My abstract algebra exercises

Evgeny (Gene) Markin

2024

Contents

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:

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

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 untill stated otherwise since it's most convinient 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 $\{1, 2, ..., n\}$ 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 exacly the factorial of the cardinality of the underlying set.

2.1.3

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

I'm pretty sure that we've proven that rigorously in the set theory course. If not, then the proof comes from contradiction and theh 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 $\phi : S \to S$ 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 $\phi : S \to S$ such that ϕ is surjjective but nnot bijective

We can set $S = \omega$ and

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

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

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

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

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

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

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

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

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

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 $k \in Z$. 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 $G = Z/5$) 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:

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

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. $l = lcm(m,n)$). 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 $l = lcm(m,n)$ is divided by both m and n we follow that $g^m h^n$'s order divides l.

If there's $k \leq lcm(m,n)$ 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 $k < lcm(m,n)$, thus h^n's order is a multiple of both m and n. h^{nk} cannot be 1, and its order must be then $lcm(m,n)$ 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 $k = lcm(m,n)$, 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 suffested 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

$$a \to (\text{h * k = e}) \to c \to b \to c \to a \to (\text{h * k = e})$$

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 practially establishes the Identity axiom. The associative law is unchanged from the stadart 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

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

but they have fewer or different asiomx 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 $N = \{1, 2, 3, ...\}$ 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 $N_0 = \{0, 1, 2, 3, ...\}$ with the composition law being addition.

handled in part (a)

(c) $(Z, +)$

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 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) $(Z, *)$

Same as previous for the same reason.

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

If there's $m \in Z$, then there's $n_0, n_1 \in Z$ 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 associaativity. 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 binanry 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 a 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 do to 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 indentity, 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 $S_n : \omega \to \omega$

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

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 agenerator of G. Prove that g^k is a generator of G if and only uf $gcd(k, n) = 1$.

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 exits $j \in Z$ 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 vertiex 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 fillow that for each $i \in Z/pZ$, $i * 1 = i$, and thus i is our identity. Associativity of multiplication under Z implies our associativity.

From group theory we know that there's x such that $ax \equiv 1(modm)$ if and only if $gcd(a, m) = 1$. We then follow that for any given $i \in Z/pZ$ we've got that $gcd(i, p) = 1$ since p is prime, and thus there's $a \in Z/pZ$ such that $a * i = 1$. Thus we've got the inverse, and Z/pZ 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 Z/pZ, which implies that only multiple of q is its multiple, or 0, which implies that it's got no inverse and hence Z/pZ is not a group, as desired. If p is not a prime, however, then we've got that Z/pZ 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 didnt 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:

$$(Z/pZ)^*$$

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

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

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

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

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 remeber 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)

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

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

(b)

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

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

(c)

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

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)

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

Does not contain the identity, and inverses arent present

(e)

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

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 clamed that the group law for Q is determined by

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

Use there formulas to prove following formulas, which completely determine the group opetrations on Q:

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

$$i * i = -1$$

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

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

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

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

where the last part comes from the note that -1 commutes with eveything. 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

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

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

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

$$\phi : G_1 \to G_2$$

The fact that ϕ is bijective means that the inverse map $\phi^{-1} : G_2 \to G_1$ 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 functiion

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

(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 ony 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

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

thus the group is abelian.

Reverse direction:

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

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

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

Since G is abelian we follow that $h_1 h_2 = h_2 h_1$, 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 $\phi : G_1 \to G_2$ is an isomorphism

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

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

$$g_1 g_2 = \phi(h_1)\phi(h_2) = \phi(h_1 h_2) = \phi(h_2 h_1) = \phi(h_2)\phi(h_1) = g_2 g_1$$

as desired.

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

2.4.5

In this exericse, C_n is a cyclic group of order n, D_n is the nh dihedral group, and S_n is the nth 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 predictible 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 isomorhic. 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 dont 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 ren'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. Importatnt 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 exacltly $n/gcd(n,k)$ 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 comrised 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

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

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

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 $h_1 * {h_2}^{-1\,-1} = h_1 * h_2 \in H$, 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.

qSuppose 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 $b^{-1} = k \in H$. 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 ve 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

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

(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

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

$q \in \langle S \rangle$ 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 $S \cap T$ 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.

Ler 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

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

(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. Supposde 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 $\phi(e, e) = e * e = e = q q^{-1} = phi(q, q^{-1})$ 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

$$\phi(\langle a_1, b_1\rangle * \langle a_2, b_2\rangle) = \phi(\langle a_1, b_1\rangle) * \phi(\langle a_2, b_2\rangle) = a_1b_1a_2b_2$$

it also implies that

$$\phi(\langle a_1, b_1\rangle * \langle a_2, b_2\rangle) = \phi(\langle a_1, b_1\rangle * \langle a_2, b_2\rangle) = \phi(\langle a_1 * a_2, b_1 * b_2\rangle) = a_1a_2b_1b_2$$

thus

$$a_1a_2b_1b_2 = a_1b_1a_2b_2$$

for all $a_1a_2 \in A, b_1, b_2 \in B$. 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 nonemptyness 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 $a \in \{1, ..., n\}$, let $q \in S_n$ be an element such that it maps a to itself, and maps $(a+1) \mod n$ 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 $a \in \{1, ..., n\}$ 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 $\{1, ..., n\}$: we take the $q(a)$ and some element $b \in \{1, ..., n\} \setminus \{q(a), a\}$, 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 $j \in \{1, ..., n-1\}$ 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 $k \in \{0, ..., n\}$. 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) Compue 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. $sr^j r = sr^j \neq srj - 1 = rsr^j$, 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 $srsr^2 = r^3$ and $sr^2sr = r$, 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 diagnogal, 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 numbder 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 $(q^{-1} g)K$ is a coset of K in H. Thus there's a unique $w \in W$ such that

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

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 $q_1 H \neq q_2 H$ by definition. $w_1 w_2 \in H$, and thus $w_1 w_2 H = H$. Since $K \subseteq H$ we follow that

$$q_1 w_1 K \subseteq q_1 H$$

$$q_2 w_2 K \subseteq q_2 H$$

and thus

$$q_1 w_1 K \neq q_2 w_2 K$$

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

$$w_1 K \neq w_2 K$$

and thus

$$q_1 w_1 K \neq q_1 w_2 K$$

and since $q_1 = q_2$ we follow that

$$q_1 w_1 K \neq q_2 w_2 K$$

This implies that if $\langle q_1, w_1\rangle, \langle q_2, w_2\rangle \in Q \times W$ then $q_1 w_1 K \neq q_2 w_2 K$, and thus we conclude that there's an injection from $Q \times W$ to a set of cosets of K. Shroder-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 inteeger satisfying $p \not| a$. Use Exercise 2.13(b) and Lagrange's theorem to prove

***Fermat's Little Theorem**: $a^{p-1} \equiv 1(\mod p)$*

We follow that if $a \not| p$, then $a \not\equiv 0 \mod p$. 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

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

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

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

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

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

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 $G_1, G_2, ..., G_n$ be groups. Generalize definition 2.54 by explaining why

$$G_1 \times ... \times G_n$$

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

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

(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 thaht $ab \neq ba$. 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.

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

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 distibuted 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

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

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

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

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

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

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

$$= a^2 + ab + ab + b^2 = f(a) + ab + ab + f(b) = f(a) + f(b) + ab(1+1) =$$

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

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

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

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

$$f(1+1) = (1+1)^3 = (1+1) * (1+1) * (1+1) = 8$$

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

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 ZZ: if f and g are homomorphims from Z to some ring R, then $f = g$.

A little note about polynomials: whenever we've got a ring R, by polynomials in R we understand a list of coefficients of R, first one on whom is not zero. This implies that athough we can have a finite ring R, its ring of polynomials $R[x]$ is infinite. Cardinality of the ring $R[x]$ is then the same, as the cardinality of the set of sequences over R.

This further implies that since the set of functions over a finite ring R is finite, but the set of polynomials is infinite, that there are two distinct polynomials, that correspond to the same function. In real numbers we know (or at the very least assume pretty heavily) that each polynomial represents a distinct function, so then the question is as follows: what are the conditions, that give us injectivity from the set of polynomials to the set of functions?

Assume that $f, g \in R[x]$, are such that $f \neq g$ in terms of polynomials. Assume that $f = g$ in terms of functions. We follow that for all $x \in R$ we have that

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

thus we have that

$$\sum a_i x^i = \sum b_i x^i$$

$$\sum (a_i - b_i) x^i$$

since $f \neq g$ in terms of polynomials we follow that there is $k \in \omega$ such that $a_k \neq b_k$. Moreover, we follow that since $f = g$ we follow that $f(0) = g(0)$, and thus $a_0 = b_0$, otherwise we're screwed. We thus conclude that there is polynomial $h = f - g$ such that h is non-constant and nonzero, and such that for all $r \in R$ we follow that

$$h(r) = 0$$

at the very least it gives us that if R is an infinite integral domain, then it's got at most $deg(h)$ roots, and thus the given case is impossible. Thus all of the Z, Q, R, and other normal things are covered.

3.2.1

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

$$\phi : Z \to Z/ZmZ, \phi(a) = a \mod m$$

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 $Z/17Z$. Compute $\alpha + \beta$ and $\alpha * \beta$.

We follow that

$$7 + 11 = 18 \equiv 1 \mod 17$$

$$7 * 11 = 77 \equiv 9 \mod 17$$

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

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

$$(3 + 2x - x^2) * (2 - 3x + x^2) = (6 - 9x + 3x^2) + (4x - 6x^2 + 2x^3) + (-2x^2 + 3x^3 - x^4) =$$

$$= 6 - 15x - 5x^2 + 5x^3 - x^4$$

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

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

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

$$= (2+2i+i-1)+(4-2i+2i+1)x+(-2-i)x^2+(1+i+3i-3)x+(2-i+6i+3)x^2+(-1-3i)x^3 =$$

$$= (1 + 3i) + 5x + (-2 - i)x^2 + (-2 + 4i)x + (5 + 5i)x^2 + (-1 - 3i)x^3 =$$

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

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

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

$$(1 + 2i - j + k) * (2 - i + 3j - k) =$$

$$= (2 - i + 3j - k) + 2i(2 - i + 3j - k) - j(2 - i + 3j - k) + k(2 - i + 3j - k) =$$

$$= (2 - i + 3j - k) + (4i + 2 + 6k + 2j) - (2j + k - 3 - i) + (2k - j - 3i + 1) =$$

$$= (2 - i + 3j - k) + (2 + 4i + 2j + 6k) + (3 + i - 2j - k) + (1 - 3i - j + 2k) =$$

$$= 8 + i + 2j + 6k$$

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 quntities

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

We follow that

$$2 + 3\sqrt{5} + 1 - 2\sqrt{5} = 3 + \sqrt{5}$$

$$(2 + 3\sqrt{5}) * (1 - 2\sqrt{5}) = 2 - 4\sqrt{5} + 3\sqrt{5} - 30 = -28 - \sqrt{5}$$

$$(2 + 3\sqrt{5})^2 = 4 + 12\sqrt{5} + 45 = 49 + 12\sqrt{5}$$

(b) Prove that the map

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

is a ring homomorphism.

We follow that identities are golden.

$$\phi(a + b\sqrt{D} + c + d\sqrt{D}) = \phi((a + c) + (b + d)\sqrt{D}) =$$

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

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

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

$$ac + bdD - ad\sqrt{D} - bc\sqrt{D}$$

thus everything checks out, as desired.

