

My abstract algebra exercises

Evgeny (Gene) Markin

2024

Contents

1	A Potpourri of Preliminary Topics	6
2	Groups - Part 1	7
2.1	Introduction to Groups	7
2.1.1	7
2.1.2	7
2.1.3	7
2.1.4	8
2.2	Abstract Groups	8
2.2.1	8
2.2.2	9
2.2.3	11
2.2.4	11
2.2.5	13
2.3	Interesting Examples of Groups	13
2.3.1	14
2.3.2	15
2.3.3	15
2.3.4	15
2.3.5	15
2.3.6	16
2.3.7	16
2.3.8	17
2.3.9	18
2.3.10	18
2.3.11	19
2.4	Group Homomorphism	19
2.4.1	19
2.4.2	20
2.4.3	20

2.4.4	20
2.4.5	21
2.4.6	22
2.5 Subgroups, Cosets, and Lagrange's Theorem	22
2.5.1	22
2.5.2	23
2.5.3	24
2.5.4	24
2.5.5	25
2.5.6	26
2.5.7	27
2.5.8	27
2.5.9	28
2.5.10	28
2.5.11	30
2.5.12	31
2.5.13	32
2.5.14	32
2.5.15	34
2.6 Products of groups	34
2.6.1	34
2.6.2	35
3 Rings - Part 1	36
3.1 Abstract Rings and Ring Homomorphisms	36
3.1.1	36
3.1.2	37
3.2 Interesting Examples of Rings	39
3.2.1	39
3.2.2	40
3.2.3	41
3.2.4	42
3.2.5	43
3.2.6	43
3.2.7	44
3.2.8	44
3.2.9	44
3.2.10	47
3.2.11	47
3.2.12	48
3.2.13	49

3.2.14	49
3.2.15	50
3.3 Some Important Special Types of Rings	51
3.3.1	51
3.3.2	52
3.3.3	52
3.3.4	52
3.3.5	53
3.3.6	53
3.3.7	53
3.3.8	54
3.3.9	56
3.4 Unit groups and Product rings	56
3.4.1	56
3.4.2	58
3.4.3	58
3.4.4	58
3.4.5	59
3.4.6	59
3.4.7	60
3.4.8	60
3.4.9	62
3.4.10	64
3.5 Ideals and Quotient Rings	64
3.5.1	67
3.5.2	68
3.5.3	68
3.5.4	69
3.5.5	69
3.5.6	70
3.5.7	70
3.5.8	71
3.5.9	72
3.5.10	73
3.5.11	74
3.6 Prime Ideals and Maximal Ideals	74
3.6.1	75
3.6.2	76
3.6.3	76
4 Vector Spaces - Part 1	78

5	Fields - Part 1	79
5.1	Introduction to Fields	79
5.2	Abstract Fields and Homomorphisms	79
5.2.1	79
5.2.2	80
5.3	Interesting Examples of Fields	80
5.3.1	80
5.3.2	80
5.3.3	80
5.3.4	81
5.3.5	83
5.4	Subfield and Extension Fields	84
5.4.1	84
5.4.2	84
5.4.3	85
5.5	Polynomial Rings	86
5.5.1	86
5.5.2	86
5.6	Building Extension Fields	87
5.6.1	88
5.6.2	90
5.6.3	91
5.6.4	93
5.7	Finite Fields	93
5.7.1	93
5.7.2	94

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.

Since it's an algebra book, and algebra has rings, that are denoted by R , and those are used in similar context with reals, that are also denoted by me by R , we can see that there's a need to differentiate between the two. Thus approximately halfway through the chapter about rings I've started using \mathbb{R} for reals.

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:

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

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 are not 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 first 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

$$bh = hb$$

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

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

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

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

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 finite list of elements of the ring (and thus the set of all polynomials is a set of all finite lists of coefficients), 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.

Although we haven't observed any product rings (i.e. rings that are made up by sticking two rings into cartesian product), it's pretty obvious that we can define them and everything will line up

We can rephrase the condition of uniqueness of homomorphism from \mathbb{Z} : if f and g are homomorphisms from \mathbb{Z} to some ring R , then $f = g$.

3.2.1

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

$$\phi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, \phi(a) = a \mod m$$

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

$$a \equiv c \mod m, b \equiv d \mod m \Rightarrow a + b \equiv c + d \mod m, a * b \equiv c * d \mod m$$

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 $\mathbb{Z}/17\mathbb{Z}$. 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.

3.2.5

This one is reasoned in the notes, and is a bunch of arithmetic

3.2.6

Let R be commutative ring, let $c \in R$, and let $E_c : R[x] \rightarrow R$ be evaluation map $E_c(f) = f(c)$.

(a) Prove that E_c is a ring homomorphism.

We follow that there's a polynomial $x - c$ and $x - c + 1$ that maps identities. We follow that

$$\begin{aligned} E_c(f + g) &= (f + g)(c) = f(c) + g(c) = E_c(f) + E_c(g) \\ E_c(f * g) &= (f * g)(c) = f(c) * g(c) = E_c(f) * E_c(g) \end{aligned}$$

by algebraic properties of functions.

(b) Prove that $E_c(f) = 0$ if and only if there's a polynomial $g(x) \in R[x]$ satisfying $f(x) = (x - c)g(x)$

$$f(x) = f(x) - 0 = f(x) - f(c) = \sum a_i(x^j - c^j)$$

We know that

$$x^n - c^n = (x - c) \sum_{i=1}^n x^{n-i} c^{i-1}$$

Which gives us the desired result (needed to look this one up). Reverse is trivial

3.2.7

Let R be a non-commutative ring, with elements $\alpha, \beta \in R$ such that $\alpha \neq \beta$. We can still turn $R[x]$ into a ring by always writing polynomials in the form

$$p(x) = \sum a_i x^i$$

and using the usual rule that x commutes with all of the elements of R . We can also define an evaluation map $E_\alpha : R[x] \rightarrow R$ by setting

$$E_\alpha(\sum a_i x^i) = \sum a_i \alpha^i$$

Prove that if R is non-commutative, then E_α is not a homomorphism.

We follow that

$$E_\alpha(0) = 0$$

$$E_\alpha(1) = 1$$

thus we've got identities, and so there's nothing there.

We know that both α and β are polynomials, but

$$E_\alpha(x * \beta) = E_\alpha(\beta x) = \beta \alpha$$

$$E_\alpha(x) * E_\alpha(\beta) = \alpha * \beta$$

which implies that $E_\alpha(x) * E_\alpha(\beta) \neq E_\alpha(x * \beta)$, which in turn implies that E_α is not a homomorphism, as desired.

3.2.8

Skip

3.2.9

For any commutative ring R , let

$$M_2(R) = \left\{ \begin{pmatrix} a & d \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$$

be the set of 2-by-2 matrices with entries in R . Define addition and multiplication in an obvious way

(a) Prove that $M_2(R)$ is a ring.

Additive identity is the matrix with zeros in it. Multiplicative identity is the one with multiplicative identities on the diagonal, and the rest being zeroes.

Properties that this thing is an abelian group under addition are following from the fact that R is an abelian group.

Closure under multiplication is derived from the definition of multiplication. Derivations of associativity and distributivity take a lot of paper, but are pretty uneventful.

(b) *Prove that $M_2(R)$ is non-commutative*

This is where our assumptions that $0 \neq 1$ are kicking in: if a trivial ring is a singleton, then this thing is commutative. But we don't assume that, and thus

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

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

which given that $1 \neq 0$ implies the desired result.

(c) *Find non-zero elements $A, B \in M_2(R)$ such that $AB = 0$*

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

as desired.

(d) *Let $A \in M_2(R)$. Prove that there's $B \in M_2(R)$ satisfying $AB = I$ if and only if $ad - bc$ has a multiplicative inverse in R .*

Let's start with the forward direction, and assume the appropriate things. We're gonna implicitly derive the determinant here. We follow that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} pa + rb & qa + sb \\ pc + rd & qc + sd \end{pmatrix} = I$$

thus we follow that

$$\begin{cases} pa + rb = qc + sd = 1 \\ qa + sb = pc + rd = 0 \end{cases}$$

thus

$$\begin{cases} (pa + rb) * (qc + sd) = 1 \\ (qa + sb) * (pc + rd) = 0 \end{cases}$$

$$\begin{cases} paqc + pasd + rbqc + rbsd = 1 \\ qapc + qard + sbpc + sbrd = 0 \end{cases}$$

$$\begin{cases} paqc + pasd + rbqc + rbsd = 1 \\ paqc + qard + sbpc + rbsd = 0 \end{cases}$$

thus

$$paqc + pasd + rbqc + rbsd - (paqc + qard + sbpc + rbsd) = 1$$

$$pasd + rbqc - (qard + sbpc) = 1$$

$$psad + rqb - rqad - psbc = 1$$

$$ps(ad - bc) + rq(bc - ad) = 1$$

$$ps(ad - bc) - rq(ad - bc) = 1$$

$$(ps - rq)(ad - bc) = 1$$

which implies that there's $ps - rq \in R$ that is a multiplicative inverse of $(ad - bc)$, as desired.

Assume that $ad - bc$ has a multiplicative inverse. The following is just a simple formula for computing inverse of the matrix in R^2 . We follow that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} da - cb & -ba + ba \\ -dc + cd & -bc + ad \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix}$$

We then follow that if we would've changed every entry e in the right matrix for $e/(ad - bc)$, then we would've gotten identity as the result. Thus we conclude that there's a matrix B such that $AB = I$, as desired

(e) Let $A, B \in M_2(R)$. Prove that $AB = I$ if and only if $BA = I$

Given previous point and lots of notation, we can conclude the desired result.

(f) More generally, prove all of the above for $M_n(R)$ for $n \geq 2$.

I'm not gonna prove this thing rigorously, but I'll outline a proof because of the fact that most of it is tedious and not particularly interesting.

When it comes to a ring, we get group properties for free, closure of multiplication is somewhat trivial. Distributivity can be handled piecewise: for $(A + B) * C$ let $q_{i,j}$ be some entry in the resulting matrix

$$q_{i,j} = \sum_{k=1}^n (a_{i,k} + b_{i,k})c_{k,j} = \sum_{k=1}^n c_{k,j}a_{i,k} + \sum_{k=1}^n c_{k,j}b_{i,k}$$

and through lots of notation we can follow the rest pretty easily, thus making $M_n(R)$ a ring.

By putting our original matrix for $M_2(R)$ into the upper left corner of the matrix we get non-commutativity.

Proof that $AA^{adj} = (\det A)I$ is heavily dependent on what we choose to be the definition of the determinant. If we start with the Laplace's formula as the definition of the determinant, we can follow that matrices with identical rows/columns are zero, and thus everything that is not on diagonal is zero. We would then follow that diagonals are determinants by definition, and thus we get desired result.

$AA^{adj} = (\det A)I$ implies that if $(\det A)$ has a multiplicative inverse in R , then we would get that $(\det A)A^{adj}$ is an inverse of A (we would need to weave through or define

scalar multiplication for matrices), which gives the desired result. Proof that invertible A commutes with A^{-1} can be shown piecewise.

One important point to note is that here we don't get any benefits for going through determinant to define such things. We would get practically the same results, if we would've gone through the usual definitions of linear transformations and whatnot.

3.2.10

Let R_1 and R_2 be commutative rings, and let $\phi : R_1 \rightarrow R_2$ be homomorphism. We define a map $\Phi : R_1[x] \rightarrow R_2[x]$ by

$$\Phi(\sum a_i x^i) = \sum \phi(a_i) x^i$$

(a) Prove that Φ is a ring homomorphism.

We get identities by the fact that ϕ is a homomorphism. We follow that

$$\begin{aligned} \Phi(\sum a_i x^i) + \Phi(\sum b_i x^i) &= \sum \phi(a_i) x^i + \sum \phi(b_i) x^i = \\ &= \sum \phi(a_i) x^i + \phi(b_i) x^i = \sum (\phi(a_i) + \phi(b_i)) x^i = \\ &= \sum (\phi(a_i + b_i)) x^i = \sum (\phi(a_i + b_i) x^i) = \Phi(\sum (a_i + b_i) x^i) = \Phi(\sum a_i x^i + \sum b_i x^i) \end{aligned}$$

$$\begin{aligned} \Phi(\sum a_i x^i) \cdot \Phi(\sum b_j x^j) &= (\sum \phi(a_i) x^i) * (\sum \phi(b_j) x^j) = \sum \sum \phi(a_i) \phi(b_j) x^{i+j} = \\ &= \sum \sum \phi(a_i b_j) x^{i+j} = \Phi(\sum \sum a_i b_j x^{i+j}) = \Phi((\sum a_i x^i) * (\sum b_j x^j)) \end{aligned}$$

as desired.

(b) If ϕ is a ring isomorphism, prove that Φ is a ring isomorphism

$R_1[x]$ is a polynomial, which by definition is the list. There's a general theorem (if not proven explicitly, then derived pretty easily), that piecewise application of a bijection on elements of a given list gives us a bijection. This implies that if ϕ is a bijection, then Φ is a bijection, which given homomorphism implies isomorphism, as desired.

