired.

(c) Prove that for all $\alpha \in Z[\sqrt{D}]$

$$\alpha * \bar{\alpha} \in Z$$

$$\begin{aligned} \alpha * \bar{\alpha} &= (a + b\sqrt{D}) * (a - b\sqrt{D}) = \\ &= a^2 - ab\sqrt{D} + ab\sqrt{D} + b^2D = a^2 + b^2D \end{aligned}$$

given that a, b, D are integers, we follow the desired conclusion.

3.2.4

Let ρ be the complex number $\rho = \frac{-1+i\sqrt{3}}{2} \in C$, and let

$$Z[\rho] = \{a + b\rho : a, b \in Z\}$$

(a) Prove that $\rho^3 = 1$. Thus ρ is a cube root of unity.

$$\begin{aligned} \left(\frac{-1+i\sqrt{3}}{2}\right)^3 &= \left(\frac{\sqrt{3}}{2}i - \frac{1}{2}\right)^3 = \left(\frac{\sqrt{3}}{2}i\right)^3 - 3\left(\frac{\sqrt{3}}{2}i\right)^2\left(\frac{1}{2}\right) + 3\left(\frac{\sqrt{3}}{2}i\right)\left(\frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^3 = \\ &= -\frac{3\sqrt{3}}{8}i + \frac{9}{8} + \frac{3\sqrt{3}i}{8} - \frac{1}{8} = 1 + 0 = 1 \end{aligned}$$

as desired.

(b) Prove that $\rho^2 + \rho + 1 = 0$

$$\rho^3 - 1 = (\rho - 1)(\rho^2 + \rho + 1)$$

we follow that lhs is not zero, and thus rhs is zero, as desired.

(c) Prove that the polynomial $X^3 - 1$ factors as

$$X^3 - 1 = (X - 1)(X - \rho)(X - \rho^2)$$

We follow that

$$\begin{aligned} (X - \rho)(X - \rho^2) &= X^2 - \rho^2X - \rho X + 1 = X^2 - \rho^2X - \rho X - X + X + 1 = \\ &= X^2 - X(\rho^2X + \rho - 1) + X + 1 = X^2 - 0X + X + 1 = X^2 + X + 1 \end{aligned}$$

thus

$$(X - 1)(X - \rho)(X - \rho^2) = (X - 1)(X^2 + X + 1)$$

and

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

as desired.

(d) Prove that $Z[\rho]$ is a subring of C .

By setting a, b appropriately we get that identities are present. Additive group is closed by general properties of C .

$$\begin{aligned} (a + b\rho) * (c + d\rho) &= ac + ad\rho + bc\rho + bd\rho^2 = ac + ad\rho + bc\rho + bd\rho^2 + bd\rho + bd - bd\rho - bd = \\ &= ac + ad\rho + bc\rho + bd(\rho^2 + \rho + 1) - bd\rho - bd = ac + ad\rho + bc\rho + bd0 - bd\rho - bd = \\ &= (ac - bd) + \rho(ad + bc - bd) \end{aligned}$$

thus this thing is also closed under multiplication, which makes $Z[\rho]$ a subring, as desired.