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

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

$$\alpha * \overline{\alpha} = (a + b\sqrt{D}) * (a - b\sqrt{D}) =$$

$$= a^2 - ab\sqrt{D} + ab\sqrt{D} + b^2D = a^2 + b^2D$$

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 tht $\rho^3 = 1$. Thus ρ is a cube root of unity.

$$\left(\frac{-1+i\sqrt{3}}{2}\right)^3 = \left(\frac{\sqrt{3}}{2}i - \frac{1}{2}\right)^3 = \left(\frac{\sqrt{3}}{2}i\right)^3 - 3\left(\frac{\sqrt{3}}{2}i\right)^2\left(\frac{1}{2}\right) + 3\left(\frac{\sqrt{3}}{2}i\right)\left(\frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^3 =$$

$$= -\frac{3\sqrt{3}}{8}i + \frac{9}{8} + \frac{3\sqrt{3}i}{8}i - \frac{1}{8} = 1 + 0 = 1$$

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 lhs 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

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

$$= X^2 - X(\rho^2 X + \rho - 1) + X + 1 == X^2 - 0X + X + 1 = X^2 + X + 1$$

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 identites are present. Additive group is closed by general properties of C.

$$(a + b\rho) * (c + d\rho) = ac + ad\rho + bc\rho + bd\rho^2 = ac + ad\rho + bc\rho + bd\rho^2 + bd\rho + bd - bd\rho - bd =$$

$$= ac + ad\rho + bc\rho + bd(\rho^2 + \rho + 1) - bd\rho - bd = ac + ad\rho + bc\rho + bd0 - bd\rho - bd =$$

$$= (ac - bd) + \rho(ad + bc - bd)$$

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 $E_c : R[x] \to R$ 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

$$E_c(f + g) = (f + g)(c) = f(c) + g(c) = E_c(f) + E_c(g)$$

$$E_c(f * g) = (f * g)(c) = f(c) * g(c) = E_c(f) * E_c(g)$$

by algebraic properties of functions.

(b) Prove that $E_c(f) = 0$ if ans 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 $E_\alpha : R[x] \to R$ 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

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

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 identites 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. Detiviations of associativity and distributivity take a lok of paper, but are pretty uneventful.

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

This is where our assumtions 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

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

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

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

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

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

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

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 onyl 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 particualarly interesting.

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

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

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 $\phi : R_1 \to R_2$ be homomorphism. We define a map $\Phi : R_1[x] \to R_2[x]$ 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

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

$$= \sum \phi(a_i)x^i + \phi(b_i)x^i = \sum (\phi(a_i) + \phi(b_i))x^i =$$

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

$$\Phi(\sum a_i x^i) + \Phi(\sum b_i x^i) = (\sum \phi(a_i)x^i) * (\sum \phi(b_i)x^i) = \sum \sum \phi(a_i)\phi(b_j)x^{i+j} =$$

$$= \sum \sum \phi(a_i b_j)x^{i+j} = \Phi(\sum \sum a_i b_j x^{i+j}) = \Phi((\sum a_i x^i) * (\sum b_i x^i))$$

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 essense 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 reagards 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 expresset 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

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

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

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 $\sum_{i=1}^{n-1} bc(n,i)x^i = g(x+y, xy)$ 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 pollynomials 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 $\overline{\alpha} = a - bi - cj - dk$.

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

$$(a+bi+cj+dk) * (a-bi-cj-dk) =$$

$$= a^2 - abi - acj - adk + abi + b^2 - bicj - bidk + acj - cjbi + c^2 - cjdk + adk - dkbi - dkcj + d^2 =$$

$$= a^2 - abi - acj - adk + abi + b^2 - bck + bdj + acj + bck + c^2 - cdi + adk - bdj + cdi + d^2 =$$

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

as desired.

(b) Prove that $\alpha\overline{\alpha} = 0$ 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 $\alpha\overline{\alpha} = q = a^2 + b^2 + c^2 + d^2$. We then follow that

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

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

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

and

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

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

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.*

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

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

Proof goes along the samy 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 $b = 0$ and $c = 0$. 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 assunming that there's a typo there (in the text of the theorem we even see the word "implication")

Now let us prove a somewhat trivial, but useful theorem. Suppose now that $f : R \to R'$ is an injective ring homomorphism, and R' is an integral domain. We can follow that if a, b are such that

$$a * b = 0$$

then

$$f(a) * f(b) = 0$$

and thus $f(a) = 0$ or $f(b) = 0$ since R' is an integral domain. Since f is injective we follow that $f(a) = 0 \Rightarrow a = 0$ or $f(b) \Rightarrow b = 0$, which implies that R is also an integral domain. Therefore

Theorem: If $f : R \to R'$ is an injective ring homomorphism, and R' is an integral domain, then R is an integral domain as well.

We don't have the same thing going on with fields, sinse for example identity for $f : Z \to R$ is injective, but Z is not a field. If f is a bijection though, then we can follow that R is a field.

3.3.1

Let m be a positive integet.

(a) Prove that Z/mZ is an integral domain if and ony 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 ony 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) $Z[i]$

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 mutliplicative, we follow that it's not a field. Same is true for the next point, but it is also not an intefral domain.

3.3.4

Let R be a commutative ring. Prove that R is an integral domain if and only of 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 multipication 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 $R = Z/6Z$. 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

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

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

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

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

$$= k^6 + 1 + k^6 + 1 + k^6 + 1 = 3k^6 + 3$$

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

thus we follow that

$$3k^6+3 = k^6+1$$

$$3(k^6+1) = k^6+1$$

thus

$$3 = 1$$

3.3.9

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

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 cancelation property.

(b) Let $p \in Z$ be a prime and let $k \geq 1$. Describe all of the nilpotent elements in Z/p^kZ

Skipped the rest of the exercises for later.

3.4 Unit groups and Product rings

3.4.1

(a) Compute the unit group 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 Q^*

All of the Q^* is the unit group.

(c) Compute the unit group $Z[i]^*$

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 deriviation 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 $(Z/pZ)^*$ for each of the primes $7, 11, 13$. Which ones are cyclic?

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

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

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

We follow that

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

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

We follow that

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

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

We follow that

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

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

3.4.4

Let $R_1, ..., R_n$ be rings.

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

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

(b) Yeah, projection is a homomorphism

Skip the rest

3.4.5

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

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

$$0 \to (0,0)$$

$$1 \to (1,1)$$

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

$$2 \to (0,2)$$

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

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

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

From this we can follow that the first index of value of our function in $Z/2Z \times Z/3Z$ 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 os 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 intself, and hence is prersent in the thing. Associativity is taken care of my 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 distibutivity 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

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

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

is a ring isomorphism.

Under assumtion 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 homomorhism.

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 whathot, 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 $\alpha = a_1 e_1 + a_2 e_2$.

Something tells me that we can use $\langle 1, 0\rangle$ and $\langle 0, 1\rangle$ as our e_1 and e_2 respectively. We then follow that if $\alpha \in R_1 \times R_2$, then it's in the form $\langle a, b\rangle$, which in turn implies that we can take

$$a * e_1, +b * e_2$$

to be our value. The fact that this factorization is unique is kinda trivial

3.4.9

We use a symbol L to define a ring

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

where definition 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) Fint 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. Identites are mapped pretty easily,

$$0 \to (0, 0)$$

$$1 \to (1, 1)$$

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.

$$f((1-L)(1-L)) = f(1-L-L+L^2) = f(2-2L) = (0,4)$$
$$f((1-L)(1-L)) = (0,2) * (0,2) = (0,4)$$

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

$$f((a+bL) * (c+dL)) = f((ac+bd) + (ad+bc)L) = (ac+bd+ad+bc, ac+bd-ad-bc)$$

$$f(a+bL) * f(c+dL) = (a+b, a-b) * (c+d, c-d) = (ac+ad+bc+bd, ac-ad-bc+bd)$$

so we're kinda shafted in this regard. Maybe the f is not a bijection then. It's ceirtanly 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 $R_1, R_2, ...$ 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 fromm the fact that the ring that is there's an inection 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 identitites 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 defnition 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 procuts 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 $+ : R/I \times R/I \to \mathcal{P}(R)$ $* : R/I \times R/I \to \mathcal{P}(R)$ 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 wont work after all. Defining product as a sum of products (as with ideals) might solve the problem, but I wont 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 $a' + b' = w$.

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 caseif 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 identitty

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

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 deriviations 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

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

Prove thaht $Rad(I)$ is an ideal of R.

Let $a \in Rad(I)$ and $b \in R$. We follow that there's $n \in \omega$ such that $a^n \in I$ by definition of $Rad(I)$. 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 $a \in Rad(I)$. 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 $a^m = a^n a^{n-i}$ 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 $a, b \in Rad(I)$ 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 $a + b \in Rad(I)$.

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

3.5.4

The goal of this exercise is to prove that every iideal 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 contradictions

(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 of $a-a' \in I$.

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 thsus $a - a' \in I$.

If $a - a' \in I$, then we follow that there's and 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

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

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

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

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

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

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 exacly 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 $\overline{r(x)} = r(\bar{i})$, 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 $\overline{a}$, i.e.

$$R \to R/I : a \to \overline{a}$$

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

$$\phi : R[x] \to (R/I)[x], \phi(\sum a_i x^i) = \sum \overline{a_i} x^i$$

by reducing the coefficieents 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:

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

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

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

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

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

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

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 $R = Z[x]$, and let I and J be the ideals

$$I = 2Z[x] + xZ[x], J = 3Z[x] + xZ[x]$$

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 $a_1 b_2 = 3x$, $a_2 b_1 = -2x$ 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 procuts, 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

$$\{\textit{ideals of } R \textit{ that contain } I\} \to \{\textit{ideals of } R/I\}, J \to J/I$$

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 element, 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 $n \in Z$, which implies thaat $1 \in J$, which in turn implies that $J = Z[x]$, as desired.

3.6.2

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

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

3.6.4

Let R be a ring, let $b, c \in R$, and let $E_{b,c} : R[x, y] \to R$ be the evaluation homomorphism as described in 3.13

(a) If R is an integral domain, prove that $\ker(E_{b,c})$ is a prime ideal of $R[x, y]$.

We firstly follow that since $E_{b,c}$ is a ring homomorphism, that $\ker(E_{b,c})$ is an ideal. Now let $q, w, e \in R[x, y]$ are such that $e \in \ker(E_{b,c})$ and

$$q * w = e$$

we follow that

$$E_{b,c}(q * w) = E_{b,c}(e) = 0$$

$$E_{b,c}(q) * E_{b,c}(w) = 0$$

since R is an integral domain, we follow that $E_{b,c}(w) = 0$ or $E_{b,c}(q) = 0$, which implies that $E_{b,c}(w) \in \ker(E_{b,c})$ or $E_{b,c}(q) \in \ker(E_{b,c})$, which implies that $\ker(E_{b,c})$ is a prime domain, as desired.

(b) If R is a field, prove that $\ker(E_{b,c})$ is a maximal ideal of $R[x, y]$.

We can try to use our fancy theorem from the cahpter this time. Presume that R is a field. We can follow that we can define an injective

$$\phi : R[x, y]/\ker(E_{b,c}) \to R$$

we then follow that $\phi(x) = x$ for all $x \in R$ which implies that ϕ is surjective, thus making ϕ an isomorphism, and thus $R[x, y]/\ker(E_{b,c})$ is a field, therefore $\ker(E_{b,c})$ is a maximal ideal, as desired.

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

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

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 $g(\alpha) = 0$. 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), simpliest proof of that comes from the fact that by multiplying any given element by that thing gives us a tuple, that constists 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

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

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

Suppose that there are $a, b, c \in Q$ 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

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

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

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

$$(2bb' + a'b\sqrt{2} + bc'\sqrt{6} + 3b\sqrt{3}d')+$$
$$(3cc' + c\sqrt{3}a' + cb'\sqrt{6} + 3c\sqrt{2}d')+$$
$$(6dd' + d\sqrt{6}a' + d2\sqrt{3}b' + 3d\sqrt{2}c') =$$

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

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

(a) 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 thaht $q^2 = 1$ and such that q is distinct from 1 and -1. We follow that

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

thus

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

F is an integral domain, this we have 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.