3.2.11

Lots of notation, but the essence boils down to the fact that we can define $R[x,y]$ - a set of polynomials with two variables. All the things that concern evaluation and whatnot are essentially the same in regards to this version. We can also define such a thing for a polynomial in an arbitrary number of variables.

3.2.12

Let $R[x, y]$ be the ring of polynomials in two variables with coefficients in R , as described in Exercise 3.13. In this exercise we will look at polynomials that don't change if we swap x and y . For example, the polynomials

$$x + y, xy, x^2 + y^2$$

are invariant under $x \Leftrightarrow y$ swap. We observe that our third example can be expressed using the first two examples,

$$x^2 + y^2 = (x + y)^2 - 2xy$$

In other words, if we let $g_2(u, v) = u^2 - 2v$, then $x^2 + y^2 = g_2(x + y, xy)$

(a) Do the same for $x^3 + y^3$ and $x^4 + y^4$

We follow that generally speaking there's a binomial expansion

$$(x + y)^n = \sum_{i=0}^n bc(i, n) x^i y^{n-i}$$

from which we follow that

$$(x + y)^n = \sum_{i=1}^{n-1} bc(i, n) x^i y^{n-i} + x^n + y^n$$

which implies that

$$\begin{aligned} x^n + y^n &= (x + y)^n - \sum_{i=1}^{n-1} bc(i, n) x^i y^{n-i} = (x + y)^n - xy \sum_{i=1}^{n-1} bc(i, n) x^{i-1} y^{n-i-1} = \\ &= (x + y)^n - xy \sum_{i=0}^{n-2} bc(i, n) x^i y^{n-i} \end{aligned}$$

Let us look at the problem at hand:

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 = x^3 + y^3 + 3xy(x + y)$$

We follow that for $n = 3$ we've got that

$$\sum_{i=1}^{n-1} bc(n, i) x^i = 3x^2y + 3xy^2 = 3xy(x + y)$$

thus $\sum_{i=1}^{n-1} bc(n, i) x^i = g(x + y, xy)$ for $n = 3$. Assume that for all j such that $j < n$ we've got that $\sum_{i=1}^{j-1} bc(j, i) x^i = g(x + y, xy)$ we then follow that for arbitrary n

$$\sum_{i=1}^{n-1} bc(i, n) x^i y^{n-i} = xy \sum_{i=1}^{n-1} bc(i, n) x^{i-1} y^{n-i-1} =$$

$$= xy \sum_{i=0}^{n-2} bc(i, n) x^i y^{n-i} = xy * g(x + y, xy)$$

thus we follow that we've got the inductive step, and thus for all $n \geq 3$ we've got the IH. This implies that for all $n \geq 3$

$$x^n + y^n = (x + y)^n - \sum_{i=1}^{n-1} bc(i, n) x^i y^{n-i} = (x + y)^n - g(x + y, xy) = g'(x + y, xy)$$

as desired.

(b) *Handled in the previous point.*

(c) *Even more generally, suppose that $f(x, y) \in R[x, y]$ is any polynomial with the symmetry property*

$$f(x, y) = f(y, x)$$

Prove that there's a polynomial g such that

$$f(x, y) = g(x + y, xy)$$

If $f(x, y) = f(y, x)$, then we follow that for every element of the sum $a_i x^i y^j$ there's an element $a_i x^j y^i$. This implies that $f(x, y)$ can be partitioned into pairs $a_i x^i y^j + a_i x^j y^i$. This implies that for each such pair we can take

$$a_i x^i y^j + a_i x^j y^i = a x^{j-i} y^{j-i} (x^i + y^i)$$

latter part $(x^i + y^i)$ of this product is a polynomial of form $g(x + y, xy)$ by the previous point, which in turn implies that the whole polynomial is a sum of polynomials in form $g(x + y, xy)$, which is itself a polynomial in form $g(x + y, xy)$, which implies the desired conclusion.

3.2.13

I've practically done this one before in the real analysis course. There might be some deviations, but I'm pretty sure that they are minor. If it isn't the case, then skip.

3.2.14

For a quaternion $\alpha = a + bi + cj + dk \in H$, let $\bar{\alpha} = a - bi - cj - dk$.

(a) Prove that $\alpha \bar{\alpha} \in \mathbb{R}$.

$$\begin{aligned} & (a + bi + cj + dk) * (a - bi - cj - dk) = \\ &= a^2 - abi - acj - adk + abi + b^2 - bicj - bidk + acj - cjb i + c^2 - cjdk + adk - dkbi - dk c j + d^2 = \\ &= a^2 - abi - acj - adk + abi + b^2 - bck + bdj + acj + bck + c^2 - cdi + adk - bdj + cdi + d^2 = \end{aligned}$$

$$= a^2 + b^2 + c^2 + d^2 \in R$$

as desired.

(b) Prove that $\alpha\bar{\alpha} = 0$ if and only if $\alpha = 0$

Follows from the fact that $a^2 + b^2 + c^2 + d^2 = 0 \Leftrightarrow a = b = c = d = 0$ for any elements of \mathbb{R}

(c) Suppose that $\alpha, \beta \in H$ and that $\alpha\beta = 0$. Prove that either $\alpha = 0$ or $\beta = 0$.

Assume that $\alpha \neq 0$. We follow that there's $q \in \mathbb{R}$ such that $\alpha\bar{\alpha} = q = a^2 + b^2 + c^2 + d^2$. We then follow that

$$\bar{\alpha} * \frac{1}{q}$$

is a multiplicative inverses of α . This in turn implies that

$$\alpha^{-1}\alpha\beta = \alpha^{-1}0$$

$$1\beta = 0$$

$$\beta = 0$$

Same idea applies to β , but from the different side, which implies the desired result.

(d) Let $\alpha, \beta \in H$. Prove that

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$$

and

$$\overline{\alpha * \beta} = \bar{\alpha} * \bar{\beta},$$

$$\begin{aligned}\bar{\alpha} + \bar{\beta} &= (a - bi - cj - dk) + (a' - b'i - c'j - d'k) = \\ &= (a + a') - (b + b')i - (c + c')j - (d + d')k = \overline{\alpha + \beta}\end{aligned}$$

by distributivity and whatnot. Multiplicity is proven in the same way, but it's more tedious.

(e) Let $\alpha \neq 0$. Prove that there's $\beta \in H$ such that $\alpha\beta = \beta\alpha = 1$

handled in point (c)

3.2.15

let R be a possibly non-commutative ring. The **center** of R consists of the elements of R that commute with every other element of R .

$$R^{\text{center}} = \{a \in R : \alpha\beta = \beta\alpha \text{ for every } \beta \in R\}$$

(a) Prove that R^{center} is a commutative subring of R

Proof goes along the same way as the center of group.

(b) What is the center of the ring of quaternions H ?

We follow that every real entry is commutative.

$$(a + bi + cj + dk) * k = ak + bik + cjk + dk^2 = ak - bj + ci - d$$

$$k * (a + bi + cj + dk) = ak + bki + ckj + dk^2 = ak + bj - ci - d$$

this implies that $(a + bi + cj + dk)$ is not commutative with k if $b \neq 0$ and $c \neq 0$. Multiplying with j will give the same result, but for c and k , which in sum implies that only reals are in the center.

Skipped the rest

3.3 Some Important Special Types of Rings

Notes

Important note: definition of the field requires a commutative ring. Thus we can follow that field is a couple of abelian groups, that are stich together, have distributivity, and thus one of them is not defined over anothers identity.

For cancelation property we require we require biconditional for some reason, but $b = c$ or $a = 0$ implies that $ab = ac$ for any given ring, and thus I'm assumning that there's a typo there (in the text of the theorem we even see the word "implication")

3.3.1

Let m be a positive integet.

(a) Prove that Z/mZ is an integral domain if and only if m is a prime

Suppose that Z/mZ is an ingeral domain. Assume that it's not a prime. if $m = 1$, then this thing is trivial, and thus assume that $m > 1$. This implies that there's a divisor n of m that is less than m . We follow that m/n is a nonzero element of Z/mZ , and thus

$$n * (m/n) = m = 0$$

which implies that Z/mZ is not an integral domain, which is a contradiction.

Suppose that m is a prime. We follow that $(Z/mZ)^*$ is a group under multiplication, and thus product of two nonzeroes is closed there, and thus is nonzero. This implies that Z/mZ is an integral domain, as desired.

(b) Prove that Z/mZ is a field if and only if m is a prime

If Z/mZ is a field, then it's an integral domain, and thus m is a prime. Implications from the fact that $(Z/mZ)^*$ is a group give us the fact that all non-zeroes got inverses, and thus Z/mZ is a field, as desired.

3.3.2

Let R be a field. Prove that R is an integral domain.

Suppose that R is a field, but not integral domain. The fact that it's not an integral domain implies that there are nonzero $\alpha, \beta \in R$ such that

$$\alpha\beta = 0$$

the fact that α is a nonzero in a field implies that there exists α^{-1} . This implies that

$$\alpha^{-1}\alpha\beta = \alpha^{-1}0$$

$$\beta = 0$$

which is a contradiction.

3.3.3

Prove that each of the following rings is not a field

(a) $\mathbb{Z}[i]$

We follow that $2 * (a + bi) = 2a + 2bi$, where the latter part is not identity.

(b) $\mathbb{R}[x]$

We follow that $x * 1 = x$ and $x * \sum a_i x^i = \sum a_i x^{i+1}$, which implies the desired.

(c) H

This one took me by surprise a bit, but it's important to note that H **has inverses**, but since it's not multiplicative, we follow that it's not a field. Same is true for the next point, but it is also not an integral domain.

3.3.4

Let R be a commutative ring. Prove that R is an integral domain if and only if it's got cancellation property.

Let R be an integral domain. Let $a, b, c \in R$ be such that $ab = ac$ and $a \neq 0$.

$$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0$$

Given that $a \neq 0$ we follow that there are no nonzero elements q of R such that $aq = 0$, and thus we conclude that

$$b - c = 0$$

which implies the desired result. Given that every implication here is biconditional, we get the reverse case for free.

3.3.5

Let R be a finite integral domain. Prove that R is a field.

Let R be a finite integral domain, and let $a \in R \neq 0$. We follow that if $ab = ac$, then $b = c$, which implies that multiplication by a is an injection. Given that R is finite and multiplication by a is a function with domain equal to its codomain, we follow that multiplication by a is a bijection, and thus there's $b \in R$ such that $a * b = 1$, which implies that R is a field, as desired.

3.3.6

This one is a lot of notation, but not a lot of substance

3.3.7

Let R be a commutative ring. The degree of a non-zero polynomial $f(x) \in R[x]$ is the highest power of x that appears in $f(x)$.

(a) Prove that for all $f(x), g(x) \in R[x]$ we have

$$\deg(f(x) + g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$$

We know that sum of polynomials is the piecewise addition of the coefficients, that correspond to each degree, thus implying that the desired result

(b) If $\deg(f) \neq \deg(g)$, prove that the previous equation is an equality

Once again, follows directly from the definition

(c) Suppose that R is an integral domain. Prove that for all non-zero $f(x), g(x) \in R[x]$ we have

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

We follow that the largest powers of $f(x)$ and $g(x)$ are in the form $a_i x^i$ and $b_j x^j$, and thus the largest power of the product is

$$a_i x^i b_j x^j = (a_i b_j) x^{i+j}$$

the fact that R is an integral domain implies that $a_i b_j$ is not zero, thus implying the desired result.

(d) Let $R = \mathbb{Z}/6\mathbb{Z}$. Find polynomials $f(x), g(x) \in R[x]$ with $\deg(f) = \deg(g) = 1$ such that previous equality does not hold.

We follow that

$$3x * 2x = 6x = 0x = 0$$

as desired.

3.3.8

Let R be a commutative ring.

(a) Prove that there's exactly one integral domain R such that the map

$$f : R \rightarrow R, f(a) = a^6$$

is a ring homomorphism.

Firstly, we want to state what exactly what "exactly one integral domain" mean. We want to follow that firstly there exists an integral domain such that all the rules apply, and that if there's another ring that that satisfies those conditions, then it's isomorphic to the ring, that we've made firstly.

We know that if there's a ring homomorphism from $f(a) = a^n$, then $2^n - 2 = 0$ (from the second exercise in this chapter). In this case we've got $62 = 0$. It is important to note that this statement is an implication, and not a biconditional.

We know that prime decomposition of 62 is

$$62 = 31 * 2$$

With $Z/2Z$ we follow that f is an identity ($f(0) = 0^6 = 0$, $f(1) = 1^6 = 1$), and this thing is a ring homomorphism. We also follow that $Z/2Z$ is a field, and thus an integral domain. Thus we follow that there's a ring such that f is a homomorphism (and isomorphism also).

With $Z/3Z$ we follow that $f(0) = 0$, $f(1) = 1$, $f(2) = 1$, which implies that

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

$$f(2 + 1) = f(3) = 0$$

which means that $Z/3Z$ does not satisfy the conditions.

For multiplication we follow that

$$f(a * b) = (ab)^6 = a^6 b^6 = f(a) * f(b)$$

which is true for all commutative rings. Identities are also pretty trivial.