(b) As a follow-up to (a), let $m \geq 2$ be an integer, that need not be prime. Prove that

$$\prod_{a \in (Z/mZ)^*} a = \pm 1$$

Suppose that $a \in (Z/mZ)^*$. We can follow that since $(Z/mZ)^*$ is a group under multiplication, that there is $a^{-1} \in (Z/mZ)$. Thus we can once again partition the whole set into pairs/singletons, and if

$$a = a^{-1}$$

then

$$a^2 = 1$$

the difference between this exercise and the previous point is that we can't state that

$$a^2 - 1 = 0 \Leftrightarrow a = \pm 1$$

since $(Z/mZ)^*$ is not an integral domain and thus

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

does not give us that $a - 1 = 0$ or $a + 1 = 0$. And thus we have nothing.

We can try to generalize this case and ask the question of what exactly is the product of all of elements in the finite group. We then have the problem that we can't adequatly generalize what exactly -1 is in this case is, since it's just an additive inverse of the multiplicative identity, and there is nothing special about it in the context of the multiplicative group.

We can follow though that the square of the lhs is 1 by the fact that then we can partition the elements into pairs of elements and its inverses (where the case with the $a = a^{-1}$ resolves into giving us a pair with identical elements). Thus we have that

$$(\prod_{a \in (Z/mZ)^*} a)^2 = 1$$

and therefore

$$\prod_{a\in(Z/mZ)^*} (a^2) = 1$$

Let $j \in (Z/mZ)^*$ be such that

$$\prod_{a\in(Z/mZ)^*} a = j$$

and assume that $j \neq \pm 1$. We follow that since $j \in (Z/mZ)^*$ that

$$\prod_{a\in(Z/mZ)^*\setminus\{j\}} a = 1$$

we can also follow that $j \in (Z/mZ)^*$ implies that $j^{-1} \in (Z/mZ)^*$, and thus

$$j^{-1} \prod_{a\in(Z/mZ)} a = 1$$

by taking away the elements of the lhs of the former equation from lhs on the latter equation we get that

$$j^{-1} j = 1$$

which gives us absolutely nothing.

Maybe induction then? We can follow that this thing is true for 2, thus if

$$\prod_{a\in(Z/nZ)^*} a = \pm 1$$

we follow that in Z there is $k \in Z$ such that

$$\prod_{a\in(Z/nZ)^*} a = nk \pm 1$$

and thus $(Z/nZ)^*$ and $(Z/(n+1)Z)^*$ don't have much in common, thus giving us absolutely nothing.

We can follow that $m-1$ is always in $(Z/mZ)^*$ by following that

$$(m-1)^2 = m^2 - 2m + 1 \equiv 1$$

Maybe we should go back a bit. If

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

we follow that in Z we have that there is $k \in Z$ such that

$$(a-1)(a+1) = mk$$

and thus

$$a^2 - mk - 1 = 0$$

we then follow that

$$a^2 = mk + 1$$
$$a = \pm\sqrt{mk+1}$$

which does not appear to give us much.

For small cases (i.e. $m = 2, 3, ..$) we have that

$$1 = 1$$
$$1 * 2 = 2 \equiv -1 \mod 3$$
$$1 * 3 = 3 \equiv -1 \mod 4$$
$$1 * 2 * 3 * 4 = 24 \equiv -1 \mod 5$$
$$1 * 5 = 5 \equiv -1 \mod 6$$
$$1 * ... * 7 \equiv -1 \mod 7$$
$$1 * 3 * 5 * 7 = 105 \equiv 1 \mod 8$$

We know that the answer should be ± 1, which kinda means that we might be having squares lying around in this thing. Suppose that $j \in (Z/mZ)$. Assume also that $j^2 = 1$. Can we follow that $j = \pm 1$? Well, we can't since for example in $(Z/8Z)$ we have that $3^2 = 9 \equiv 1$, and $3 \neq \pm 1$.

After some careful search for hints on the internet, I got an idea to pair up elements that procude -1. Let $a \in (Z/mZ)^*$. We can follow that if $a * b = -1$, then there is $a^{-1} \in (Z/mZ)^*$, and thus

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

can $a = -a^{-1}$ then? If $a = -a^{-1}$, then $a^2 = -1$, thus $a^2 + 1 \equiv 0 \mod m$. We follow that the order of a is 4 in this case.

Suppose that $a \in (Z/mZ)^*$. We follow that $-a * -(a^{-1}) = 1$, and thus $-a \in (Z/mZ)^*$. We can also follow that $a = -a \Rightarrow 2a = 0 \Rightarrow a \notin (Z/mZ)^*$. Thus we can pair up $(a, -a)$ with $a \neq -a$.

Therefore let us look at $(Z/mZ)^*$. We can divide this set into two subsets: elements that are equal to its inverse, and the ones that aren't. If an element a is equal to its inverse, then $(-a)^2 = 1$, and thus $-a \neq a$ and $-a$ is also present and not equal to its inverse, and thus we can pair up $(a, -a)$, whose product is -1. If an element is not equal to its inverse, then we can pair this element with its inverse. Thus we have a set of pairs, whose individual product is either 1 or -1, which implies that the product of the entire set is ± 1, as desired.

5.3.6

(a) is pretty much just checking, and the answer to (b) is the fact that F_4 is a field, and $(Z/4Z)$ is not an integral domain, let alone a field.

5.4 Subfields 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 $f * 1 = k$, 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 fiels 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 $\alpha_1, ...\alpha_n \in K$ such that

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

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-fector space, and proved that C is linearly independent. Prove that C is a spanning set

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

$$l = \sum c_i b_i$$

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

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

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 addntion between a random element of omega (or $-\infty$) with $-\infty$ in an obvious manner.

Another thing that is clear here is the fact that $F[x]$ is an integral domain. We can also follow that if R is an integral domain, then by the same idea $R[x]$ is an integral domain as well.

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

$$f(x) = g(x)q_1(x) + r_1(x)$$
$$f(x) = g(x)q_2(x) + r_2(x)$$

we follow that

$$g(x)q_1(x) + r_1(x) - (g(x)q_2(x) + r_2(x)) = f(x) - f(x) = 0$$

$$g(x)q_1(x) + r_1(x) - (g(x)q_2(x) + r_2(x)) = 0$$
$$g(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x)) = 0$$
$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

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 reductible. Equivalently irreductible polynomials dont have roots. Reverse is not necessarily true, we can have rootless reductible 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 irreductible

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 irreductible if and only if it has no roots in F.

Irreductibility 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 reductible, 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 irreductible 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 irreductible 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 reductible, 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 degreee 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.

(e) Let $f = x^4 + 4$. Prove tht f is reductible 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 irreductible 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

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

and then substract 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 remainter

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

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 mmove forward to actually do that

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

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

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

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

be a polynomial of degree $d \ge 1$

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

We follow that

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

and thus

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

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

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

$$0 = c_0 + a \sum_{1 \le i \le d} c_i a^{i-1} b^{-i}$$
$$-c_0 = a \sum_{1 \le i \le d} c_i a^{i-1} b^{-i}$$
$$-c_0 b^d = a b^d \sum_{1 \le i \le d} c_i a^{i-1} b^{-i}$$
$$-c_0 b^d = a \sum_{1 \le i \le d} c_i a^{i-1} b^{d-i}$$

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 dont have any common primes as multiples, which implies that

$$a | c_0$$

as desired.

We can then do similar trich with c_d to get

$$0 = f(a/b) = \sum_{0 \le i \le d} c_i a^i b^{-i} = c_d b^{-d} + \sum_{0 \le i \le d} c_i a^i b^{-i}$$
$$0 = c_d a^d b^{-d} + \sum_{0 \le i \le d-1} c_i a^i b^{-i}$$
$$0 = c_d a^d + b^d \sum_{0 \le i \le d-1} c_i a^i b^{-i}$$
$$-c_d a^d = b^d \sum_{0 \le i \le d-1} c_i a^i b^{-i}$$
$$-c_d a^d = b \sum_{0 \le i \le d} c_i a^i b^{d-1-i}$$

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

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

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 irreductible

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 irreductible 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

Firstly, let us check that I is indeed an ideal. For addition we have

$$(x-a)g(x,y) + (y-b)h(x,y) + (x-a)g'(x,y) + (y-b)h'(x,y) =$$

$$= (x-a)g(x,y)g'(x,y) + (y-b)h(x,y)h'(x,y) \in I$$

and for multiplication we follow that

$$q(x,y)((x-a)g(x,y) + (y-b)h(x,y)) = (x-a)q(x,y)g(x,y) + (y-b)q(x,y)h(x,y)$$

thus we have that I is indeed an ideal.

Since $f(a,b) = 0$ we follow that

$$f(a,b) = \sum q_c a^i b^j = 0$$

and thus

$$f(x,y) = f(x,y) - f(a,b) = \sum q_c x^i y^j - \sum q_c a^i b^j = \sum q_c x^i y^j - q_c a^i b^j = \sum q_c (x^i y^j - a^i b^j) =$$

We can follow that if $q \in I$, then $q = (x-a)g(x,y) + (y-b)h(x,y)$ for some $g, h \in F[x,y]$, and for it we have

$$q(a,b) = 0 * g(a,b) + 0 * h(x,y) = 0$$

thus proving that $I \subseteq \ker(E_{a,b})$.

We can fudge around a bit in order to get ourselves closer to the right idea:

$$f(x,y) = x + y - a - b = (x-a) + (y-b)$$

$$f(x,y) = x^2 + y^2 - (a^2 + b^2) = (x^2 - a^2) + (y^2 - b^2) = (x-a).. + (y-b)...$$
$$f(x,y) = x^2 + y^2 + xy - (a^2 + b^2 + ab) = (x^2 - a^2) + (y^2 - b^2) + (xy - ab) =$$
$$= (x-a)(x+a) + (y-b)(y+b) + (xy - ab) =$$
$$= (x-a)(x+a) + (y-b)(y+b) + (xy - ab - ay + bx + ay - bx) =$$
$$= (x-a)(x+a) + (y-b)(y+b) + (xy - ab - ay + bx) + (ay - bx) =$$
$$= (x-a)(x+a) + (y-b)(y+b) + (x-a)(y+b) + (ay - bx) = ...$$

Which seems to be boiling down to the question of how does $f(x,y) = xy - ab$ factor in the desired way? Let's then try to fudge around with this one:

$$(x-a) * y + (y-b) * x = xy - ay + xy - bx$$

this one is a non-starter

$$(x-a)(y+b) + (y-b) * (x+a) = xy - ay + xb - ab + xy - bx + ay - ab =$$

$$= xy - ay + xb - ab + xy - bx + ay - ab = 2xy - 2ab$$

which is hell of a lot closer. Thus we have that

$$1/2(x-a)(y+b) + 1/2(y-b) * (x+a) = xy - ab$$

which is dope. This lets us conclude that $xy - ab \in I$. Next task is to push it into the higher degree:

$$f(x,y) = x^2y^2 - a^2b^2 = (xy)^2 - (ab)^2 = (xy - ab) * (xy + ab)$$

We then know that the lhs of the latter product is in I, which implies that the whole thing is in I. In general we have that

$$x^n y^n - a^n b^n = (xy)^n - (ab)^n = (xy - ab) * \sum ...$$

just as with the single variable polynomial (look up an exercise in 3rd chapter with polynomial evaluation to get details), which proves that

$$x^n y^n - a^n b^n \in I$$

which is cool as heck. This case tackles only polynomials where we have equal degrees for x and y, but polynomials of two variables have unequal ones as well. For example there is a polynomial

$$f(x,y) = x^2 y - a^2 b$$

that exemplifies this case. Let's try to solve this one then:

$$x^2y - a^2b$$

after some fudging around with maxima I got that

$$x^2y - a^2b = (x + a)(xy - ab) - ax(y - b)$$

we know that $(xy - ab)$ is an element of I, latter part of the sum (i.e. $ax(y - b)$) is in I by definition, thus the whole thing is in I. Generalizing this thing is not going to be trivial. We can follow that x^iy^j is a term of a sum in $(x - y)^{i+j}$. Fudging around a bit more we get that

$$x^{n+1}y^n - a^{n+1}b^n = (x - a) * (x^ny^y - a^nb^n) + a * x * (x^{n-1} * y^n - a^{n-1}b^n)$$

which by induction gives us that

$$x^{n+1}y^n - a^{n+1}b^n \in I$$

We then follow that

$$(x^2y + a^2b) * (x - a) + ax(xy - ab) = x^3y - a^3b$$

and in general

$$x^{n+1}y - a^{n+1}b = (x - a)(x^n * y + a^n * b) + ax(x^{n-1}y - a^{n-1}b)$$

which by induction gives us that for arbitrary n we follow that $x^ny - a^nb \in I$

In way more general sense we get

$$x^ny^m - a^nb^m = (x - a) * (x^{n-1}y^m + a^{n-1}b^m + ax(x^{n-2}y^m - a^{n-2}b^m)$$

thus for an arbitrary $i > j$ we can get up to

$$x^jy^j - a^jb^j \in I$$

with a point that was made a couple of paragraphs ago, and then by using this formula by induction we get that

$$x^iy^j - a^ib^j \in I$$

with some notation we can get the same case for $i < j$ as well.

Thus we can get back to our main point. If $f(a, b) = 0$ for some $a, b \in F$, then

$$f(x, y) = f(x, y) - f(a, b) = \sum q_cx^iy^j - \sum q_ca^ib^j \sum q_cx^iy^j - q_ca^ib^j = \sum q_c(x^iy^j - a^ib^j)$$

each $x^i y^j - a^i b^j$ is in I, thus $q_c(x^i y^j - a^i b^j) \in I$, therefore the whole sum is in I, and thus $f(x,y) \in I$, which proves that $I = \ker E_{a,b}$, and since our $f(x,y) \in \ker E_{a,b}$ by definition, we get the first inclusion (not proper inclusion though).

We then follow that $I \subset R$ (where R is presumed to be $F[x,y]$) with proper inclusion, since R can have arbitrary polynomials, whose root is not a, b (for example constant polynomials), that aren't present in I.

Thus the last thing that is leftto prove is proper inclusion of $f(x,y)F[x,y]$ in I. If f is a zero polynomial, then we follow that $f(x,y)F[x,y] = \{0\}$, and since I has nonzero polynomials in it, we follow proper inclusion. f cannot be a constant nonzero polynomial (i.e. a number) since it's got roots. Thus let m and n be the highest powers of x and y respectively in $f(x,y)$. We follow that at least one of those is greater than 0 (assume with no loss in generality that it is m), and thus every polynomial in $f(x,y)F[x,y]$ is either 0 or its power of y is greater or equal than m. Polynomials in I can have no powers in y (simple $(x-a)$ will do as an example), and thus we conclude that this polynomial is not a multiple of f, thus giving us proper inclusion, as desired.

Skipping the rest of this exercise

5.6.5

The mathematical term for the property that at non-constant polynomials have at least one roots is 'algebraically closed'.

(a) Proe that the only irreductible polynomials in $C[x]$ are linear polynomials.

If $C[x]$ is a polynomial of degree two or more, then it's got a root a, and thus can factor into $(x-a)g(x)$ for some polynomial $g(x)$.

(b) Let $f(x) \in R[x]$ and suppose that $a + bi \in C$ is a root of $f(x)$. Prove that $a - bi$ is also a root of $f(a)$

Follows directly from the fact that $\overline{a}\overline{b} = \overline{ab}$.

(c) Let $f(x) \in R[x]$ be an irreductible polynomial in $R[x]$. Prove that $\deg(f) \leq 2$

We can follow that there is $a \in C$ such that $f(a) = 0$. If $a \in R$, then we're done, thus assume that $a \notin R$. From previous point we get that $f(\overline{a}) = 0$. Thus

$$f(x) = (x-a)(x-\overline{a})g(x)$$

and thus

$$f(x) = (x^2 - x\overline{a} - xa + |a|^2)g(x) = (x^2 - x(\overline{a}+a) + |a|^2)g(x)$$

we then follow that $\overline{a} + a \in R$, and thus lhs is in R as well, thus producting the desired result.

5.6.6

Let F be a field, let $f(x) \in F[x]$ be a possibly reductible non-constant polynomial, and let $\deg(f) = d$.

(a) Prove that there exists a field extension K/F satisfying $[K : F] \leq d$ such that $f(x)$ has a root in K

If f has roots in F, then we're done, thus assume that it does not have them.

If $f(x)$ is irreductible then let $g(x) = f(x)$, and otherwise let $g(x)$ be an irreductible factor of f (we can follow that those exist since all the linear polynomials are irreductible, and $\deg(f) \geq 1$). We then follow that we have that $\deg(g) \leq \deg(f)$, and since g is irreductible by theorem 5.27 we have that there is an extension field K of F such that it's got roots for g. Since g is a factor for f we follow that the same root is also a root for f, and we also have that

$$[K_f : F] = \deg(g) \leq \deg(f)$$

as desired.

(b) Prove that there exists a field extension L/F and elements $c \in F$ and $\alpha_1, ..., \alpha_d \in L$ such that

$$f(x) = c(x - \alpha_1)(x - \alpha_2)...(x - \alpha_d)$$

(α's need not be distinct). Prove that it is always possible to find such an L that also satisfies

$$[L : F] \leq d!$$

The field L is called a splitting field for the polynomial $f(x)$ oveer the field F.

From previous point we follw that there is K/F such that

$$[K : F] \leq d$$

and such that $f(x)$ has a root α_1 in K. We then follow that there is $g(x)$ such that

$$f(x) = (x - \alpha_1)g(x)$$

Then we can follow that $\deg(g(x)) = \deg(f(x)) - 1$, and by applying the same logic we follow by induction that there is a desired field.

5.7 Finite Fields

5.7.1

Let F be a finite field with q elements

(a) Prove taht 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 muultiplication, 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 precicely $q - 1$. 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 Z.

Suppose that m divides n. Definition states that there exists $k \in N_+$ such that $n = mk$. Thus

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

and thus

$$(x^m - 1) * \sum_{0 \le i \le k-1} x^{im} = \sum_{0 \le i \le k-1} x^{im} * (x^m - 1) = \sum_{0 \le i \le k-1} x^{(i+1)m} - x^{im} =$$

$$= \sum_{0 \le i \le k-1} x^{(i+1)m} - \sum_{0 \le i \le k-1} x^{im} = \sum_{1 \le i \le k} x^{im} - \sum_{1 \le i \le k-1} (x^{im}) - 1 =$$

$$= x^{km} + \sum_{1 \le i \le k-1} x^{im} - \sum_{1 \le i \le k-1} (x^{im}) - 1 = x^{km} - 1$$

as desired (deriviation 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

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

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

$$x^n + x^m g(x) - x^{n-m} - g(x) = x^n - 1$$

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

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

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 m, 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.

The rest of this section is marked as TODO

Chapter 6

Groups - Part 2

6.1 Normal Subgroups and Quotient Groups

Notes

With definition of G/H in terms of a set of cosets of H we note that the Lagrange's Theorem can be rephrased as

$$|G/H| = |G|/|H|$$

6.1.1

Let $\psi : G \to G'$ be a homomorphism of groups.

(a) Prove that the image of ψ is a subgroup of G'

We can follow that if $h', g' \in \psi[G]$, then there are by definition $h, g \in G$ such that

$$\psi(h) = h', \psi(g) = g'$$

thus

$$\psi(h^{-1} g) = \psi(h^{-1})\psi(g) = \psi(h)^{-1} \psi(g) = h'^{-1} g$$

as desired.

(b) Suppose that G is a finite group. Prove that

$$|G| = |\ker(\phi)| * |\phi[G]|$$

Let $a * \ker(\phi)$ be a left coset of G. We follow that if $q \in a * \ker(\phi)$, then there is $b \in \ker(\phi)$ such that

$$q = a * b$$

and thus

$$\phi(q) = \phi(a * b) = \phi(a) * \phi(b) = \phi(a) * 1 = \phi(a)$$

Thus we can follow that different element of the same cosets are sent to the same element of G' , which implies that there is a bijection between a set of cosets, and elements in the range of $\phi[G]$. Thus there is by definition the same number of elements of $\phi[G]$ and cosets of $\ker(\phi)$. Then Lagrange's theorem implies the desired conclusion

6.1.2

Let G be a group, and let $H \subseteq G$ be a subgroup.

(a) Suppose that $g^{-1}Hg \subseteq H$ for all $g \in G$. Prove that H is a normal subgroup of G.

Fix $g \in G$ and let us assume that

$$g^{-1}Hg \subseteq H$$

we can also follow that by our assumptions we've got that

$$gHg^{-1} \subseteq H$$

Now let $h \in H$. We want to prove that there is $h' \in H$ such that

$$h = g^{-1}h'g$$

we follow that

$$h' = ghg^{-1}$$

thus $h' \in gHg^{-1}$, and since $gHg^{-1} \subseteq H$ we follow that $h' \in H$, as desired.

(b) Let $g \in G$. Prove that $g^{-1}Hg$ is a subgroup of G

Since $e \in H$, we follow that

$$e = g^{-1}g = g^{-1}eg \in h^{-1}HG$$

We can also follow taht if $q, w \in g^{-1}Hg$, then there are $h, h' \in H$ such that

$$q = g^{-1}hg, w = g^{-1}h'g$$

then

$$q^{-1}w = g^{-1}hgg^{-1}h'g = g^{-1}hh'g$$

and since $hh' \in H$ we conclude that $q^{-1}w \in g^{-1}Hg$, thus making $g^{-1}Hg$ a subgroup

(c) Let $g \in G$. Prove that the following map is a group isomorphism:

$$H \to g^{-1}Hg, h \to g^{-1}hg$$

Multiplication by an element is injective, and definition of $g^{-1}Hg$ implies that the map is surjective, thus making the map bijective.

We can also see that

$$\psi(ab) = g^{-1}abg = g^{-1}aebg = g^{-1}agg^{-1}bg = \psi(a)\psi(b)$$

as desired

(d) If H is finite. prove that every conjugate of H has the same number of elements as H

Bijection in the previous point implies that

6.1.3

Skip

6.1.4

Prove that every subgroup of the quaternion group is normal

Quaternion group has 8 elements, which implies that its only subgroups are of order $1, 2, 4, 8$. We then follow that 1 and 8 are trivial and the entire group respectively, the only group of order 2 is $\{\pm 1\}$, and thus the only order that is left is 4. We then follow that the only groups of order 4 are in the form

$$\{\pm 1, \pm x\}$$

where $x \in \{i, j, k\}$. After this we can proceed with a simple enumeration, that we're gonna skip, which implies the desired result

6.1.5

Let G be a group and let $H \subseteq G$ be a subgroup of G of index 2. Prove that H is a normal subgroup of G.

Suppose that there is an element $g \in G$ such that there exists $h \in H$ so that $g^{-1}hg \notin H$. We then follow that if $g^{-1}h \in H$, then $g^{-1} \in H$, and thus $g \in H$ and $g^{-1}hg \in H$, which is a contradiction, and thus $g, g^{-1} \notin H$. This implies that $g^{-1}H, gH \neq H$, and thus we follow that $g^{-1}hg \in gH$. Thus there is $h' \in H$ such that

$$g^{-1}hg = g^{-1}h'$$

$$hg = h'$$

$$g = h^{-1}h'$$

which implies that $g \in H$, which is a contradiction. Thus we conclude that there is no element $g \in G$ such that there is $h \in H$ so that $g^{-1}hg \notin H$. This implies that for all $g \in G$ and all $h \in H$ we have that

$$g^{-1}hg \in H$$

which implies that

$$g^{-1}Hg \subseteq H$$

which implies the desired result. (did this one een without a hit, what a rush)

6.1.6

Let G be a group, let $H \subseteq G$ and $K \subseteq G$ be subgroups, and assume that K is a normal subgroup of G

(a) Prove that $HK = \{hk : h \in H, k \in k\}$ is a subgroup of G

We can follow that $e \in H$ and $e \in K$, and thus $e = e * e \in HK$. Now let $q, w \in HK$. We folllow that they can be deconstructed to $q = hk, w = h'k'$. We then conclude that

$$qw^{-1} = hk(h'k')^{-1} = hkk'^{-1}h'^{-1} = hekk'^{-1}h'^{-1} = hh'^{-1}h'kk'^{-1}h'^{-1} = hh'^{-1}(h'kk'^{-1}h'^{-1})$$

We then can see that $hh'^{-1} \in H$ and by the fact that K is normal we follow that $(h'kk'^{-1}h'^{-1}) \in K$, which implies that the whole thing is in HK, as desired.