Addition is a bit more interesting:

$$f(a + b) = (a + b)^6 = \sum bc(n, i) a^n b^{n-i}$$

$$f(a) + f(b) = a^6 + b^6$$

thus we need

$$\sum_{i=1}^{n-1} bc(n, i) a^n b^{n-i} = 0$$

list of binomial coefficients in this case is

$$6, 15, 20, 15, 6$$

$$(a + b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$$

We can also follow that

$$\sum_{i=1}^{n-1} bc(n, i)a^n b^{n-i} = ab \sum_{i=1}^{n-1} bc(n, i)a^{n-1} b^{n-i-2}$$

We'll then follow that both a, b are nonzero, then ab is also nonzero, and thus

$$\sum_{i=1}^{n-1} bc(n, i)a^{n-1} b^{n-i-2}$$

must be zero. We then follow that none of the products of powers of a and b are zeroes. We then can also follow that

We follow that

$$f(1 + 1) = 2^6 = f(1) + f(1) = 2$$

thus

$$2^6 = 2$$

we then follow by induction that

$$a^6 = a$$

thus by cancellation property $a^5 = 1$ or $a = 0$.

Suppose that there's a ring, that's got distinct elements $0, 1, k$. We follow that

$$f(k + 1) = (k + 1)^6$$

$$f(k) + f(1) = f(k) + 1 = k^6 + 1$$

Let's start over:

Let $0, 1, k$ be all distinct items of R . We follow that

$$f(k) + f(1) = k^6 + 1$$

$$\begin{aligned} f(k + 1) + f(k - 1) + f(1 - k) &= f(k) + f(1) + f(k) + f(-1) + f(k) + f(-1) = \\ &= k^6 + 1 + k^6 + 1 + k^6 + 1 = 3k^6 + 3 \end{aligned}$$

$$f(k+1+k-1+1-k) = f(k+1) = k^6 + 1$$

thus we follow that

$$\begin{aligned} 3k^6 + 3 &= k^6 + 1 \\ 3(k^6 + 1) &= k^6 + 1 \end{aligned}$$

thus

$$3 = 1$$

3.3.9

Let R be a ring. We define three properties that an element $a \in R$ may possess.

a is nilpotent if $a^n = 0$ for some $n \geq 1$.

a is unipotent if $a - 1$ is nilpotent

a is idempotent if $a^2 = a$.

(a) If R is an integral domain, describe all of the nilpotent, unipotent, and idempotent elements of R .

We follow that if $a^n = 0$, then $a = 0$ by cancellation property, which implies that there's one nilpotent element.

If $a - 1$ is nilpotent, then $(a - 1)^n = 0$, thus $(a - 1) = 0$, and therefore $a = 1$.

If a is idempotent, then $a^2 = a$, thus $a = 0$ or $a = 1$ by cancellation property.

(b) Let $p \in \mathbb{Z}$ be a prime and let $k \geq 1$. Describe all of the nilpotent elements in $\mathbb{Z}/p^k\mathbb{Z}$.
Skipped the rest of the exercises for later.

3.4 Unit groups and Product rings

3.4.1

(a) Compute the unit group \mathbb{Z}^*

We follow that anything times zero is zero, so it's out of the question for all the subsequent things.

We know that $-1, 1$ have themselves as inverses, and any other number fails to have one.

(b) Compute the unit group \mathbb{Q}^*

All of the \mathbb{Q}^* is the unit group.

(c) Compute the unit group $\mathbb{Z}[i]^*$

We follow that $-1, 1$ are in the unit group. $i^4 = 1$, and thus $i, -i$ are also in the group. Thus we follow that for the more general case

$$a + bi$$

that if one of the numbers a, b are equal to 1, while the other is zero, we've got it in the unit group. If $a = b = 1$, then we're out of luck though.

We know that

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

and thus in order to $a + bi$ to be in $Z[i]$ we need both $\frac{a}{a^2 + b^2}$ and $\frac{b}{a^2 + b^2}$ to be integers. We follow that

$$|a| \leq a^2 \leq a^2 + b^2$$

and for $a \notin \{-1, 0, 1\}$ we follow that

$$|a| < a^2 \leq a^2 + b^2$$

which implies that there for the case $a \notin \{-1, 0, 1\}$ there are no inverses for $a + bi$. We've got the same conclusions for b , and thus we conclude that $\{1, -1, i, -i\}$ is the unit group (which seems to be pretty straightforward).

(d) Consider the ring $Z[\sqrt{2}]$. Prove that $1 + \sqrt{2} \in Z[\sqrt{2}]^*$. Prove that the powers of $1 + \sqrt{2}$ are all different, and use that fact to deduce that $Z[\sqrt{2}]$ has infinitely many elements.

We follow that

$$\frac{1}{1 + \sqrt{2}} = \frac{(1 - \sqrt{2})}{(1 - \sqrt{2})(1 + \sqrt{2})} = \frac{(1 - \sqrt{2})}{1 - 2} = -(1 - \sqrt{2}) = -1 + \sqrt{2}$$

by pretty much same derivation we can follow that $(1 + \sqrt{2})^n$ (and by extension $(1 - \sqrt{2})^n$) are in $Z[\sqrt{2}]^*$. We follow that power function is strictly increasing, and thus $(1 + \sqrt{2})^n$ are all different for all $n \in \omega$, and thus $Z[\sqrt{2}]^*$ has infinite amount of elements.

(e) Prove that $\mathbb{R}[x]^* = \mathbb{R}^*$

We follow that by multiplying any nonzero polynomial in \mathbb{R} by other polynomial nonzero we get only polynomials of equal or greater degree, and thus follow that the only one order of polynomial that has an option of having multiplicative inverses is the polynomial of degree 1.

(f) Prove that $1 + 2x$ is a unit in the ring $(Z/4Z)[x]$

$$1 + 2 * 0 = 1$$

$$1 + 2 * 1 = 3$$

$$1 + 2 * 2 = 1$$

$$1 + 2 * 3 = 3$$

we then follow that in order to be constant, elements that result in 3 should be, when multiplied, be equal to 1. We follow that $3 * 3 = 1$ in this case, and thus we follow that

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

which implies that $1 + 2x$ has itself for an inverse, as desired

Maybe I'll tackle the last one later

3.4.2

(a) Let R be commutative ring, and suppose that its unit group R^* is finite with $|R^*| = n$. Prove that every element of $a \in R^*$ satisfies

$$a^n = 1$$

We follow that since R^* is finite that a has an order k . This order k divides order of the group n , and thus

$$a^n = a^{k*j} = 1^j = 1$$

as desired.

(b) - already taken care of in previous exercises

3.4.3

(a) Compute the unit group $(\mathbb{Z}/p\mathbb{Z})^*$ for each of the primes 7, 11, 13. Which ones are cyclic?

Since they are all primes, we follow that groups are exactly $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.

In $(\mathbb{Z}/7\mathbb{Z})^*$ we follow that order of 3 is 6. In $(\mathbb{Z}/11\mathbb{Z})^*$ we follow that order of 2 is 10. For 13 we've got that 2 has order 12.

(b) Compute the unit group $(\mathbb{Z}/m\mathbb{Z})^*$ for each of the composite numbers $m = 8, 9, 15$. Which ones are cyclic?

We follow that

$$(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$$

we then follow that $3^2 = 5^2 = 7^2 = 1$, and thus none of them are cyclic.

We follow that

$$(\mathbb{Z}/9\mathbb{Z})^* = \{1, 2, 4, 5, 7, 8\}$$

Order of 2 is 6, which means that this thing is cyclic.

We follow that

$$(\mathbb{Z}/15\mathbb{Z})^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

Orders of those elements get up to 4, so this group is not cyclic.

3.4.4

Let R_1, \dots, R_n be rings.

(a) Prove that the product $R_1 \times \dots \times R_n$ is a ring.

Follows directly from piecewise application of standard rules of the respective rings.

(b) Yeah, projection is a homomorphism

Skip the rest

3.4.5

Prove that the product ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}/6\mathbb{Z}$ by writing down an explicit isomorphism $\mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Let f be a presumed isomorphism between the rings. We follow that

$$0 \rightarrow (0, 0)$$

$$1 \rightarrow (1, 1)$$

by properties of homomorphism. The fact that $\mathbb{Z}/6\mathbb{Z}$ is cyclic and generated by 1 gives us an idea on how to proceed:

$$2 \rightarrow (0, 2)$$

$$3 \rightarrow (1, 0)$$

$$4 \rightarrow (0, 1)$$

$$5 \rightarrow (1, 2)$$

From this we can follow that the first index of value of our function in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is 0 on even numbers and 1 on odd, which kinda gives us an idea that it might have to do something with % operation. Same goes for the latter index, which gives us an explicit definition.

$$f(x) = (x \% 2, x \% 3)$$

Explicit enumeration here gives us the proof that the function is a bijection. Properties of homomorphism can be followed by either explicit enumeration, of perhaps operations are transferred by % function.

3.4.6

Let R be a non-commutative ring. The group of units of R is

$$R^* = \{a \in R : \exists b, c \in R : ab = ca = 1\}$$

(a) *If $ab = ca = 1$, prove that $b = c$.*

We follow that

$$b = eb = cab = ce = c$$

(b) *Prove that R^* is a group, where we use multiplication for the group law.*

Identity is an inverse for itself, and hence is present in the thing. Associativity is taken care of by the properties of the ring, and thus we need only to handle the closure on inverses. Let $a \in R^*$. We follow that there are $b, c \in R$ such that

$$ab = ca = 1$$

Previous point implies that $b = c$, and thus

$$ab = ba = 1$$

and thus we conclude that b is the inverse of a . By the same point we follow that $b \in R^*$, and thus we conclude that $a \in R^* \Rightarrow a^{-1} \in R^*$, as desired.

3.4.7

Skip

3.4.8

Let R be a ring. e is idempotent if $e^2 = e$.

Errata shows that there's an error in this exercise, either R should be commutative, or e should be in the center.

(a) Let $e \in R$ be idempotent. Prove that $1 - e$ is idempotent and that the product of e and $1 - e$ is 0.

We follow that

$$(1 - e)^2 = (1 - e)(1 - e) = 1 * 1 - 1 * e - e * 1 + e * e = 1 - e - e + e = 1 - e$$

thus $1 - e$ is idempotent by definition.

We follow that

$$(1 - e)e = e - e * e = e - e = 0$$

once again by definitions.

(b) Let $e \in R$ be idempotent with $e \neq 0$. Prove that we can turn $eR = \{ea : a \in R\}$ into a ring by treating e as the multiplicative identity.

We follow that $0 \in eR$, $a \in R \Rightarrow -a \in R$, and thus $ea \in eR \Rightarrow -ea \in eR$, thus we've got inverses, and associativity and commutativity is handled by properties of R , thus making R into an abelian group under $+$.

Let $q \in eR$. We follow that there's $a \in R$ such that $q = ea$, and thus $eq = eea = ea = q$, thus making e into an identity over R . Since $1 \in R$, we follow also that $e \in eR$. Associativity and distributivity over eR is inherited by R , and thus we conclude that eR is indeed a ring, as desired.

(c) Let $e \in R$ be idempotent with $e \neq 0, e \neq 1$. Prove that the map

$$R \rightarrow eR \times (1 - e)R$$

$$a \rightarrow (ea, (1 - e)a)$$

is a ring isomorphism.

Under assumption that R is commutative we follow that

$$e(a + b) = ea + eb$$

$$e(a * b) = e * e * a * b = e * a * e * b$$

for any idempotent e , which implies that given function is a product of homomorphisms, which means that the whole thing is a homomorphism.

Let $a, b \in R$ be arbitrary. If $f(a) = f(b)$ we follow that $ea = eb$ and $(1 - e)a = (1 - e)b$. Since $ea = eb$ we follow that

$$(1 - e)a = (1 - e)b$$

$$b - ea = a - eb$$

$$b - ea = a - ea$$

$$b = a$$

which gives us an implication $f(a) = f(b) \Rightarrow a = b$, which implies that f is injective.

Let $q \in eR \times (1 - e)R$. We follow that there are $a, b \in R$ such that

$$q = (ea, (1 - e)b)$$

We follow that

$$f(ea) = (eea, (1 - e)ea) = (ea, 0a) = (ea, 0)$$

$$f((1 - e)b) = (e(1 - e)b, (1 - e)(1 - e)b) = (0b, b) = (0, b)$$

and thus

$$f(ea + (1 - e)b) = f(ea) + f((1 - e)b) = (ea, 0) + (0, (1 - e)b) = (ea, (1 - e)b) = q$$

by homomorphisms and whatnot, which implies that for arbitrary q there's an elements of R that is mapped into q , which means that f is surjective, which gives us isomorphism, as desired.

(d) Let R_1, R_2 be rings. Find idempotents $e_1, e_2 \in R_1 \times R_2$ that also satisfy $e_1 e_2 = 0$. Prove that if $\alpha \in R_1 \times R_2$, then there are unique elements $a_1 \in R_1$ and $a_2 \in R_2$ such that $\alpha = a_1 e_1 + a_2 e_2$.

There's no typo, TODO

3.4.9

We use a symbol L to define a ring

$$R = \{a + bL : a, b \in Z\}$$

where addition is defined in an obvious way and multiplication is defined by using the rules

$$L^2 = 1, La = aL$$

For the rest of this thing we're assuming that $L \notin Z$, since otherwise some things don't hold

(a) Find a formula for the product $(a + bL) * (c + dL)$.

We follow that

$$(a + bL) * (c + dL) = ac + adL + bLc + bLdL = ac + bd + (ad + bc)L$$

(b) Prove that the ring R has zero divisors

If $L = 1$, then it does not. But if we add an assumption that $L \notin Z$, then

$$(1 - L)(1 + L) = 1 + L - L - L^2 = 1 - 1 = 0$$

(c) Prove that the ring R is not isomorphic to the ring $Z \times Z$

Assume that there's an isomorphism f . Identities are mapped pretty easily,

$$0 \rightarrow (0, 0)$$

$$1 \rightarrow (1, 1)$$

but we then need to map L somewhere. We follow that there is (a, b) such that $f(L) = (a, b)$. Since L is not in the Z , we conclude that $a \neq b$. We then follow that $L * L = 1$, and thus

$$a * a = 1$$

$$b * b = 1$$

and since there are no multiplicative inverses for any $a, b \in Z$ apart from 1 and -1 we follow that $a, b \in \{1, -1\}$. This in turn implies that either $f(L) = (-1, 1)$ or $f(L) = (1, -1)$. Assume the latter. We then follow that

$$f(1 + L) = (2, 0)$$

$$f(1 - L) = (0, 2)$$

Now let's try to square some numbers:

$$f((1 + L)(1 - L)) = f(1 - L + L - L^2) = f(0) = 0$$

$$f((1+L)(1-L)) = (2, 0) * (0, 2) = 0$$

which is unhelpful.

$$\begin{aligned} f((1-L)(1-L)) &= f(1-L-L+L^2) = f(2-2L) = (0, 4) \\ f((1-L)(1-L)) &= (0, 2) * (0, 2) = (0, 4) \end{aligned}$$

which is also unhelpful.

I'm pretty sure that we somehow need to prove that the R has multiplicative inverses for some elements, but $Z \times Z$ does not. We can follow that

$$(2-L) * (1+L) = 2 + 2L - L - 1 = 1 + L$$

while

$$((2, 2) - (1, -1)) * ((1, 1) + (1, -1)) = (1, 3) * (2, 0) = (2, 0)$$

which might be wrong again.

Let us try to prove the thing then, and maybe we'll have some problems then. All the identities are handled, additivity is trivial, and for multiplication we've got

$$\begin{aligned} f((a+bL) * (c+dL)) &= f((ac+bd) + (ad+bc)L) = (ac+bd+ad+bc, ac+bd-ad-bc) \\ f(a+bL) * f(c+dL) &= (a+b, a-b) * (c+d, c-d) = (ac+ad+bc+bd, ac-ad-bc+bd) \end{aligned}$$

so we're kinda shafted in this regard. Maybe the f is not a bijection then. It's certainly a function from R to $Z \times Z$, and is defined on all R . If there are $a, b \in R$ such that $a \neq b$ and $f(a) = f(b)$, then we conclude that $f(a-b) = f(a) - f(b) = 0$, and hence there's a nonzero element $q \in R$ such that it maps to 0. Construction of f though prohibits such a thing, and thus we must conclude that it's an injection.

Okay, now I've got it. Let $a+bL \in R$. We follow that

$$f(a+bL) = (a+b, a-b)$$

we then conclude that the difference between those two

$$a+b-a+b=2b$$

is always even. Thus we conclude that there's no way for example to map the thing to $(1, 0)$, since the difference between indices is odd, and thus we conclude that f is not surjective, and thus we conclude that R and $Z \times Z$ are not isomorphic.

(d) However, prove that the ring

$$S = \{a+bL : a, b \in Q\}$$

is isomorphic to the ring $Q \times Q$.

This case grants us on the other hand the ability to get surjectivity, that we can prove through a lot of notation, but it's easy to see why it is the case from the last paragraph of the previous point.

3.4.10

Let R_1, R_2, \dots be an infinite list of rings. blah-blah-blah, we can define rings from infinite list of rings by the same reason as for the multiple rings (i.e. piecewise application). Part (b) comes from the fact that the ring that is there's an injection from 2^ω to $Z/2Z^\omega$

Skip the rest

3.5 Ideals and Quotient Rings**Notes**

Firstly it's important to note that ideals are mostly not subrings due to the fact that the ones that aren't equal to the whole space R don't have multiplicative identities in them. They are subgroups under addition however, which is evident from their definition.

Given that ideals are subgroups under the addition, we can conclude from our endeavours in group theory that the set of distinct cosets of an ideal constitutes a partition of a ring R . A partition of a ring R with respect to an ideal I is denoted by R/I . Apart from the initial ideal I we can follow that no other element of R/I is an ideal due to the fact that any given ideal I has got to have 0 in it.

Suppose that we've got an R/I . Let $q \in R/I$ and $b \in q$. Since $q \in R/I$ we follow that by definition there is an element $j \in R$ such that

$$q = j + I$$

(where sum of an element of R and a subset of R is defined in an obvious way). $b \in q$, and thus by definition of addition of a set to an element we conclude that there's an element $k \in I$ such that

$$b = j + k$$

and thus

$$j = b - k$$

and therefore if $w \in q$ is an arbitrary element, then there's $e \in I$ such that

$$w = j + e$$

thus

$$w = b - k + e$$

since $k, e \in I$ we follow that $-k \in I$, thus $-k + e \in I$, and therefore $w \in b + I$. Thus $q \subseteq b + I$. The case with \supseteq is kinda similar, which gives us an identity $q = b + I$, which together with the fact that b and q are arbitrary element gives us a biconditional

$$q \in R/I \wedge b \in q \Leftrightarrow q = b + I$$

thus any given element of R/I can be represented as a sum of any of its elements and I .

Formulas that were given in the book don't give out too much rigor, and thus let us clarify the whole shebang:

In the book we're given formulas

$$(a + I) + (b + I) = (a + b) + I$$

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

and without any context this thing does not make much sense. We know that for any given coset q there's an element $a \in R$ such that $q = a + I$ (which we're gonna call an *additive representation* of a coset). Additive representations are only representations, and from our previous point in the notes we can follow that any given coset can have several additive representations, and a single representation refers only to one coset. Thus this representation can be formulated as "one-to-many" from cosets to representations.

With our notion of representations we can now make sense of the formulas. Given two representations we follow that there exists a single representation, that conforms to the provided formulas. Given that there is a single coset that is represented by a representation, we conclude that formula essentially is a binary function from representations to cosets. In the book (and further in the exercises) we are proving the fact that those formulas are "well defined", i.e. that given two cosets, there exists only one coset, to which their respective representations are being sent, and thus that we can define a proper function from pairs of cosets to cosets, that conforms to the formula.

Although with proper maintenance we can define sums and products in a way, that they were defined in the book, I wonder if we could define the same thing in terms of ranges. Given $a, b \in R/I$, we can define sum and product functions $+: R/I \times R/I \rightarrow \mathcal{P}(R)$ $*: R/I \times R/I \rightarrow \mathcal{P}(R)$ by

$$a + b = \{q + w \in R : q \in a \wedge w \in b\}$$

$$a * b = \{q * w \in R : q \in a \wedge w \in b\}$$

where it is essentially a range of underlying $+$ and $*$ respectively over a set of pairs between elements of a and b . Problem is that those functions are having a codomain of $\mathcal{P}(R)$, but we want to prove specifically that we can restrict codomains of those functions to R/I . Material in the book and the exercises certainly implies that ranges of functions over underlying sets are subsets of a single coset (i.e. given $a, b \in R/I$ there's $c \in R/I$ such that $a + b \subseteq c$ and the same goes for $*$).

UPDATE: after doing some exercises, I became convinced that this thing won't work after all. Defining product as a sum of products (as with ideals) might solve the problem, but I won't investigate this thing further.

In order to try to prove that our definitions are indeed equivalent to the ones in the book, we might want to prove some other things about cosets. Notably we need to show

that if $b' \in R/I$, $w \in I$, and $b \in b'$, then $b + w \in b'$. We can do that by a straightforward application of the definition of coset.

Let $a', b', w \in R/I$ be such that $a' + b' \subseteq w$. Let $q \in w$. We follow that since $q \in w$ that $w = q + I$. Let $a \in a'$, $b \in b'$. We follow that $a + b \in w$, and thus $a + b \in q + I$. Therefore there is an element $e \in I$ such that $a + b = q + e$. Therefore $a + b - e = q$. Since $e \in I$ we follow that $-e \in I$, thus $b - e \in b'$, and therefore we conclude that for $q \in w$ there is a pair of element $\langle a, b - e \rangle \in a' \times b'$ such that $q = a + b - e$, and thus $w \subseteq a' + b'$, which implies that $a' + b' = w$.

Let $a', b', w \in R/I$ be such that $a' * b' \subseteq w$. Let $q \in w$. We follow that since $q \in w$ that $w = q + I$. Let $a \in a'$, $b \in b'$. We follow that $a * b \in w$, and thus $a * b \in q + I$. Therefore there is an element $e \in I$ such that $a * b = q + e$. Therefore $a * b - e = q$.

$$(a + w) * (b + e) = ab + wb + ae + we$$

$$a * (b - e) = ab - ae$$

$$(a - w) * b = ab - wb$$

$$(a - w) * (b - e) = ab - wb - ae + we$$

$$(a + w) * (b + e) + (a - w) * (b - e) = 2ab + 2we = 2(ab + we)$$

TODO

With our definitions we can try to produce formulas, that were given in the book: Let $a', b' \in R/I$. Let $a \in a'$, $b \in b'$. We follow that

$$a' = a + I$$

and

$$b' = b + I$$

as discussed previously. Now let us prove the identity in the book. Let

$$q \in (a + b) + I$$

We follow that it is the case if and only if there's $w \in I$ such that

$$q = (a + b) + w \Leftrightarrow q = (a + 0) + (b + w)$$

which implies that

$$q \in (a + I) + (b + I)$$

Now assume that $q \in (a + I) + (b + I)$. We follow that there are $w, e \in I$ such that

$$q = a + w + b + e$$

thus

$$q = (a + b) + (w + e)$$

given that $w, e \in I$ we follow that $w + e \in I$ and thus

$$q \in (a + b) + I$$

thus giving us an identity

$$(a + I) + (b + I) = (a + b) + I$$

which gives us the formula from the book.

Let $a, b \in R$. We follow that

$$q \in (a + I) * (b + I)$$

implies that there are $c, d \in I$ such that

$$q = (a + c) * (b + d)$$

$$q = ab + cb + ad + cd$$

we follow that $cb, ad, cd \in I$ by definition of ideal, and thus

$$cb + ad + cd \in I$$

therefore

$$q \in ab + I$$

which gives us a statement

$$(a + I) * (b + I) \subseteq a * b + I$$

3.5.1

Let R be a commutative ring.

(a) Let $c \in R$. Prove that

$$\{cR : r \in R\}$$

is an ideal of R .

Let's name the unnamed set Q and assume that $q, w \in Q$. We follow that there are $a, b \in R$ such that $q = ca$ and $w = cb$. We then follow that

$$q + w = ca + cb = c(a + b) \in Q$$

where we derive the last relation by definition of Q .

If $r \in R$, then we conclude that

$$rq = rca = cra \in Q$$

where derivations come from the fact that R is commutative. Hence we conclude that Q is an ideal by definition.

(b) ... straightforward applications of definitions and commutative/distributive properties of R will give us this conclusion

3.5.2

Let R be a commutative ring. Prove that R is a field if and only if its only ideals are the zero ideal and the entire ring R .

Assume that R is a field and let $c \in R$ be nonzero. We follow that there's $c^{-1} \in R$, and thus $c^{-1}R$ is a subset of R by closure. Multiplying c by this subset we get that $R \subseteq cR$, and thus $c \neq 0 \Rightarrow cR = R$. If $c = 0$ we can trivially conclude that $cR = \{0\}$.

Now assume that R is a commutative ring whose only ideals are $\{0\}$ and R . Let $q \in R$ be nonzero. We follow that $qR = R$, and thus there's $w \in R$ such that $qw = 1$. This implies that $w = q^{-1}$, and thus we conclude that the fact that q is arbitrary together with this implication constitutes a definition of a field, as desired.

3.5.3

Let R be a commutative ring, and let I be an ideal of R . The radical of I is defined to be the set

$$\text{Rad}(I) = \{a \in R : (\exists n \in \omega)(n \geq 1 \wedge a^n \in I)\}$$

Prove that $\text{Rad}(I)$ is an ideal of R .

Let $a \in \text{Rad}(I)$ and $b \in R$. We follow that there's $n \in \omega$ such that $a^n \in I$ by definition of $\text{Rad}(I)$. We also follow that since $b \in R$ that $b^n \in R$ and thus we follow that $(ab)^n = a^n b^n$ is a product of an element of I and an element of R , and thus is in I by the fact that I is an ideal.

Let $a \in \text{Rad}(I)$. We follow that there's a $n \in \omega$ such that $a^n \in I$. We then follow that for all $m \geq n$ that $a^m = a^n a^{m-n}$ and thus a^m is a multiple of an element of I (a^n) and an element of R , and thus it is itself an element of I .