(b) Prove that $H \cap K$ is a normal subgroup of H and that K is a normal subgroup of HK

We can follow that $H \cap K$ is a subgroup of H by properties of subgroups. Let $h \in H$ and $q \in H \cap K$ be arbitrary. We follow that $h^{-1}qh \in H$ by the fact that it's a product of elements of H, and $h^{-1}qh \in K$ by the fact that K is normal subgroup of G. Thus $h^{-1}qh \in H \cap K$, which means that $H \cap K$ is a normal subgroup of H, as desired

K is a normal subgroup of G, and thus it's a normal subgroup of any subgroup that contains it by a pretty straightforward application of definition.

(c) Prove that HK/K is isomorphic to $H/(H \cap K)$

We can follow that $f_1 : H \to HK$ defined by identity is a homomorphism, and since K is a normal subgroup of HK we can follow there is a homomorphism $f_2 : HK \to HK/K$. Thus there is a homomorphism $f_3 : H \to HK/K$. We follow that if $q \in H \cap K$, then $q \in K$, and thus

$$f_3(q) = qK = K = f_3(0)$$

If $w \in H \setminus K$,then

$$f_3(w) = wK \neq K = f_3(0)$$

which implies that $H \cap K$ is a kernel of f_3. Thus we can define $f_4 : H/(H \cap K) \to HK/K$, which will be an injective homomorphism. We can also follow that if $C \in HK/K$, then there is $q \in HK$ where $q = hk$ such that

$$C = qK = hkK = hK = f_4(h(H \cap K))$$

which implies that f_4 is surjejctive, and thus it is bijective, which implies the desired result.

(d) Skip

6.1.7

Let G be a group, let $K \subseteq H \subseteq G$ be subgroups, and assume that K is normal.

(a) Prove that H/K is naturally a subgroup of G/K

We can follow that if $C \in H/K$, then there is $h \in H$ such that $C = hK$, and since $H \subseteq G$ we follow that $C \in G/K$, which implies that $f : H/K \to G/K$ defined as an identity with the expanded codomain is an injective homomorphism

(b) Conversely, prove that every subgroup of G/K looks like H/K for some subgroup H satisfying $K \subseteq H \subseteq G$

Let $Q \subseteq G/K$ be a subgroup. We follow that each $q \in Q$ is of the form $q = gK$ for some $g \in G$. We then can unionize Q in order to get

$$H = \bigcup Q$$

we then follow that if $w, r \in H$, then there are cosets $wK, rK \in Q$, and since Q is a group there is $w^{-1} inK$. Thus

$$w^{-1} KrK = w^{-1} rK \in Q$$

this implies that $w^{-1} rK \subseteq H$, and thus

$$w^{-1} re = w^{-1} r \in H$$

which implies that H is a subgroup of G. We also follow that since Q is a group that $eK = K \in Q$, which implies that $K \subseteq H$. Then we follow that if $q \in Q$, then there for all $t \in q$ we have that $q = tK$. Thus $t \in H$ and therefore $tK \in H/K$, which implies that $Q \subseteq H/K$. Similar argument shows the inverse inclusion, which implies the desired result.

(c) Prove tha H is a normal subgroup of G if and only if H/K is a normal subgroup of G/K

Assume that H is normal, and let $gK \in G/K, hK \in H/K$. We follow that

$$g^{-1} KhKgK = (g^{-1} hg)K$$

since h is normal we follow that $(g^{-1} hg) \in H$ and this implies that H/K is normal.

Assume that H/K is normal. We follow that if $g \in G, h \in H$, then

$$g^{-1} hg \in g^{-1} hgH = g^{-1} HhHgH = g^{-1} HgH = H$$

which implies that H is normal

(d) If H is a normal subgroup of G, prove that

$$\frac{G/K}{H/K} \cong G/H$$

There's a surjective homomorpshism $f_1 : G \to G/H$ with kernel H, and since $K \subseteq H$ we follow that there is a surjective homomorphism $f_2 : G/K \to G/H$.

Let $q \in G/K$. If $q \in H/K$, then $q = hK$ for some $h \in H$ and thus

$$f_2(q) = f_2(hK) = f_1(h) = e$$

if $q \notin H/K$, then there is $g \in G \setminus H$ such that $q = gK$. Thus

$$f_2(q) = f_2(gK) = f_1(g) \neq 0$$

which implies that H/K is the kernel of f_2. This implies that there is an isomorphism $f_3 : \frac{G/K}{H/K} \to G/H$, which implies the desired result.

6.1.8

Let G be a group, let $K \subseteq G$ be a normal subgroup of G, and let $H \subseteq H' \subseteq G$ be subgroups of G.

(a) Finished this one before

(b) Prove that $H/(H \cap K)$ is naturally a subgroup of $H'/(H' \cap K)$

We can define $\phi : H/(H \cap K) \to H'/(H' \cap K)$ by

$$\phi(h(H \cap K)) = h(H' \cap K)$$

we then follow that if $h, h' \in h(H \cap K)$ then there is $k \in (H \cap K)$ such that $h = h'k$, and thus

$$h(H' \cap K) = h'k(H \cap K) = h'(H \cap K)$$

where the second definition is given by properties of cosets. Thus ϕ is well defined. The proof that ϕ is a homoomrphism is somewhat trivial, and we also have that if there are $h(H \cap K), h'(H \cap K)$ such that

$$\phi(h(H \cap K)) = \phi(h'(H \cap K))$$

then

$$h'(H' \cap K) = h'(H' \cap K)) \Leftrightarrow \exists k \in K : h' = hk \Rightarrow h(H \cap K)h(H' \cap K)$$

thus proving that ϕ is injective, as desired.

(c) Suppose further that H is a normal subgroup of H'. Prove that $H/(H \cap K)$ is a normal subgroup of $H'(H' \cap K)$.

There is a somewhat trivially followed with a lot of notation involved

6.2 Group Acting on Sets

Notes

Initial definition of the group action is a tad bit lacking, by action we denote a function $\cdot : G \times A \to A$ with all the axioms attached

Then, I want to follow some things. If $x, y \in A$ and $g \in G$, then we follow that

$$gx = gy$$

implies that

$$g^{-1}(gx) = g^{-1}(gy)$$
$$(g^{-1}g)x = (g^{-1}g)y$$
$$ex = ey$$
$$x = y$$

which implies that with fixed $g \in G$, our initial map is injective.

If $x \in A$ is fixed, then if $g_1, g_2 \in G$ we have

$$g_1x = g_2x$$
$$g_1{}^{-1}g_1x = g_1{}^{-1}g_2x$$
$$ex = (g_1{}^{-1}g_2)x$$

and we might not have cancelation properties here, so we're assuming that injectivity is not implied here.

Orbit is the image of an element of X, and the stabilizer is the values of G that leave particular $x \in X$ unchanged. Thus orbit is a subset of X and stabilizer is a subset of G. Both of them are indexed by a particular $x \in X$.

Now I want to re-word the proof of 6.19(b):

With fixed $x \in X$ our initial map becomes a function of G, whose range is the orbit of X. A union of the set of all orbits constitutes X (we have that $e * x = x$, which implies this). And on top of that, if there are two elements x, y such that

$$Gx \cap Gy \neq \emptyset$$

then there are $g_1, g_2 \in G$ such that

$$g_1x = g_2y$$
$$x = g_1{}^{-1}g_2y$$
$$x = (g_1{}^{-1}g_2)y$$

which means that $x \in Gy$ and $y \in Gx$.

If $q \in Gx$, then there is $g' \in G$ such that $q = gx \Leftrightarrow x = g^{-1}q$, and then we follow that if $r \in Gq$, then

$$(\exists g \in G)(r = gq) \Rightarrow (\exists g, g' \in G)(r = gg'x) \Rightarrow r \in Gx$$

thus $Gq \subseteq Gx$. By the similar logic if $r \in Gx$ then

$$(\exists g \in G)(r = gx) \Rightarrow (\exists g, g' \in G)(r = gg'q) \Rightarrow r \in Gq$$

which implies that $Gq = Gx$.

Combining our discovery into the previous point, we get that

$$Gy = Gx$$

which means that orbits of elements of X constitute partition of X This gives us a thing, that is similar to cosets: they can be indexed by any on their elements. Moreover, if we have $x \in X$, then $ex = x \in Gx$, which implies that $x \in Gy \iff Gy = Gx$

Let us also re-word the 6.19(c): *If G is a group that acts on X, then for every $x \in X$ there is a bijection*

$$\alpha : G/G_x \to Gx$$

such that

$$(\forall C \in G/G_x) : (\forall g \in C)(\alpha(C) = gx)$$

Proof: If $C \in G/G_x$ and $g, g' \in C$, then by definition of the coset for all $q \in C$ we have $C = qG_x$. Thus $C = gG_x = g'G_x$. This implies that there is $h \in G_x$ such that

$$g = g'h$$

and therefore

$$gx = g'hx = g'(hx) == g'x$$

where $hx = x$ is derived from the definition of G_x. This implies that

$$(\forall C \in G/G_x)(\forall g \in C)(\exists! y \in X)(gx = y)$$

which means that there is a function $\beta : G/G_x \to X$ that satisfies

$$(\forall C \in G/G_x)(\forall g \in C)(\beta(C) = gx)$$

Furthermore, since for every $C \in G/G_x$ we have that $\beta(C) = gx$ for some $g \in G$ we can follow that $\beta[G/G_x] \subseteq Gx$, and thus we can restrict its codomain to $\beta : G/G_x \to Gx$.

We then follow that if $q \in G_x$, then $qx = x$, and thus

$$\beta(G_x) = x$$

Moreover, if $g \in G$, then $g \in gG_x$, and thus by restriction on β we have that

$$\beta(gG_x) = gx$$

thus if $y \in Gx$, then there is $g \in G$ such that $y = gx$ by definition, and thus

$$\beta(gG_x) = gx = y$$

which implies that β is surjective.

Let $C_1, C_2 \in G/G_x$ and assume that $\beta(C_1) = \beta(C_2)$. We follow then that for all $g \in C_1$ and $g' \in C_2$ we have

$$gx = g'x$$

by definition of β. This gives us

$$x = g^{-1} g'x \Rightarrow g^{-1} g' \in G_x$$

Thus there is $r \in G_x$ such that $g^{-1} g' = r$, and therefore $g' = gr$. Therefore we conclude that

$$C_1 = g'G_x = grG_x = gG_x = C_2$$

which implies that β is injective, and thus we have the desired bijection.

6.2.1

Let $G = C_n$ be a cyclic group of order n, and let $X = \{x_1, ..., x_n\}$ be a set containing n elements. For each part, find an action of G on X that there is an element $x \in X$ having the indicated property

Firstly, for convenience's sake we note that every cyclic group of order n is isomorphic to Z/nZ, and thus we're gonna take $G = Z/nZ$. We're also gonna take $X = Z/nZ$ for some easy notation.

(a) The stabilizer is $G_x = \{e\}$

We can set $\times$ to be normal $+$, which gives this thing trivial.