Now assume that $a, b \in \text{Rad}(I)$ and $m, n \in \omega$ are such that $a^n, b^m \in I$. We follow that

$$(a + b)^k = \sum_{i \in \{0..k\}} bc(i, k) a^i b^{k-i}$$

for any $k \in \omega$. Thus if $k \geq 2 \max(m, n)$, then for any element of the sum

$$bc(i, k) a^i b^{k-i}$$

either i or $k - i$ is greater than $\max(m, n)$, and thus a^i or b^{k-i} is in I , thus the whole product is in I , and thus then the sum is a sum of elements of I , thus making the whole sum an element of I . Thus we follow that there's an element n of ω such that $(a + b)^n \in I$, and therefore we conclude that $a + b \in \text{Rad}(I)$.

Those two properties constitute a definition of the ideal, as desired.

3.5.4

The goal of this exercise is to prove that every ideal in Z is principal ideal.

(a) *Let I be a non-zero ideal in Z . Prove that I contains a positive integer.*

If I is a non-zero ideal, then it's got $a \in I$ such that $a \neq 0$. If $a > 0$, then we're done, and if not, then we follow that $-1 * a > 0 \in I$.

(b) *Let I be a non-zero ideal in Z . Let c be the smallest positive integer in I . Prove that every element of I is a multiple of c .*

We follow that all the multiples of c are in I . If there's some element $q \in I$ that is not a multiple of c , then we follow that $\gcd(q, c) < c$, and thus there are integers $a, v \in Z$ such that $aq + vc = \gcd(q, c)$. Since $q, c \in I$ we follow that $\gcd(q, c) \in I$, and thus we conclude that there's a positive element of I that is less than c , which is a contradiction.

(c) *Prove that every ideal in Z is principal.*

Directly follows from the previous point.

3.5.5

Prove the remaining parts of Proposition 3.32. Let R be a commutative ring, and let I be an ideal of R .

(a) *Let $a + I$ and $a' + I$ be two cosets. Prove that $a + I = a' + I$ if and only if $a - a' \in I$.*

Suppose that $a + I = a' + I$. We follow that there are elements $i, i' \in I$ such that $a + i = a' + i'$. Then we follow that $a - a' = i' - i$. Since $i', i \in I$ we follow that $-i \in I$ and $i' - i \in I$, and thus $a - a' \in I$.

If $a - a' \in I$, then we follow that there's an element $i \in I$ such that $a - a' = i$, thus $a = a' + i$. We then follow that for every element in $q \in a + I$ there's an element $i' \in I$ such that $q = a + i'$, and thus $q = a' + i + i'$. By the additive closure of I we follow that $i + i' \in I$, and thus we conclude that $q \in a' + I$, which gives us the \subseteq relation between those sets. Reverse direction is kinda similar, and thus we conclude the desired reverse implication.

(b) *Prove that addition of cosets is well-defined.*

Was taken care of in the notes.

(c) *Prove that addition and multiplication of cosets turns R/I into a commutative ring.*

Definition of the sum and the axioms of underlying ring imply all the necessary conditions in a straightforward fashion.

3.5.6

Let R be a commutative ring.

(a) Let I be an ideal of R . Prove that the map f

$$R \rightarrow R/I, a \rightarrow a + I$$

sending an element to its coset is a surjective ring homomorphism whose kernel is I . This is proposition 3.34(a)

R/I is a partition of R , and thus if $q \in R/I$, then there's $w \in q \subseteq R$, thus $f(w) = q$, which implies that f is surjective. Identities are mapped properly by definition, and the fact that the thing is a homomorphism is handled by definitions of R/I . If $q \in I$, then $f(q) = q + I = 0 + I$, and otherwise it isn't, which implies that the whole $f(q) = 0$ if and only if $q \in I$, thus making I into the kernel of f .

(b) Let I and J be ideals of R . Prove that the map g

$$R \rightarrow R/I \times R/J, a \rightarrow (a + I, a + J)$$

is homomorphism. What is its kernel? Give an example where it is surjective and an example for which it is not surjective.

Although this thing looks unconventional, it is nothing but a concatenation of homomorphisms and thus a homomorphism itself. Kernel of this thing is the intersection of underlying rings (I and J respectively in this case).

We can set $I = 2Z$, $J = 3Z$, and thus if $(a, b) \in Z/2Z \times Z/3Z$, then we follow that we have set $b + 3Z$ has both even and odd elements, and thus we're able to produce proper element depending on a , thus making the map surjective. We can also set $I = J = 2Z$, from which we can't produce element $(1, 0)$, which gives us a non-surjective map.

3.5.7

Let I be the principal ideal of $\mathbb{R}[x]$ generated by polynomial $x^2 + 1$. Prove that the map

$$\phi : \mathbb{R}[x]/I \rightarrow C, \phi(f(x) + I) = f(i)$$

is a well-defined isomorphism, where $i = \sqrt{-1}$, as usual.

If q is an element in R/I , then we follow that for all $f \in q$ we get

$$q = f + I$$

Thus if for any $q \in R/I$ we follow that for all $f_1, f_2 \in q$

$$f_1(i) = f_2(i)$$

then can conclude that any element of q maps i to the same value, and thus there's a function from R/I to C that maps the things exactly in a way that the exercise describes.

Now let us try to prove that and let $q \in R/I$ and $f_1, f_2 \in q$. We follow that there's $w \in C$ such that

$$f_1(i) = w$$

Since $f_1, f_2 \in q$ we follow that $f_1 - f_2 \in I$, and by definition of I we follow that there's $c \in \mathbb{R}[x]$ such that

$$f_1 - f_2 = c(x^2 + 1)$$

therefore

$$f_2 = f_1 - c(x^2 + 1)$$

and thus

$$f_2(i) = f_1(i) - c(x^2 + 1) = w - c(-1 + 1) = w - c0 = w$$

which all implies the fact that the whole shebang is "well-defined".

Now we need to prove that this thing is an isomorphism. Identities are easy, functions are as well, and hence this thing is a homomorphism. Bijectivity is kinda interesting though.

If $r \in I$, then $r(i) = c(-1 + 1) = 0$. From our previous exercises know that for any polynomials in commutative rings

$$r(k) = 0 \iff r(x) = (x - k)f(x)$$

for some $f \in R$, and thus $r(i) \neq 0$ implies that there's no polynomial $g \in R$ such that $r = (x - i)g$. In polynomials in real coefficients it's also not too complicated to prove that $r(x) = r(\bar{i})$, which means that $-i$ is also not a root for this polynomial, which gives us the fact that $r \neq (x - i)(x + i)g = (x^2 + 1)$. This implies that $r \notin I$, and thus kernel of ϕ is I . Theorem in the book proves then that ϕ is injective.

If $k \in C$, then we follow that there are $a, b \in R$ such that $k = a + bi$, and thus

$$f(x) = a + bx$$

is an element of R such that $f(i) = k$, which implies that ϕ is surjective, which gives us the fact that ϕ is an isomorphism, as desired.

3.5.8

Let R be a commutative ring and let I be an ideal of R . For $a \in R$, we will denote the coset $a + I$ by \bar{a} , i.e.

$$R \rightarrow R/I : a \rightarrow \bar{a}$$

is the reduction modulo I homomorphism. We define a map of polynomial rings

$$\phi : R[x] \rightarrow (R/I)[x], \phi(\sum a_i x^i) = \sum \bar{a}_i x^i$$

by reducing the coefficients modulo I . Prove that ϕ is a ring homomorphism.

We can easily follow that identities are mapped as expected. The rest is basically taken care of by the definitions and previous proves:

$$\phi(a + b) = \phi\left(\sum a_i x^i + \sum b_i x^i\right) = \phi\left(\sum (a_i + b_i) x^i\right) = \sum \overline{(a_i + b_i)} x^i$$

$$\phi(a) + \phi(b) = \sum \overline{a_i} x^i + \sum \overline{b_i} x^i = \sum \overline{(a_i + b_i)} x^i$$

$$\phi(a * b) = \phi\left(\sum a_i x^i * \sum b_j x^j\right) = \phi\left(\sum \sum a_i b_j x^{i+j}\right) = \sum \sum \overline{a_i b_j} x^{i+j}$$

$$\phi(a) * \phi(b) = \sum \overline{a_i} x^i * \sum \overline{b_j} x^j = \sum \sum \overline{a_i b_j} x^{i+j}$$

as desired.

3.5.9

Let R be a commutative ring and let I and J be ideals of R

(a) Prove that the intersection $I \cap J$ is an ideal of R .

We follow that if $w, e \in I \cap J$, then $w + e \in I$ by axioms of I and $w + e \in J$ by axioms of J , and thus $w + e \in I \cap J$. If $q \in R$ is arbitrary, then $wq \in I$ by axioms of I and $wq \in J$ by axioms of J , which implies that $wq \in I \cap J$. This constitutes a definition of an ideal, as desired.

(b) Prove that the ideal sum (that is defined in an obvious way) is an ideal of R

If $q, w \in I + J$, then there are $a, b \in I$ and $c, d \in J$ such that $q = a + c, w = b + d$, and we can follow that then

$$q + w = a + b + c + d = (a + c) + (b + d) \in I + J$$

If $e \in R$ is arbitrary, then

$$e + q = e + a + b = (e + a) + b \in I + J$$

which implies that $I + J$ is indeed an ideal, as desired.

(c) The ideal product of two ideals is defined to be

$$IJ = \left\{ \sum a_i b_i : n \geq 1 \wedge a_n \in I \wedge b_n \in J \right\}$$

Prove that IJ is an ideal of R

Pretty much the same idea as before: sums do not even need to be rearranged, and

$$c \sum a_i b_i = \sum c a_i b_i = \sum (c a_i) b_i$$

which by power of the fact that I is an ideal gives us the desired result.

(d) One might ask why the product IJ of ideals isn't simply defined as the set of products. The answer is that the set of product need not be an ideal. Here is an example. Let $R = \mathbb{Z}[x]$, and let I and J be the ideals

$$I = 2\mathbb{Z}[x] + x\mathbb{Z}[x], J = 3\mathbb{Z}[x] + x\mathbb{Z}[x]$$

Prove that the set of products is not an ideal.

We follow that

$$a_1 = x, a_2 = -2 \in I$$

$$b_1 = x, b_2 = 3 \in I$$

We then follow that $a_1b_2 = 3x$, $a_2b_1 = -2x$ are in the set of products. We then follow that $3x - 2x = x$ is a sum of elements of the set of products. Let $i \in I$ and $j \in J$ be arbitrary. We follow that if $i * j = x$, then degrees of i and j got to be 1 and 0 in order for the product to be of order 1. Since 1 is a multiple of neither 2 or 3 we can follow that there are no polynomials, which implies that the set is not closed under addition, and thus is not an ideal.

(e) On the other hand, prove in general that if either I or J is a principal ideal, then the set of products is an ideal.

Assume that I is a principal ideal. We follow that if $a', c' \in I$ and $b, d \in J$ are elements, then their pairwise products are in the set of products, and thus for arbitrary $e \in R$ we've got that

$$ca'b = (ea') * b$$

which satisfies the multiplication part of the definition of an ideal. Since I is a principal ideal, we follow that there's $q \in R$ that is a defining element of I , and thus there are $a, c \in R$ such that $a' = qa, c' = qc$. Thus

$$a'b + c'd = qab + qcd = q(ab + cd)$$

$b, d \in J$, and thus $ab \in J$ and $cd \in J$. Together with the fact that $q \in I$ we follow that the abovementioned element is indeed an element of the set of products, which gives us the closure of the set under addition.] Together with the previous part it constitutes a definition of an ideal, as desired.

3.5.10

Let R be a ring, let I be an ideal of R , and for any other ideal J of R , let \overline{J} be the following subset of the quotient ring R/I :

$$\overline{J} = \{a + I : a \in J\}$$

(a) Prove that \overline{J} is an ideal of R/I .

If $q', w' \in \overline{J}$, we follow that

$$q' + w' = q + I + w + I = (q + w) + I$$

$q + w \in J$ by the powers of J , and thus the whole thing is \overline{J} . By similar logic product of any element of R/I and \overline{J} is in \overline{J} , which concludes the proof.

(b) Let \overline{K} be an ideal of R/I . Prove that the set

$$Q = \bigcup_{a+I \in \overline{K}} (a + I)$$

is an ideal of R that contains I .

By definition of \overline{K} and underlying K we follow that $0 \in K$, and thus $0 + I = I \in \overline{K}$, which implies that $I \subseteq Q$. If $a, b \in Q$, then there are appropriate $a', b' \in K$, and thus

$$ca = c(a + k) = ca + ck$$

$ck \in K$, and thus the abovementioned thing is an element of $ca + K$.

$$a + b = a_1 + k_1 + b_1 + k_2 = (a_1 + b_1) + (k_1 + k_2)$$

and thus blah-blah-blah, it is all covered.

(c) Conclude that there is a bijective map

$$\{\text{ideals of } R \text{ that contain } I\} \rightarrow \{\text{ideals of } R/I\}, J \rightarrow J/I$$

By point (a) for every ideal of R (whether or not it contains I) there's an appropriate ideal of R/I . If $R_1 \neq R_2$ are ideals that contain I , then we follow that there is $r_1 \in R_1 \setminus I$ such that $r_1 \notin R_2$ (if not, then swap'em around and assume so). Thus $r_1 + I$ is in the $\overline{R_1}$ but not in $\overline{R_2}$ by their respective definitions. Thus the whole thing is injective. If Q is an ideal of R/I , then by point (b) we've got an ideal of R that contains I . If $I \subseteq J$ and J is an ideal, then we can follow that point (b) is essentially an inverse function of construction of \overline{J} , which produced the desired result.

3.5.11

Prove that the set of nilpotent elements is an ideal of R .

It's the radical of ideal $\{0\}$.

3.6 Prime Ideals and Maximal Ideals

Notes

There's gotta be an easier way to do this, but we gonna try to prove that for every non-invertible element of an R there's a maximum ideal, that contains it. Let us assume that

$q \in R$ is such that $q \notin R^*$. We follow that all of the $\mathcal{P}(R)$ is a set, and thus there's a set of all ideals of R . Therefore there's a set of all ideals of R that contain q , and if we remove R from this set, then we get a set of all ideals of R , that are not R , but contain q (this set is not empty due to restriction on q ; this can be derived, but it's not that complicated, key is to assume that since $q \notin R^*$ that there's no nonzero power of q that is equal to 1). We then follow that this thing is a poset under \subseteq , and let C be a chain in it. We then conclude that

$$1 \in \cup C \Rightarrow \exists Q' \in C : 1 \in Q' \Rightarrow Q' = R$$

which implies that $1 \notin \cup C$. Now if $r, w \in \cup C$, then we follow that $r \in Q_1, w \in Q_2$, and by the fact that C is a chain we follow that $r \in Q_2$ or $w \in Q_1$, which in turn implies that $r + w \in Q_1$ or $r + w \in Q_2$, and thus $r + w \in \cup C$. By similar process we conclude that for arbitrary $r \in R$ and $c \in \cup C$ we've got that $rc \in \cup C$, which implies that $\cup C$ is an ideal that contains q , and thus $\cup C \in C$.

By Zorn's lemma then we follow that there's a maximal element M in the set of ideals of R that aren't R and contain q under \subseteq . Let now $r \in R \setminus M$. We follow that if J is an ideal such that $M \subseteq J$ and $r \in J$, then by definition of M and r , J is not an ideal of R that isn't R , and thus $J = R$, which implies that M is a maximal ideal. Thus we conclude the following:

Let R be a commutative ring. If $q \notin R^*$, then there's a maximal ideal M that contains q .

3.6.1

Let I be the following subset of the ring $Z[x]$ of polynomials having integer coefficient.

$$I = \{2a(x) + xb(x) : a(x), b(x) \in Z[x]\}$$

(a) Prove that I is an ideal of $Z[x]$.

We follow that both $a(x), b(x)$ are ideals, both $2a(x)$ and $xb(x)$ are principal ideals, and thus I is a set of sums of two ideals, and thus itself an ideal (as proven in the exercises).

(b) Prove that $I \neq Z[x]$

1 is not present in I

(c) Prove that I is not a principal ideal

Assume that $q(x)$ is an ideal, that generates I . We follow that it generates both 2 and x , for which the only common multiple is 1, which implies that $q = 1$, which implies that $I = Z[x]$, which is not true.

(d) Prove that I is a maximal ideal of $Z[x]$

Let J be an ideal of $Z[x]$ that properly contains I . Assume that $q \notin I$. We follow that since $q \notin I$ that it cannot be a multiple of x , and thus it has to contain an element b of sum of degree 0. Since $q \notin I$ we follow that this element is not even (and thus odd). Thus we then follow that $q - b$ is a multiple of x that does not have an element of the sum of

degree 0, and thus is a multiple of x . Therefore we can state that $q - b \in I$, which implies that $q - (q - b) = b \in J$. Since $b \in J$ is an odd number, we follow that $b - 2n \in J$ for all $n \in \mathbb{Z}$, which implies that $1 \in J$, which in turn implies that $J = \mathbb{Z}[x]$, as desired.

3.6.2

(a) Let $m \neq 0$ be an integer. Prove that the ideal $m\mathbb{Z}$ is a maximal ideal if and only if $|m|$ is a prime number

Assume that $m\mathbb{Z}$ is a maximal ideal. If m is not a prime, then there are $a \in \mathbb{Z} \setminus \{0, 1\}, b \geq 2$ such that $m = ab$. By the restriction on b we follow that a, b aren't multiples of m , and thus $m\mathbb{Z}$ is not a prime ideal. Thus contrapositive of this statement implies that m is a prime, as desired.

Assume now that m is a prime and let $b \in \mathbb{Z} \setminus m\mathbb{Z}$. We follow that $\gcd(m, b) = 1$, thus there are integers a, v such that $am + bv = 1$, which implies that if J is an ideal that contains both $m\mathbb{Z}$ and b , then $J = \mathbb{Z}$, which implies that $m\mathbb{Z}$ is a maximal ideal, as desired.

(b) Let F be a field, and let $a, b \in F$ with $a \neq 0$. Prove that the principal ideal $(ax + b)F[x]$ is a maximal ideal of the polynomial ring $F[x]$.

Since $a \in F$ and $a \neq 0$ we follow that $a^{-1} \in F$. Thus by pretty much the same logic as in previous exercise (part c) we conclude the same result.

(c) Skip

3.6.3

Let R be a ring, let $M \subseteq R$ be a maximal ideal, and let R^* be its group of units. Prove that the following is equivalent

(a) M is the only maximal ideal of R

(b) $R = M \cup R^*$.

A ring having a unique maximal ideal is called a local ring.

What is interesting is that if $r \in R^*$, then there is $r^{-1} \in R^*$, and thus if $r \in M$ then $rr^{-1} = 1 \in M$ by properties of an ideal, and thus $M = R$, which is not true. This implies that $M \cap R^* = \emptyset$ for any maximal ideal M . Thus the whole thing is a partition.

Assume (a) and contradict (b). Let $q \in R \setminus (M \cup R^*)$. Theorem in the notes implies that there's a maximal ideal, that contains q , and thus definition of q implies that M is not the only maximal ideal, which is a contradiction (holy heck, that was an overkill)

Let us assume (b). Prerequisites of the exercise imply that M has got to be a maximal ideal, so we are only required to derive the uniqueness of it. Assume that M' is a maximal ideal of R , that is different from M . We follow that M' cannot be a subset of M , since M' is a maximal ideal, and thus there's $q \in M' \setminus M$. (b) now implies that $q \in R^*$, and thus there's $q^{-1} \in R$, which means that $qq^{-1} = 1 \in M'$, which implies that $M' = R$, which is false, and thus we conclude the desired result, which was pretty easy.

The rest of the exercises are skipped for now

Chapter 4

Vector Spaces - Part 1

Practically all the material here was covered in my course on linear algebra

Chapter 5

Fields - Part 1

5.1 Introduction to Fields

5.2 Abstract Fields and Homomorphisms

5.2.1

Let F be a field and let $f(x) \in F[x]$ be a non-zero polynomial.

(a) Suppose that $\alpha \in F$ is a root of $f(x)$. Prove that there is a polynomial $g(x) \in F[x]$ such that $f(x) = (x - \alpha)g(x)$.

This one is a repeat of an exercise two chapters before (3.8(b))

(b) More generally, suppose that $\alpha_1, \dots, \alpha_n \in F$ are distinct roots of $f(x)$. Prove that there is a polynomial $g(x)$ such that

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)g(x)$$

We're gonna use the induction on this one. Part (a) will suffice as a base case. Let $f(x) = (x - \alpha_1)g(x)$ and $\alpha_2 \neq \alpha_1$ is a root of $f(x)$. We follow then that

$$(\alpha_2 - \alpha_1)g(\alpha_2) = 0$$

Since F is a field, it's an integral domain, and thus it's got cancellation property. $(\alpha_2 - \alpha_1) \neq 0$ by our assumption, and thus we follow that $g(\alpha_2) = 0$. Part(a) implies all the things that it needs to imply, which gives us the desired result.

(c) Use (b) to deduce the following important result:

Theorem Let F be a field, and let $f(x) \in F[x]$ be a nonzero polynomial. Then $f(x)$ has at most $\deg(f)$ distinct roots in F .

If there are more roots, than the degree, then part (b) implies that it's got such a decomposition, which gives it greater degree than it's got, which gives us a contradiction.

5.2.2

Done this one.

5.3 Interesting Examples of Fields**5.3.1**

Prove that each of the following subsets of R is a field

(a) $Q(\sqrt{3})$

The same idea as with $\sqrt{2}$ works here as well: inverses are found in a same way as inverses of complex numbers, closure is kinda trivial, and the rest is inherited from R .

(b) $Q(\sqrt{4})$

Since $\sqrt{4} = 2$, it's just Q

(c) *Skip*

5.3.2

Prove that each of the following rings is not a field:

(a) $Z[i]$

We can follow that there's no inverse of 2 (or any other non-1 element), simplest proof of that comes from the fact that by multiplying any given element by that thing gives us a tuple, that consists of multiples of that number, and 1 is not a multiple of any non-1 number

(b) $Z[\sqrt{2}]$

Same idea as in (a)

(c) Z/p^2Z , where p is a prime

We can follow that $p \neq 0$, but $p^2 = 0$, which implies that the whole thing is not an integral domain, and thus not a field.

(d) Z/mnZ , where $m, n \geq 2$

Same idea as in (c)

5.3.3

The fields $Q(i)$ and $Q(\sqrt{2})$ are both contained in the field C .

(a) *Prove that $Q(i)$ is not contained in $Q(\sqrt{2})$*

i is not present in $Q(\sqrt{2})$

(b) *Prove that $Q(\sqrt{2})$ is not contained in $Q(i)$*

$\sqrt{2}$ is not present in $Q(i)$.

5.3.4

(a) Prove that

$$\sqrt{6} \notin \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$$

and conclude that this set of real numbers is not a ring

Suppose that there are $a, b, c \in \mathbb{Q}$ such that

$$\sqrt{6} = a + b\sqrt{2} + c\sqrt{3}$$

we follow then that

$$\begin{aligned}\sqrt{6} - a &= b\sqrt{2} + c\sqrt{3} \\ (\sqrt{6} - a)^2 &= (b\sqrt{2} + c\sqrt{3})^2 \\ 6 - 2a\sqrt{6} + a^2 &= 2b^2 + 2bc\sqrt{6} + 3c^2 \\ 6 + a^2 - 3c^2 - 2b^2 &= 2bc\sqrt{6} + 2a\sqrt{6} \\ 6 + a^2 - 3c^2 - 2b^2 &= \sqrt{6}(2bc + 2a)\end{aligned}$$

lhs here is rational, and thus if $(2bc + 2a) \neq 0$ we've got a contradiction. Thus we conclude that $2bc + 2a = 0 \Rightarrow bc + a = 0 \Rightarrow a = -bc$.

$$\begin{aligned}\sqrt{6} - c\sqrt{3} &= a + b\sqrt{2} \\ 6 + c^2 3 - 6c\sqrt{2} &= a^2 + 2b^2 + 2ab\sqrt{2} \\ 6 + c^2 3 - a^2 - 2b^2 &= 2ab\sqrt{2} + 6c\sqrt{2} \\ 6 + c^2 3 - a^2 - 2b^2 &= \sqrt{2}(2ab + 6c)\end{aligned}$$

by the same logic $2ab + 6c = 0$

$$\begin{aligned}\sqrt{6} - b\sqrt{2} &= a + c\sqrt{3} \\ 6 + 2b^2 - 4b\sqrt{3} &= a^2 + 3c^2 + ac\sqrt{3} \\ 6 + 2b^2 - (a^2 + 3c^2) &= ac\sqrt{3} + 4b\sqrt{3} \\ 6 + 2b^2 - (a^2 + 3c^2) &= \sqrt{3}(ac + 4b)\end{aligned}$$

by the same logic $ac + 4b = 0$ thus

$$\begin{cases} a = -bc \\ 2ab + 6c = 0 \\ ac + 4b = 0 \end{cases}$$

$$\begin{cases} 2(-bc)b + 6c = 0 \\ (-bc)c + 4b = 0 \end{cases}$$

$$\begin{cases} -2b^2c + 6c = 0 \\ -bc^2 + 4b = 0 \end{cases}$$

$$\begin{cases} c(-b^2 + 3) = 0 \\ b(-c^2 + 4) = 0 \end{cases}$$

the fact that $b \in Q$ implies that $b^2 \neq 3$, and thus $c = 0$. Therefore $-c^2 + 4 \neq 0$, which implies that $b = 0$, and thus $a = 0$. Therefore we conclude that $a = b = c = 0$, which implies

$$a + b\sqrt{2} + c\sqrt{3} = 0$$

which is a contradiction (I might've messed up some of the calculations here, but it has got to get the same result w/ the right ones). More general case of this thing is somewhat whacky, maybe I'll try to get a hold of it sometime in the future.

(b) *Prove that the set*

$$Q(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, a, b, c, d \in Q\}$$

is a subring of R .

It's closed under all the respective properties and it has zeroes.