We can also see that $|G|/|G_x| = |Gx|$, which knocks out point (d)

(b) The stabilizer is $G_x = G$

We can set

$$j \times x_i = x_i$$

same idea applies to point (c)

6.2.2

Let G be a group, let X be a set, and let S_X be the symmetry group of X. Let

$$\alpha : G \to S_X$$

be a function, and for $g \in G, x \in X$, let $g * x = \alpha(g)(x)$. Prove that this defined a group action if and only if α is a group homomorphism.

Suppose that this thing defines a group action. This means that we can define a function $\times : G \times X \to X$ by

$$g \times x = \times(g, x) = \alpha(g)(x)$$

with properties that

$$e \times x = \times(e, x) = x$$

and

$$(g * g') \times x = \times(g * g', x) = \alpha(g * g')(x) = \times(g, \times(g', x)) = \alpha(g)(\alpha(g')(x))$$

Thus for all $g, g' \in G, x \in X$

$$\alpha(gg')(x) = (gg') \times x = g(g' \times x) = \alpha(g)(\alpha(g')(x))$$

which gives us

$$\alpha(g * g') = \alpha(g) \cdot \alpha(g')$$

which proves that this thing is a homomorpism.

Now if α is a homomorphism, then

$$\alpha(e) = Id$$

and thus

$$\alpha(e)(x) = x$$

thus satisfying the first condition. We also have the same deriviation, but in reverse for the rest of conditions.

6.2.3

(a) Prove that G acts transitively in X if and only there is at least one $x \in X$ such that $Gx = X$.

Forward implication is handled by definition.

Suppose that there exists $x \in X$ such that $Gx = X$. This means that for all $y \in X$ there is $g \in G$ such that $gx = y \Leftrightarrow x = g^{-1} y$. Thus we follow that if $j \in X$, then there is $g' \in G$ such that $g'x = j$, and therefore $g'g^{-1} y = j$, thus implying that $j \in Gy$, thus implying that $X \subseteq Gy$, which gives us the desired result.

(b) Prove that G acts transitively on X if and only if for every pair of elements $x, y \in X$ there exists a group element $g \in G$ such that $gx = y$.

If G acts transitively, then if $x, y \in X$ we follow that $y \in X = Gx$, and thus there is $g \in G$ such that $y = gx$.

We then follow that if for all $x, y \in X$ there is $g \in G$ such that $gx = y$ then by fixing x and shoving y into the thing we get a surjective function from Gx to G, which implies the desired result.

(c) If G acts transitively in X, prove that $|X|$ divides $|G|$.

Probably we're assuming here that everything is finite.

If G acts transitively, then $X = Gx$ for all $x \in X$, and thus

$$|X| = |Gx| = |G|/|G_x|$$

which implies the desired result.

6.2.4

Let G be a group that acts on a set X. We say that the action is doubly transitive if it has the following property:

For all $x_1, x_2, y_1, y_2 \in X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$ there exists an element $g \in G$ of the group satisfying $gx_1 = y_1$, $gx_2 = y_2$.

(a) Let Z be the following set of ordered pairs:

$$Z = \{(z_1, z_2) \in X \times X : z_1 \neq z_2\}$$

Let G act on Z by the rule

$$g(z_1, z_2) = (gz_1, gz_2)$$

Prove that the action of G on X is doubly transitive if and only if the action of G on Z is transitive.

Suppose that the action on X is doubly transitive. Fix $q = (q_1, q_2) \in Z$. Since $q \in Z$ we follow that $q_1 \neq q_2$. Let $z \in Z$. We follow that $z = (z_1, z_2)$ for some $z_1, z_2 \in X$ such that $z_1 \neq z_2$. We then follow that for $q_1, q_2 \in X$ there is $g \in G$ such that $gq_1 = z_1$ and $gq_2 = z_2$. Thus $g(q_1, q_2) = (z_1, z_2)$ and thus $z \in Gq$. Since z is arbitrary we conclude that $Z \subseteq Gq$, which implies the desired result. Running about the same result but in reverse gives us the reverse implication.

(b) skip

6.3 The Orbit-Stabilizer Counting Theorem

6.3.1

Let G be a group, and let X be a set on which G acts.

(a) Suppose that $|G| = 15$ and $|X| = 7$. Prove that there is some element of X that is fixed by every element of G.

OSCT states that

$$|X| = \sum_{i=1}^{k} \frac{|G|}{|G_{x_i}|}$$

elements in the sum in rhs are nonzero divisors of 15 (by the fact that $|G| = 15$), of which there are $1, 3, 5$. The only way that we can have them sum up to $|X| = 7$ is

$$3 + 3 + 1$$

or

$$5 + 1 + 1$$

which implies that there's gotta be an element x_i such that $|G_{x_i}| = |G|$, which implies that there is x_i such that $G_{x_i} = G$, which implies the desired result.

(b) What goes wrong with your proof in (a) if $|G| = 15$ *and* $|X| = 6$ *or* $|X| = 8$*?*

The fact that then we can sum up the divisors into this number:

$$6 = 3 + 3$$

$$8 = 5 + 3$$

6.3.2

Skip

6.3.3

Let G act on itself by conjugation as described in 6.25. Let $x \in G$. The conjugacy class of x is the orbit of X for this action.

(a) Prove that G is the disjoint union of its conjugacy classes.

We can follow that for every $g \in G$ we have $g = ege$, thus implying that every element of G is in some conjugacy class, which implies the union part.

We then follow that if C is a conjugacy class, and $q \in C$, then there is $g, g' \in C$ such that g generates this class, and $q = g'gg'^{-1}$. Thus $g = g'^{-1}qg'$, and if $w \in C$, then there is $r \in G$ such that

$$w = rgr' = rg'^{-1}qg'r^{-1} = rg'^{-1}q(rg'inv)^{-1}$$

which implies that w is in conjugacy class of q, and thus C is a subset of the conjugacy class of q. Reverse inclusion is similar to this one, which implies that

$$C_1 \cap C_2 \neq \emptyset \Rightarrow C_1 = C_2$$

which implies the desired result.

(b) Prove that G is abelian if and only if each conjugacy class of G contains a single element.

If G is abelian, then $gqg^{-1} = gg^{-1}q = q$ for all $g \in G$, which implies that conjugacy classes are singletons.

If G's conjugacy classes are singletons, then for every pair $g, q \in G$ we have

$$gqg^{-1} = q$$

(the only element in conjugacy class is q since $e \in G$). This implies that

$$gq = qg$$

which implies the desired result.

Skip the rest

6.3.4

Let p be a prime. We proved in 6.26 that a group with p^2 elements must be abelian. Let G be a group with p^3 elements

(a) Mimic the proof of corollary 6.26 to try to prove that G is abelian. Where does the proof do wrong?

We firstly can show that p divides $|Z(G)|$, since nothing else in that part of the proof is dependent on the square. We then follow that

$$G/Z$$

does not have to be cyclic, which diverts from our initial proof.

(b) Give two examples of non-abelian groups with 2^3 elements

Q and D_4.

(c) What sort of information about G can you deduce from the proof in (a) that failed?

That $G/Z(G)$ is an abelian group (since its order is p^2)

6.3.5

Let G be a group, and let $a, b \in G$. We say that a commutes with b if $ab = ba$. Is "commutes with" an equivalence relation

By direct implication of valious definitions, "commutes with" is reflexiva and symmetric, but I think that transitiveness is not exaclty covered here. For example a commutes with e and e commutes with b does not imply that a commutes with b (e.g. $i * 1$, $1 * k$, $ik \neq ki$ in Q)

6.3.6

Let G be a group.

(a) Prove that the center $Z(G)$ of G is a normal subgroup of G.

We follwo that e commutees with evverything, and thus $e \in Z(G)$. Let $g, h \in Z(G)$, then let q be arbitrary. We follow that

$$qg^{-1} = (g^{-1}g)qg^{-1} = g^{-1}(gq)g^{-1} = g^{-1}qgg^{-1} = g^{-1}q$$

which gives us that $g^{-1} inZ(G)$. We also have that

$$ghq = gqh = qgh$$

thus implkying that $Z(G)$ is a subgroup, as desired.

Now assume that $g \in G, z \in Z(G)$. We follow that

$$g^{-1}zg = g^{-1}gz = z \in Z(G)$$

which implies that $Z(G) \subseteq g^{-1} Z(G) g$, thus making $Z(G)$ normal, as desired

(b) Let $H \subseteq G$ be a subgroup of G. Prove that the centralizer $Z_G(H)$ is a subgroup of G.

We follow that $e \in Z_G(H)$ since $eHe = H$. If $g \in Z_G(H)$, then for all $q \in H$

$$qg^{-1} = (g^{-1} g) qg^{-1} = g^{-1}(gq)g^{-1} = g^{-1} qgg^{-1} = g^{-1} q$$

and if $g, g' \in Z_G(H)$ then

$$gg'h = ghg' = hgg'$$

thus implying the desired result

(c) Let $H \subseteq G$ be a subgroup of G. Prove the the normalizer $N_G(H)$ is a subgroup of G.

We once again follow that $e \in N_G(H)$. If $g, g' \in N_G(H)$ then

$$gHg^{-1} = gg^{-1} Hgg^{-1} = H$$

thus $g^{-1} \in N_G(H)$ and

$$gg'H(gg')^{-1} = gg'Hg'g = gHg = H$$

as desired.

6.3.7

Skip

6.4 Sylow's Theorem

6.4.1

Fix a prime p and an integer $n \geq 1$. For $m \geq 1$, we consider the product

$$A_m = \prod_{i=0}^{p^n - 1} p^n m - i$$

Suppose that we factor A_m as $A_m = p^k B_m$ with $p \nmid B_m$

(a) Assume that $p \nmid m$. Find a simple closed formula for k that depends only on p and n.

Let us look at $p^n m - i$. Let us factor p out of i and get $i = p^j s$, where p does not divide s. We follow then that

$$p^n m - i = p^j (p^{n-j} m - s)$$

For every $i \in \omega$ such that $i \neq 0$ there is j such that $i = p^j s$ and $p \not| s$, and thus we conclude that there is a function $f : \omega_+ \to \omega$ such that $f(i) = j$. We then follow that if $a, b \in \omega_+$, then

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

(as can be proven quite trivially) and we also note that $k = f(A_m)$ in our conditions. Thus

$$A_m = \prod_{i=0}^{p^n-1} p^n m - i$$

$$k = f(A_m) = f(\prod_{i=0}^{p^n-1} p^n m - i) = \sum_{i=0}^{p^n-1} f(p^n m - i)$$