(c) *Prove that $Q(\sqrt{2}, \sqrt{3})$ is a subfield of R*

Assume that

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in Q(\sqrt{2}, \sqrt{3})$$

we want to find $a' + b'\sqrt{2} + c'\sqrt{3} + d'\sqrt{6} \in Q(\sqrt{2}, \sqrt{3})$ such that

$$(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) * (a' + b'\sqrt{2} + c'\sqrt{3} + d'\sqrt{6}) = 1$$

moreover, we can relax this thing, to get any given number

$$(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) * (a' + b'\sqrt{2} + c'\sqrt{3} + d'\sqrt{6}) = j$$

so that $j \in Q$ and $j \neq 0$ we follow that

$$(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) * (a' + b'\sqrt{2} + c'\sqrt{3} + d'\sqrt{6}) =$$

$$\begin{aligned} & (aa' + ab'\sqrt{2} + ac'\sqrt{3} + ad'\sqrt{6}) + \\ & (b\sqrt{2}a' + 2bb' + b\sqrt{2}c'\sqrt{3} + b\sqrt{2}d'\sqrt{6}) + \\ & (c\sqrt{3}a' + c\sqrt{3}b'\sqrt{2} + 3cc' + c\sqrt{3}d'\sqrt{6}) + \\ & (d\sqrt{6}a' + d\sqrt{6}b'\sqrt{2} + d\sqrt{6}c'\sqrt{3} + 6dd') = \end{aligned}$$

$$(aa' + ab'\sqrt{2} + ac'\sqrt{3} + ad'\sqrt{6}) +$$

$$\begin{aligned}
& (2bb' + a'b\sqrt{2} + bc'\sqrt{6} + 3b\sqrt{3}d') + \\
& (3cc' + c\sqrt{3}a' + cb'\sqrt{6} + 3c\sqrt{2}d') + \\
& (6dd' + d\sqrt{6}a' + d2\sqrt{3}b' + 3d\sqrt{2}c') = \\
& (aa' + ab'\sqrt{2} + ac'\sqrt{3} + ad'\sqrt{6}) + \\
& (2bb' + a'b\sqrt{2} + 3bd'\sqrt{3} + bc'\sqrt{6}) + \\
& (3cc' + 3cd'\sqrt{2} + ca'\sqrt{3} + cb'\sqrt{6}) + \\
& (6dd' + 3c'd\sqrt{2} + 2db'\sqrt{3} + da'\sqrt{6})
\end{aligned}$$

thus given (presumed) linear independence of roots of integers under Q , we follow that we need to find such $a', b', c', d' \in Q$ so that

$$\begin{cases} ab' + a'b + 3cd' + 3c'd = 0 \\ ac' + 3bd' + ca' + 2db' = 0 \\ ad' + bc' + cb' + da' = 0 \end{cases}$$

now let us move some variables around (the ones without the dash are our given constants in this case)

$$\begin{cases} ba' + ab' + 3dc' + 3cd' = 0 \\ da' + cb' + bc' + ad' = 0 \\ -ca' + 2db' + ac' + 3bd' = 0 \end{cases}$$

and probably this one leads to the satisfying answer TODO

5.3.5

Let F be a finite field. Prove that

$$\prod_{\alpha \in F^*} \alpha = -1$$

Given $\alpha \in F^*$ we can follow that there is $\alpha^{-1} \in F^*$ as well, but they do not need to be distinct (i.e. there's a case when $\alpha = \alpha^{-1}$). Thus we can partition the whole set into subsets, that contain one or two elements, where each subset that contains two elements is a set of an element and its inverse. Product of those sets is then 1, and thus we follow that the entire product is the product of all elements, that are equal to its inverses.

For our not-so general case of F_{13} we have a case that the whole product can be partitioned into

$$\{2, 7\}, \{3, 9\}, \{4, 10\}, \{5, 8\}, \{6, 11\}, \{12\}$$

(needed a hint on this one) Suppose that there is an element $q \in F$ such that $q^2 = 1$ and such that q is distinct from 1 and -1 . We follow that

$$(q - 1)(q + 1) = q^2 - 1 = 1 - 1 = 0$$

thus

$$(q - 1)(q + 1) = 0$$

this implies that $q - 1 = 0$ or $q + 1 = 0$, which implies that $q = \pm 1$, which is a contradiction. Thus we conclude several things, chief among them is the fact that any element that is not equal to ± 1 is distinct from its inverse. Thus we conclude by previous point (1st paragraph) the desired result.

The rest of this section is TODO

5.4 Subfield and Extension Fields

5.4.1

(a) Let K/F be an extension of fields. Prove that

$$[K : F] = 1 \Leftrightarrow K = F$$

Since K/F is an extension, by definition we have that $F \subseteq K$.

Suppose that $[K : F] = 1$. This means that $\dim_F(K) = 1$, and therefore $\{1\}$ spans K . Thus if $k \in K$, then there is $f \in F$ such that $f \cdot 1 = k$, and thus $f = k$. Therefore we have that $k \in F$, and thus $K \subseteq F$, which implies the right side. Reverse is trivial.

(b) Let L/F be a finite extension of fields, and suppose that $[L : F]$ is a prime. Suppose further that K is a field such that $F \subseteq K \subseteq L$. Prove that either $K = F$ or $K = L$.

We follow that $[L : K]$ is finite (if it's infinite, then $[L : F]$ is infinite, which is not the case), and thus

$$[L : F] = [L : K] * [K : F]$$

the fact that $[L : F]$ is prime implies that $[L : K]$ or $[K : F]$ is equal to one, which by previous point implies the desired result

5.4.2

Let K/F be a finite extension of fields. Prove that there is a finite set of elements $\alpha_1, \dots, \alpha_n \in K$ such that

$$K = F(\alpha_1, \dots, \alpha_n)$$

The fact that K/F is finite extension by definition implies that there is $n \in \omega$ such that

$$\dim_F(K) = n$$

thus there is a basis (don't know whether or not we need AoC in this case) A of elements of K . Linear combination under F of elements of A will span K by the fact that it is the basis, which gives us the desired conclusion.

5.4.3

let $L/K/F$ be extensions of fields.

(a) Assume that L/K and K/F are finite extensions. During the proof of Theorem 5.18 we defined a set

$$C = \{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

claimed that C is a basis for L as an F -vector space, and proved that C is linearly independent. Prove that C is a spanning set

Let $l \in L$. We follow that there are $c_1, \dots, c_n \in K$ such that

$$l = \sum c_i b_i$$

each c_i is an element of K and thus there are $q_1, \dots, q_m \in F$ such that

$$c_i = \sum q_{i,j} a_j$$

and thus

$$l = \sum \sum q_{i,j} a_j b_i$$

by unfolding this sum we get the desired result.

(b) Prove that $|C| = mn$, i.e. prove that the mn products of $a_i b_j$ are distinct.

Assume that there are $a_i b_j$ and $a_q b_w$ such that $a_i \neq a_q$ and $b_j \neq b_w$, but

$$a_i b_j = a_q b_w$$

One thing that we can follow is that $a_i, a_q, b_j, b_w \neq 0$ since they are part of a basis for L and K respectively. We then follow that

$$a_i a_q^{-1} b_j = b_w$$

which implies that b_j is a nonzero multiple of b_w in L/K , which implies that the list is then not linearly independent, thus making B not a basis, which gives us a contradiction

(c) Prove that L/F is an infinite extension if and only if at least one of L/K or K/F is an infinite extension

Part (a) of this theorem is fully cooked at this point, which gives us an easy forward implication. Thus assume that one of the L/K or K/F is infinite. We can then see that the proof for finite case does not depend on finality of A nor B , and thus we conclude that C in that case is indeed a basis for L/F . We then see that

$$[L : F] = \dim_F(L) = |C|$$

which is still the case for infinite sets, which gives us the desired conclusion

The rest of this section was previously attempted in the notes, not foint to repeat it here

5.5 Polynomial Rings

Notes

Let us reiterate a couple of things here: given a ring R there is a set of finite lists of elements of R , whose first element is not zero. We call those lists polynomials, and denote the set of them by $R[x]$. Degree of a polynomial is the length of a given list minus 1 for nonzero polynomials, and $-\infty$ for the zero polynomial. Thus \deg is a function

$$\deg : R[x] \rightarrow \omega \cup \{-\infty\}$$

for any given R . Purpose of including $-\infty$ to the mix is to ensure that we've got an identity

$$\deg(f_1 f_2) = \deg(f_1) + \deg(f_2)$$

where we define addition between a random element of ω (or $-\infty$) with $-\infty$ in an obvious manner.

5.5.1

Repeat of a previous exercise

5.5.2

Let F be a field, let $f(x), g(x) \in F[x]$ be polynomials with $g(x) \neq 0$, and suppose that there are polynomials $q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$ satisfying

$$f(x) = g(x)q_1(x) + r_1(x) \text{ with } \deg(r_1) < \deg(g)$$

$$f(x) = g(x)q_2(x) + r_2(x) \text{ with } \deg(r_2) < \deg(g)$$

prove that $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$.

If $\deg(f) < \deg(g)$, then we follow that if $q_1 \neq q_2$, then one of q_1, q_2 aren't zero. Assume that $q_1 \neq 0$, and then

$$\deg(g(x)q_1(x)) = \deg(g(x)) + \deg(q_1(x))$$

since $\deg(r(x)) < \deg(g(x))$, we follow that

$$\deg(g(x)q_1(x) + r(x)) = \deg(g(x)) + \deg(q_1(x)) \geq \deg(g(x)) > \deg(f(x))$$

and thus

$$g(x)q_1(x) + r(x) \neq f(x)$$

which gives us a contradiction.

Since

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x) \\ f(x) &= g(x)q_2(x) + r_2(x) \end{aligned}$$

we follow that

$$\begin{aligned} g(x)q_1(x) + r_1(x) - (g(x)q_2(x) + r_2(x)) &= f(x) - f(x) = 0 \\ g(x)q_1(x) + r_1(x) - (g(x)q_2(x) + r_2(x)) &= 0 \\ g(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x)) &= 0 \\ g(x)(q_1(x) - q_2(x)) &= r_2(x) - r_1(x) \end{aligned}$$

thus

$$\deg(g(x)(q_1(x) - q_2(x))) = \deg(r_2(x) - r_1(x))$$

If $q_1 \neq q_2$, then we follow that $q_1 - q_2 \neq 0$, and thus $\deg(g(x)(q_1(x) - q_2(x))) \geq \deg(g(x))$. Degree of rhs here is less than $\deg(g(x))$, which gives us a contradiction. Thus we conclude that $q_1 = q_2$, which then implies that

$$r_2(x) - r_1(x) = g(x) * 0 = 0$$

which implies the desired result.

5.6 Building Extension Fields

Notes

One thing that we can say is that if a polynomial has roots, then an exercise from chapter 3 implies that it is reducible. Equivalently irreducible polynomials don't have roots. Reverse is not necessarily true, we can have rootless reducible polynomials.

We also follow that if $f \in F[x]$ is of degree 1, then we can follow that $f(x) = a_1x + a_0$ and thus

$$a_1x + a_0 = 0$$

$$a_1x = -a_0$$

$$x = -a_0/a_1$$

and thus f has roots.

5.6.1

Let F be a field

(a) Prove that every polynomial of degree 1 in $F[x]$ is irreducible

Let $g \in F[x]$ be a polynomial of degree 1. We follow that if there are $h, k \in F[x]$ such that

$$g = h * k$$

then

$$\deg(g) = \deg(h * k) = \deg(h) + \deg(k)$$

thus

$$\deg(h) + \deg(k) = 1$$

Thus we conclude that $\deg(h) = 0$ or $\deg(k) = 0$, which implies the desired result.

(b) Let $f \in F[x]$ be a polynomial of degree 2. Prove that $f(x)$ is irreducible if and only if it has no roots in F .

Irreducibility implies lack of roots in general, as indicated in the notes. Now assume that f has no roots in F . We follow that if f is reducible, then there are nonconstant $g, h \in F[x]$ such that

$$f(x) = g(x) * h(x)$$

we then follow that

$$\deg(f(x)) = \deg(g(x) * h(x)) = \deg(g(x)) + \deg(h(x)) = 2$$

Since g, h are nonconstant, we follow that $\deg(g(x)) = \deg(h(x)) = 1$, which implies that they have roots, and thus f has roots as well, which is a contradiction.

(c) Let $f \in F[x]$ be a polynomial of degree 3. Prove that $f(x)$ is irreducible if and only if it has no roots in F .

Same kind of idea as in point (b), but we follow that either g or h has roots.

(d) Let $f(x) = x^4 + 2$. Prove that $f(x)$ is irreducible in $Q[x]$.

We can follow that if f has roots, then

$$x^4 + 2 = 0$$

$$x^4 = -2$$

which is a contradiction, and thus f has no roots. If f is reducible, then there are $g, h \in Q[x]$ such that

$$f(x) = g(x)h(x)$$

this implies that either $g(x)$ or $h(x)$ has degree 1 or 2 (other needs to have degree 3 or 2).

If $g(x)$ has degree 1, then it's got roots, and thus f has roots, which is not the case.