(none of the elements in the product are zero, which gives us this result) we then can follow that if $p|a$, and $b \neq 0$ then

$$f(a + b) = \min(f(a), f(b))$$

and in our case where $0 \leq i \leq p^n - 1$ we have that

$$f(p^n m - i) = f(i)$$

for $i \neq 0$ and

$$f(p^n m - 0) = n$$

If S is a finite sequence in ω, then we can follow an interesting thing. Namely that if J is a finite sequence of elements of ω, then we can define $Q_i : J \to \omega$ as

$$Q_i(S) = \text{the number of the elements of } S \text{ that are greater or equal to } i$$

or more formally

$$Q_i(S) = |\{j \in S[\omega] : j \geq i\}|$$

and then

$$\sum S = \sum_{i=1}^{\omega} Q_i(S)$$

and also if j is the highest element of S, then

$$\sum S = \sum_{i=1}^{j} Q_i(S)$$

thus we have that

$$k = \sum_{i=0}^{p^n-1} f(p^n m - i) = f(p^n m) + \sum_{i=1}^{p^n-1} f(p^n m - i) =$$

$$= f(p^n m) + \sum_{i=1}^{\omega} Q_i(f[\{p^n m - j : 1 \leq j \leq p^n - 1\}])$$

we then follow that since $j \neq 0$ and $j \leq p^n - 1 < p^n m$ we have

$$k = f(p^n m) + \sum_{i=1}^{\omega} Q_i(f[\{j : 1 \leq j \leq p^n - 1\}])$$

then we follow that the maximum possible value of $f[\{j : 1 \leq j \leq p^n - 1\}]$ is $n-1$, which gives us

$$k = f(p^n m) + \sum_{i=1}^{n-1} Q_i(f[\{j : 1 \leq j \leq p^n - 1\}])$$

and then we can also follow that for $i \in N_+$

$$Q_i(f[\{j : 1 \leq j \leq p^n - 1\}])$$

is the number of divisors of p^i in the set $1 \leq j \leq p^n - 1$. We then can follow that for $j \in N_+$ we have $p^{n-j} - 1$ (from p^i to $p^n - p^i = p^{n-i}p^i - p^i = p^i(p^{n-i} - 1)$) multiples of p^i. Thus

$$k = f(p^n m) + \sum_{i=1}^{n-1} Q_i(f[\{j : 1 \leq j \leq p^n - 1\}]) =$$

$$= f(p^n m) + \sum_{i=1}^{n-1} (p^{n-i} - 1) = f(p^n m) - n + 1 + \sum_{i=1}^{n-1} (p^{n-i})$$

then we can refactor the sum to get

$$\sum_{i=1}^{n-1} (p^{n-i}) = p^{n-1-1} + ... + p^1 = \sum_{i=1}^{n-2} p^i = \sum_{i=0}^{n-2} p^i - 1 = \frac{p^n - 1}{p - 1} - 1$$

and thus we have

$$k = f(p^n m) - n + 1 + \frac{p^n - 1}{p - 1} - 1 = f(p^n m) - n + \frac{p^n - 1}{p - 1}$$

Since p does not divide m we conclude that $f(p^n m) = n$ and thus

$$k = \frac{p^n - 1}{p - 1}$$

as desired

(b) Use (a) to give a quick proof of Lemma 6.30

Proof is essentialy the same, but we note that the maximal power of p in both numerator and denominator are the same, and thus the whole shebang is not divisible by p

(c) What happens if we allow p to divide m?

We get that if j is the highest power of p that divides m then the whole product's highest power of p is also j (as seen in the proof of (a)).

6.4.2

Let p be a prime, and let G be a group of order p^n. Prove that for evert $0 \leq r \leq n$ there is a subgroup H of order p^r.

Sylow's theorem implies the existence for p^n (i.e. the whole group), and we can state also that $\{e\}$ is also a subgroup of order p^0.

Assume that $|G| \geq 2$, and let $q \in G$ be non-identitiy. We follow that its order j divides $|G|$, and thus since it's a non-identity, its order is p^k for some $1 \leq k \leq n$. Then we follow that order of j^k is p, which implies that there is a subgroup of G, whose order is p.

Assume that for some $n \in \omega$ we have the desired property. Let G be an arbitrary group of order p^{n+1}. We follow that its center is non-trivial, and then follow that its center has a subgroup H of order p. Since H is a subgroup of the center, we can quickly follow that it's normal, and thus G/H constitues a group. Order of G/H is going to be p^n by Lagrange's theorem. We then follow that by our assumption, there are subgroups of G/H of order $p^0, p^1, ..., p^n$. Let us label them by $C_0, C_1, ..., C_n$. Exercise 6.7(b) (one, that is also solved in this work), implies that for each C_j there is a subgroup $Q_j \subseteq G$ such that $C_j = Q_j/H$. In the proof of that exercise we essentially state that the union of all the elements of C_j is itself a subgroup of G, and now we're adding that by the fact that all the elements of C_j are disjoint (by properties of cosets) we conclude that $|Q_j| = |C_j| * |H| = p^j * p = p^{j+1}$. Thus we conclude that for all $0 \leq j \leq n$ there are subgroups of G of order p^{j+1}. In combination with the fact that the trivial subgroup $\{e\}$ is a subgroup of G, we conclude that G has subgroups of p^j for all $0 \leq j \leq n+1$. By the fact that G is arbitrary, we conclude that it is true for all groups of order p^{n+1}.

If we now take our previous proof, and combine it with one of the deriviation at the start, we get a proof by induction of the fact all groups G of order p^n with $n \in \omega$ have the desired property. We also note, that we did not restrict p, which also implies that the result is true for any prime p.

6.4.3

This exercise asks you to give two different proofs of the following stronger version of the first part of Sylow's Theorem

Theorem: *Let G be a finite group. let p be a prime, and suppose that $|G|$ is divisible by p^r for $r \in \omega$. There is a subgroup of G of order p^r.*

(a) Give a proof that directly mimics the proof in the book.

Let n be the highest power of p that divides $|G|$. We follow then that

$$|G| = p^n m$$

where $p \not| m$, and thus for any given $1 \leq j \leq n-1$ we have

$$|G| = p^{n-j} p^j m$$

then we state that there are $C(p^{n-j}p^jm, p^j)$ subsets of $|G|$ that are of size p^j, and thus

$$C(p^{n-j}p^jm, p^j) = \sum_{i=1}^{r} \frac{p^{n-j}p^jm}{|G_{A_r}|}$$

we then follow that by first exercise in this section, the maximal power of p in $C(p^{n-j}p^jm, p^j)$ is p^j, and thus there is B such that $p \not| B$ and

$$C(p^{n-j}p^jm, p^j) = p^jB = \sum_{i=1}^{r} \frac{p^{n-j}p^jm}{|G_{A_r}|}$$

thus

$$p^jB = \sum_{i=1}^{r} \frac{p^{n-j}p^jm}{|G_{A_r}|}$$

$$p^jB_m = p^j \sum_{i=1}^{r} \frac{p^{n-j}m}{|G_{A_r}|}$$

$$B_m = \sum_{i=1}^{r} \frac{p^{n-j}m}{|G_{A_r}|} =$$

which implies that there is r such that $|G_{A_r}||p^{n-j}$. After this point, the proof is practically the same as well, thus giving us implication that for all $1 \leq j \leq n-1$ we have a subgroup of G of order p^{n-j}, which is equivalent to the desired conclusion.

(b) Combine the version of Sylow's Theorem that we did prove with the previous exercise.

Let G be a finite group. We follow that if n is the highest order of a prime p such that $p^n||G|$, then there is a subgroup of G of order p^n. Previous exercise implies that the resulting subgroup has subgroups of order $p^0, p^1, ..., p^n$ of its own, and since subgroup J of a subgroup K of a group L is a subgroup of L we get the desired result.

6.4.4

In example 6.36 we showed that there are exactly two groups of order 10*. Do a similar calculation to find all groups of order* 15

15 is divided by 5 and 3, and thus we follow that there are H_5 and H_3. We then once again follow that the only k such that $k \mid |G|$ and $k \equiv 1(\mod 5)$ is 1, thus implying that H_5 is the only subgroup of order 5 and thus normal

Then let us uncombine those groups to get

$$H_3 = \{e, a, a^2\}, H_5 = \{e, b, b^2, b^3, b^4\}$$

we then note that since $gcd(3,5)$ that $H_3 \cap H_5 = \{e\}$, and thus $a, a^2 \notin H_5$. This in turn gives us that

$$eH_5 = H_5, aH_5, a^2H_5$$

are cosets of H_5 that decompose the group, and thus any given $g \in G$ is of the form $g = a^i b^j$ for some $i, j \in \omega$.

We then note that $a^{-1}ba \in H_5$ and thus there is $0 \leq j \leq 4$ such that

$$aba^{-1} = b^j$$

which is equivalent to

$$b = a^{-1}b^j a$$

thus we can follow that

$$b = a^{-1}b^j a = (a^{-1}ba)^j = (a^{-1}(a^{-1}b^j a)a)^j =$$

$$= (a^{-1}(a^{-1}ba)^j a)^j = (a^{-1}(a^{-1}(a^{-1}b^j a)a)^j a)^j =$$

$$= (a^{-1}(a^{-1}b^j a)a)^{j^2} = (a^{-1}b^j a)^{j^2} = b^{j^3}$$

which is practically the same deriviation as in the book, but with an extra appplication of substitution of b for $a^{-1}b^j a$. Thus we have that

$$b = b^{j^3} \Leftrightarrow e = b^{j^3-1}$$

thus we have that

$$j^3 \equiv 1(\mod 5)$$

we then follow that the only such j is $j = 1$, which implies that G is abelian, and then by the same deriviation we conclude that G is cyclic group of order 15.

6.4.5

Let G be a finite group, and let H_1, H_2 be normal subgroups having the property that $gcd(|H_1|, |H_2|) = 1$. Prove that elements of H_1 and H_2 commute.

Let us look at

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1}$$

since H_2 is normal we follow that $aba^{-1} \in H_2$ and thus

$$aba^{-1}b^{-1} \in H_2b^{-1}$$

by the fact that $b^{-1} \in H_2$ we conclude thta

$$H_2b^{-1} = H_2$$

and thus

$$aba^{-1}b^{-1} \in H_2$$

by similar logic we have

$$aba^{-1}b^{-1} = a(ba^{-1}b) \in aH_1 = H_1$$

and thus

$$aba^{-1}b^{-1} \in H_1 \cap H_2$$

If $H_1 \cap H_2$ is non-trivial, then we follow that there is $h \in H_1 \cap H_2$ such that $h \neq e$. Thus the order of h is some $j > 1$ and therefore h generates a cyclic subgroup of order j. Therefore we follow that j divides both $|H_1|$ and $|H_2|$ by Lagrange's theorem, which implies that $gcd(|H_1|, |H_2|) > 1$, which is a contradiction. Thus we conclude that $H_1 \cap H_2$ is trivial, and therefore

$$aba^{-1}b^{-1} = e \Rightarrow ab = ba$$

which is the desired result.

6.4.6

Let G be a finite group of order $|G| = pq$ where p, q are primes satisfying $p > q$. Assume further that $p \not\equiv 1(\mod q)$.

(a) Prove that G is an abelian group.

We follow that there are H_p, H_q - respective p-Sylow and q-Sylow subgroups of G of order p and q respectively. Their order implies that H_p and H_q are abelian. Example 6.37 implies that H_p is normal (while we know nothing of the H_q). We then follow that our assumption that $p \not\equiv 1(\mod q)$ gives us an ability to use example 6.37 to prove by same idea mutatis mutandis that H_q is also normal. Thus previous exrcise implies that elements of H_p and H_q commute.

We then follow that every element $g \in G$ can be expressed as

$$g = ab$$

for some $a \in H_p$ and $b \in H_q$ (by the same deriviation as in example 6.36 or two exercises ago). Thus let $g_1, g_2 \in G$. We follow that there are $a, a' \in H_p$ and $b, b' \in H_q$ such that

$$g_1 = ab, g_2 = a'b'$$

and thus

$$g_1g_2 = aba'b' = a(ba')b' = aa'bb' = (aa')(bb') = a'(ab')b = a'b'ab = g_2g_1$$

which implies the desired result.

(b) Prove that G is a cyclic group

We can use the same deriviation as in example 6.36

6.4.7

Let G be a group. An isomorphism from G to itself is called an automorphism of G. The set of automorphisms is denoted

$$Aut(G) = \{ \text{ group isomorphisms } G \to G\}$$

We define a composition law on $Aut(G)$ by composition of functions

(a) Prove that this composition law makes $Aut(G)$ into a group

We can follow that the general identity is the identity for the group. If $f \in Aut(G)$ is an element, then f^{-1} is a function by the fact that everything in $Aut(G)$ is a bijection. Inverse of an isomorphism is an isomorphism itself, and thus we have inrverses in the $Aug(G)$. Association is taken care of by the general association of the composition of functions, which gives us the desired result

(b) Let $a \in G$. Define a map $\phi_a : G \to G$ by the formula

$$\phi_a(g) = aga^{-1}$$

Prove that $\phi_a \in Aut(G)$ and that the map

$$q : G \to Aut(G), q(a) = \phi_a$$

is a group homomorphism.