Suppose that there is $g(x)$ such that there is $h(x)$ so that

$$x^4 + 2 = g(x)h(x)$$

we follow that both g and h have degree 2. Assume that g, h are both monic polynomials. Then we can give indicate indices of g as a and indices of h as b , which gives us

$$(x^2 + a_1x + a_2) * (x^2 + b_1x + b_2) = x^4 + 2$$

$$x^4 + b_1x^3 + b_2x^2 + a_1x^3 + a_1b_1x^2 + a_1b_2x + a_2x^2 + a_2b_1x + a_2b_2 = x^4 + 2$$

$$x^4 + (b_1 + a_1)x^3 + (b_2 + a_1b_1 + a_2)x^2 + (a_1b_2 + a_2b_1)x + a_2b_2 = x^4 + 2$$

$$(b_1 + a_1)x^3 + (b_2 + a_1b_1 + a_2)x^2 + (a_1b_2 + a_2b_1)x + a_2b_2 = 2$$

therefore

$$\begin{cases} b_1 + a_1 = 0 \\ b_2 + a_1b_1 + a_2 = 0 \\ a_1b_2 + a_2b_1 = 0 \\ a_2b_2 = 2 \end{cases}$$

$$\begin{cases} a_1 = -b_1 \\ b_2 - b_1^2 + b_2^{-1} 2 = 0 \\ -b_1b_2 + b_2^{-1} 2b_1 = 0 \\ a_2 = b_2^{-1} 2 \end{cases}$$

$$\begin{cases} a_1 = -b_1 \\ b_2 - b_1^2 + b_2^{-1} 2 = 0 \\ b_1(-b_2 + b_2^{-1} 2) = 0 \\ a_2 = b_2^{-1} 2 \end{cases}$$

Let us concentrate on the third equation, which by the fact that Q is a field, and thus an integral domain, gives us two cases: $b_1 = 0$ or $-b_2 + b_2^{-1} 2 = 0$. If we assume the former, then second equation becomes

$$b_2 + b_2^{-1} 2 = 0$$

$$b_2^2 + 2 = 0$$

and no such elements of Q exist. Thus we conclude the latter case, which gives us that

$$-b_2 + b^{-1} 2 = 0$$

$$-b_2^2 + 2 = 0$$

$$b_2^2 = 2$$

and once again, no such element of Q exists, which implies that there are no monic polynomials of degree 2, that multiply to f . Now if $g(x)$ and $h(x)$ are arbitrary polynomials of degree 2, that multiply to f , then we conclude that coefficients for x^2 in both g and h has got to multiply to 1. Thus we conclude that multiplying both polynomials by inverses of their coefficients for x^2 gives us a pair of monic polynomials, which gives us a hasty contradiction, and thus implies the desired result.

One last thing to point out: if we generalize the case, and include

(e) Let $f = x^4 + 4$. Prove tht f is reducible in $Q[x]$, despite the fact that it has no roots in Q .

$$x^4 + 4 = (x^2 + 2x + 2) * (x^2 - 2x + 2)$$

5.6.2

Let F be a field, and suppose that the polynomial $X^2 + X + 1$ is irreducible in $F[X]$. Let

$$K = F[X]/(X^2 + X + 1)F[X]$$

be the quotient ring.

(a) Find a polynomial $p(X) \in F[X]$ of degree at most 1 such that

$$\overline{p(X)} = \overline{(X + 3)} * \overline{(2X + 1)}$$

We follow that

$$(X + 3) * (2X + 1) = 2X^2 + 7X + 3$$

we then want to get an element of $(X^2 + X + 1)F[X]$, whose sum with given element is of power of 1 or less. This is easy, we can get

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

and then subtract one from another to get

$$2X^2 + 7X + 3 - 2X^2 - 2X - 2 = 5X + 1$$

(b) Find a polynomial $q(X) \in F[X]$ of degree at most 1 satisfying

$$\overline{q(X)} * \overline{X + 1} = \overline{1}$$

Exercise says that we can get an element of degree 1 in here, so let's try that

$$x * (x + 1) = x^2 + x$$

initial guess wont do, so let us try dividing the initial polynomial with the remainder

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

thus we might get a guess of plugging $-x$, which gives us

$$(-x) * (x + 1) = -x^2 - x \equiv 1$$

as desired. Here we might try to develop a proper way of finding multiplicative inverses, but I'm too eager to move forward to actually do that

(c) Find a polynomial $r \in F[x]$ of degree at most 1 satisfying

$$\bar{r}^2 = \overline{-3}$$

We can follow that

$$\overline{-3} = \overline{x^2 + x + 1 - 3} = \overline{x^2 + x - 2} = \overline{(x - 1) * (x + 2)}$$

we then try to plug in some coefficients into $x^2 + x + 1$ so that its sum with -3 is a square. We follow that 4 is such a number:

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

which in turn implies that

$$\overline{(2x + 1)^2} = \overline{4x^2 + 4x + 1} = \overline{-3}$$

as desired.

5.6.3

Let

$$f(x) = \sum_{0 \leq i \leq d} c_i x^i \in Z[x]$$

be a polynomial of degree $d \geq 1$

(a) Prove that if $a/b \in \mathbb{Q}$ is a root of $f(x)$, written in lowest terms, then $a|c_0$ and $b|c_d$

We follow that

$$\sum_{0 \leq i \leq d} c_i x^i = c_0 + \sum_{1 \leq i \leq d} c_i x^i$$

and thus

$$f(a/b) = c_0 + \sum_{1 \leq i \leq d} c_i (a/b)^i = c_0 + \sum_{1 \leq i \leq d} c_i a^i b^{-i} = c_0 + a \sum_{1 \leq i \leq d} c_i a^{i-1} b^{-i}$$

since a/b is a root of $f(x)$ we follow that

$$f(a/b) = c_0 + a \sum_{1 \leq i \leq d} c_i a^{i-1} b^{-i}$$

$$\begin{aligned}
0 &= c_0 + a \sum_{1 \leq i \leq d} c_i a^{i-1} b^{-i} \\
-c_0 &= a \sum_{1 \leq i \leq d} c_i a^{i-1} b^{-i} \\
-c_0 b^d &= a b^d \sum_{1 \leq i \leq d} c_i a^{i-1} b^{-i} \\
-c_0 b^d &= a \sum_{1 \leq i \leq d} c_i a^{i-1} b^{d-i}
\end{aligned}$$

by our multiplication by b^d we got rid of elements of Q , and now this whole shebang is in Z . We then follow that since a/b are in their lowest terms that they don't have any common primes as multiples, which implies that

$$a | c_0$$

as desired.

We can then do similar trick with c_d to get

$$\begin{aligned}
0 &= f(a/b) = \sum_{0 \leq i \leq d} c_i a^i b^{-i} = c_d b^{-d} + \sum_{0 \leq i \leq d} c_i a^i b^{-i} \\
0 &= c_d a^d b^{-d} + \sum_{0 \leq i \leq d-1} c_i a^i b^{-i} \\
0 &= c_d a^d + b^d \sum_{0 \leq i \leq d-1} c_i a^i b^{-i} \\
-c_d a^d &= b^d \sum_{0 \leq i \leq d-1} c_i a^i b^{-i} \\
-c_d a^d &= b \sum_{0 \leq i \leq d} c_i a^i b^{d-1-i}
\end{aligned}$$

which also implies the desired result.

(b) Use (a) to find the small finite set of integers A and B so that all of the rational roots of the polynomial

$$g(x) = 45x^4 + 62x^3 + 56x^2 + 11x - 6$$

are in the set

$$\left\{ \pm \frac{a}{b} : a \in A, b \in B \right\}$$

Part (a) here gives us the idea that we can get a total set of divisors of the first and the last coefficients of any given polynomials, then get a set of fractions out of those two sets, and this set in the end will contain all of the rational roots of the given polynomial. I've written the desired program (polyq.py in progs/, bruteforced a couple of things), and the result is pretty fun

5.6.4

Let F be a field, and let $f(x, y) \in F[x, y]$ be a polynomial in two variables. For example, you could take f to be irreducible

Definitions of irreducibility (and so on) are transferring nicely to two variables. On top of that, polynomials of one variable can be viewed as a polynomial in two variables, which allows us to conclude that for example $(x + 1)$ is an irreducible polynomial of two variables.

Definitions of degrees is kinda non-applicable, but the fact that we include only non-constant polynomials are applicable in this case

(a) Suppose that there are values $a, b \in F$ such that $f(a, b) = 0$. Let I be the ideal

$$I = \{(x - a)g(x, y) + (y - b)h(x, y) : g, h \in F[x, y]\}$$

Prove that

$$f(x, y)F[x, y] \subset I \subset R$$

(proper subsets) and conclude that the principal ideal $f(x, y)F[x, y]$ generated by $f(x, y)$ is not maximal

We can follow that if I contains f , then it contains $f(x, y)F[x, y]$ properly by the fact that I is an ideal (proof of the fact that I is an ideal is kind of trivial).

We can follow that since f is a polynomial implies that there is a maximal power of either x or y that we're going to denote by d , and thus we can set

$$f(x, y) = \sum_{0 \leq i, j \leq d} c_{i,j} x^i y^j$$

from the fact that

$$x^n - c^n = (x - c) \sum_{0 \leq i \leq n-1} x^i c^{n-1-i}$$

$$\begin{aligned} f(x, y) &= f(x, y) - 0 = f(x, y) - f(a, b) = \\ &= \sum_{0 \leq i, j \leq d} c_{i,j} x^i y^j - \sum_{0 \leq i, j \leq d} c_{i,j} a^i b^j = \sum_{0 \leq i, j \leq d} c_{i,j} (x^i y^j - a^i b^j) = \end{aligned}$$

TODO

the rest of this section is marked as TODO

5.7 Finite Fields

5.7.1

Let F be a finite field with q elements

(a) Prove that every non-zero element of F is a root of the polynomial $x^{q-1} - 1$

We can follow that F^* is an abelian group under multiplication, and since it is finite, we follow that for $a \in F : a \neq 0$ its order m divides the order of F^* , which is precisely $q - 1$. We then follow that

$$a^{q-1} = (a^m)^{(q-1)/m} = 1^{(q-1)/m} = 1$$

which implies the desired result.

(b) Prove that every element of F is a root of the polynomial $x^q - x$

We follow that

$$x^q - x = x(x^{q-1} - 1)$$

and thus its zeroes are all nonzero elements, and zero (i.e. the whole field)

(c) Prove the formula

$$\prod_{a \in F} (x - a) = x^q - x$$

Since every $a \in F$ is a root of $x^q - x$ we follow that it can be deconstructed into lhs (exercise 5.1(b) directly implies it)

5.7.2

Let m and n be positive integers

(a) Prove that $x^m - 1$ divides $x^n - 1$ in $F[x]$ if and only if m divides n in \mathbb{Z} .

Suppose that m divides n . Definition states that there exists $k \in \mathbb{N}_+$ such that $n = mk$.

Thus

$$x^n - 1 = x^{mk} - 1$$

and thus

$$\begin{aligned} (x^m - 1) * \sum_{0 \leq i \leq k-1} x^{im} &= \sum_{0 \leq i \leq k-1} x^{im} * (x^m - 1) = \sum_{0 \leq i \leq k-1} x^{(i+1)m} - x^{im} = \\ &= \sum_{0 \leq i \leq k-1} x^{(i+1)m} - \sum_{0 \leq i \leq k-1} x^{im} = \sum_{1 \leq i \leq k} x^{im} - \sum_{1 \leq i \leq k-1} (x^{im}) - 1 = \\ &= x^{km} + \sum_{1 \leq i \leq k-1} x^{im} - \sum_{1 \leq i \leq k-1} (x^{im}) - 1 = x^{km} - 1 \end{aligned}$$

as desired (derivation of the desired polynomial was done by observing polynomial division for lower powers, i.e. $x^6 - 1$ and $x^2 - 1$, and then generalizing the hypothesis).

Now assume that $x^m - 1$ divides $x^n - 1$. Thus there is a polynomial $h(x)$ such that

$$(x^m - 1) * h(x) = x^n - 1$$

We follow that there is $g(x)$ such that

$$\begin{aligned}(x^m - 1) * (x^{n-m} + g(x)) &= x^n - 1 \\(x^m - 1) * (x^{n-m} + g(x)) &= x^n - 1 \\x^n + x^m g(x) - x^{n-m} - g(x) &= x^n - 1 \\x^m g(x) - x^{n-m} - g(x) &= -1 \\(x^m - 1)g(x) &= x^{n-m} - 1\end{aligned}$$

and this is the moment where induction should kick somewhere here.

Our hypothesis is that if $x^m - 1$ divides $x^n - 1$, then for all $k \in N_+$ such that $mk \leq n$ we have that $x^m - 1$ divides $x^{n-mk} - 1$. Base case is provided, and the inductive step is not much different from the base case, which gives us the desired conclusion. We then can state that if m does not divide n , then there is $k \in N_+$ and $0 < r < m$ such that

$$n = km + r$$

and thus

$$x^n - 1 = x^{km+r} - 1$$

our little lemma gives us that since $x^m - 1$ divides $x^n - 1$ that $x^m - 1$ divides $x^r - 1$, which is impossible by the degrees rule, which gives us the desired contradiction.

(b) Let $a \geq 2$ be an integer. Prove that a^m divides $a^n - 1$ in Z if and only if m divides n in Z .

Proof is similar to the proof of previous point, where we swap appropriate things.