We follow that ϕ_a is a composition of products of elements of a group, and thus is injective. If $h \in G$, then

$$\phi_a(a^{-1} ha) = h$$

thus making h surjective, which implies that $\phi_a \in Aut(G)$. Then we follow that

$$q(ab) = \phi_{ab}$$

$$q(a)q(b) = \phi_a\phi_b$$

now let $g \in G$. We follow that

$$\phi_{ab}(g) = abg(ab)^{-1} = abgb^{-1}a$$

$$\phi_a\phi_b(g) = \phi_a(bgb^{-1}) = abgb^{-1}a^{-1}$$

which implies that q is indeed a homomorphism, as desired.

(c) Prove that the kernel of homomorphism 6.23 is the center $Z(G)$ of G.

Let $c \in Z(G)$. We follow that for $g \in G$

$$\phi_c(g) = cgc^{-1} = cc^{-1}g = eg = g$$

and if $v \notin Z(G)$, then if $q(v) = id$ then for all $g \in G$

$$\phi_v(g) = g$$

thus

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

$$vg = gv$$

which implies that $v \in Z(G)$, which is a contradiction. Thus we have the desired result.

(d) Elements of $Aut(G)$ that are equal to ϕ_a for some $a \in G$ are called inner automorphisms, and all other elements of $Aut(G)$ are called outer automorphisms. Prove that G is abelian if and only if its only inner automorphism is the identity map

Inner automorphisms are essentially images of q. If G is abelian, then $Z(G) = G$, and thus $q(g) = id$ as per the previous exercise. If the range of q is $\{id\}$, then for all $v, g \in G$

$$\phi_v(g) = g$$

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

$$vg = gv$$

which implies the desired result.

(e) More generally, if H is a normal subgroup of G, prove that there is a well-defined group homomorphism

$$w : G \to Aut(H), q(a)(h) = aha^{-1}$$

and that the kernel of this homomorphism is the centralizer of H in G

We can follow that if f is an inner automorphism of G, then for $h \in H$ we have

$$f(h) = aha^{-1}$$

and more generally

$$f[H] = aHa^{-1} = H$$

thus we can make f into an automorphism on H by restricting its domain. We call the function that does such a thing j. Thus by composing homomorphism from (b) with j we get the desired function. We then follow that if $k \in Z_G(H)$, then

$$w(k)(h) = khk^{-1} = kk^{-1}h = h$$

for all $h \in H$, thus implying that $w(k) = id$. Now assume that $k \notin Z_G(H)$ and we have that $w(k) = id$. Then for all $h \in H$

$$h = w(k)(h) = khk^{-1} \Rightarrow kh = hk \Rightarrow k \in Z_G(H)$$

which is a desired contradiction.

6.4.8

Let C_n be a cyclic subgroup of order n, and let $Aut(C_n)$ be the automorphism group of C_n; Prove that $Aut(C_n)$ is isomorphism to $(Z/nZ)^*$.

We notice that C_n by definition is generated by some element $g \in C_n$. That is,

$$C_n = \{g^i : 0 \leq i < n\}$$

Let $q \in [0, n) \cap \omega$ be such that it's relatively prime to n. We follow that g^q also generates C_n, as was proven somewhere in the book. Thus we can follow that there is a function $h : C_n \to C_n$

$$h(g^j) = (g^q)^j$$

that is bijective. We then can trivially follow that this thing is a homomorphism, and thus isomorphism, and thus an element of $Aut(C_n)$.

We then follow that if $k : C_n \to C_n$ is an isomorphism, then there is $0 < j < n$ such that

$$k(g) = g^j$$

which gives us the fact that for every element of $Aut(C_n)$ there is a unique $0 < j < n$ and vice versa. We then notice that j can only be a number that is relatively prime to n, which in combination with the previous paragraph gives us the idea that $\phi : (Z/nZ)^* \to Aut(C_n)$ defined by

$$phi(j)(g) = g^j$$

is the desired isomorphism

6.4.9

Let G be a group of order $|G| = 75$.

(a) Prove that G has a subgroup H with all three of the folllowing properties: $|H| = 25$, H is a normal subgroup of G, H is abelian

Let H be a 5-Sylow subgroup of G. We follow that its order is 25. Since its order is a square of a prime, it's abelan. Numbers that divide 75 are

$$1, 3, 5, 15, 25, 75$$

none of which give 1 mod 5, except for 1, which implies that this is the only 5-Sylow subgroup, which implies that the thing is normal.

(b) Suppose that the subgroup H in (a) is cyclic of order 25. Prove that G is abelian.

We follow that there is also a 3-Sylow subgroup. Since its order is 3 we follow that it's cyclic. By the example's deriviation we have

$$aba^{-1} = b^j$$

$$b = a^{-1} b^j a$$
$$b = b^{j^3}$$
$$j^3 \equiv 1 \mod 25$$

the only such j is 1, which implies that 3-Sylow and H commute. Let a now generate H and b generate the 3-Sylow subgroup. We follow that ab's order is finite and let this order be j. We follow that

$$e = (ab)^j \Rightarrow e = a^j b^j \Rightarrow a^{-j} = b^j \in H \cap H_3 = \{e\} \Rightarrow$$
$$\Rightarrow a^k = b^k = e \Rightarrow 3|k \wedge 25|k \Rightarrow k = 75$$

which is pretty much the same deriviation as in one of the examples in the chapter

6.5 Double Cosets and Sylow's Theorem

6.5.1

Let G be a finite group of order $|G| = pm$, where p is prime and $p \not| m$. Assume further that m has the following property: The only divisor d of m, that satisfies $d \equiv m(\mod p)$ is $d = m$.

(a) Prove the p-Sylow subgroup of G is a normal subgroup of G.

Let us name the p-Sylow sugroup of G as H.

We firstly follow that if p-Sylow subgroup is normal, then its conjugates are equal to the group, thus making this group the one and only p-Sylow subgroup of G. Same goes in the other direction, thus p-Sylow is normal if and only if $k = 1$ (variables definition here is the same as in the text in the book).

Now assume that H is not normal. We follow that $k > 1$. We also have that $k|pm$. If $p|k$, then $k \equiv 0 \mod p$, which is a contradiction, which implies that $p \not| k$. Since $p \not| m$ we follow then that

$$k|m$$

which implies that there is $n \in N_+$ such that $m = kn$. Moreover we have that $n < m$ since $k > 1$. Now we can follow that

$$k \equiv 1(\mod p)$$
$$nk \equiv n(\mod p)$$
$$m \equiv n(\mod p)$$
$$n \equiv m(\mod p)$$

which directly contradicts the premise (this proof is somewhat awkward, and can be easily converted to the direct one).

Skipping the rest of those exercises, maybe will come back for them later

Chapter 7

Rings - Part 2

7.1 Irreducible Elements and Unique Factorization Domains

7.1.1

Let R be an integral domain, and let $a, b \in R$. Prove that the following are equivalent:

(a) $a|b$ and $b|a$

(b) There is a unit $u \in R^*$ satisfying $a = bu$.

(c) There is an equality of principal ideals $aR = bR$.

There's probably a cyclical imlication here, so assume that $a|b$ and $b|a$. Definition implies that $a, b \neq 0$ and also that there are $k_1, k_1 \in R$ such that $a = bk_1$ and $b = ak_2$. We follow then that

$$a = bk_1 = ak_2k_1$$

thus

$$a * 1 = ak_2k_1$$

which by the fact that $a \neq 0$ and R being integral domain implies that

$$k_2k_1 = 1$$

thus implying that $k_1, k_2 \in R^*$, which implies (b) from deriviation that $a = bk_1$.

Now if $a = bu$ for some $u \in R^*$, then we follow that

$$h \in aR \Rightarrow (\exists r \in R)(h = ar) \Rightarrow (\exists r \in R)(h = bur) \Rightarrow (\exists ur \in R)(h = b(ur)) \Rightarrow h \in bR$$

thus implying that $aR \subseteq bR$. Reverse inclusion is kinda similar here, which implies (c)

If $aR = bR$, then $a \in bR$, which implies that there is $r \in R$ such that $a = br$, which implies that $b|a$. Similar implication holds for the other condition.

7.1.2

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

(a) Suppose that $b = au$ for some unit $u \in R^*$. Prove that the principal ideals aR and bR are equal.

In the previous exercise we had the assumption that R is an integral domain, which we don't have here. However out proof holds the same since the deriviation from (b) to (c) does not involve any properties of an integral domain

(b) Give an example of a ring R and elements $a, b \in R$ having the property that $aR = bR$, but there does not exist a unit $u \in R^*$ satisfying $b = au$.

Hint gives us that R cannot be an integral domain (which is kinda obvious from the previous point). The fact that it is a challenging problem perhaps suggests that we're going to have to deal with the polynomials.

Simpliest ring that is not an integral domain that I can think of is the $Z/4Z$. We can follow that the only units are 1 and -1 that give us the only nonzero element that exists apart from that is 2, which does not give us much room to move around.

With $Z/6Z$ we have that $1, 5$ are units, and $2, 3, 4$ are non-units. We follow that their respective principal ideals are

$$2 * Z/6Z = \{0, 2, 4\} = 4 * Z/6Z$$

$$3 * Z/6Z = \{0, 3\}$$

we follow that $2 * 5 = 4 \mod 6$ which does not give us the desired result.

After some fudging around with python we can find out that none of the Z/nZ for n up to 100 are satisfying those ideas.

Looking into the proof of 7.1 we can follow that $(b) \Rightarrow (c), (c) \Rightarrow (a)$ without the usage of the fact that R is an ID. The only requirement of ID comes from the b to c implication.

TODO

7.2 Eucledian Domains and Principal Ideal Domains

7.2.1

Let R be a PID, let $a, b \in R$ be elements that are not both 0, and let $d \in R$ be an element that generates the (principal) ideal generated by a and b:

$$dR = aR + bR$$

(a) Prove that d divides both a and b

We can follow that since $dR = aR + bR$ we have that $0 \in bR$ and thus $aR = aR + 0 \subseteq dR$. Therefore we have that $a \in dR$ and thus there is $r \in R$ such that $a = dr$, which implies that $d|a$, as desired. Similar thing holds for b.

(b) Let $c \in R$ be a non-zero element that divides both a and b. Prove that c divides d.

Since $c|a$ and $c|b$ we follow that there are $n, k \in R$ such that $nc = a$ and $kc = b$. Since $dR = aR + bR$ and $d \in dR$ we follow that there are $r, r' \in R$ such that

$$d = ar + br' = ncr + kcr' = c(nr + kr')$$

which implies the desired result

7.2.2

Let R be a Eucledian domain with size function σ and let $a \in R$ be a nonzero element of R. Prove that

$$a \in R^* \iff \sigma(a) = \sigma(1)$$

$a \in R^*$ implies that for all $b \in R \setminus \{0\}$ we have

$$\sigma(ba) = \sigma(b)$$

thus since $1 \neq 0$ we have

$$\sigma(a) = \sigma(1 * a) = \sigma(1)$$

which gives us the forward implication.

Since $\sigma(1) = \sigma(a) = \sigma(1 * a)$ we follow the desired result by 7.15

7.2.3

Let R be an integral domain, and let

$$\sigma : R \setminus \{0\} \to \omega$$

be a function that has property (1) in the definition of a Eucledian domain. Define a new function

$$\tau : R \setminus \{0\} \to \omega, \tau(r) = \min\{\sigma(rc) : c \in R \setminus \{0\}\}$$

Prove that τ has both properties (1) and (2)

Suppose that $b, c \in R$ are arbitrary nonzero elements. We follow that there are $a, a' \in R \setminus \{0\}$ such that $\tau(b) = \sigma(ab)$, $\tau(cb) = \sigma(acb)$. Since R is an integral domain and a, c are nonzero we follow that $ac \neq 0$. By definition of τ we follow that for all $q \in R \setminus \{0\}$ we have that $\tau(b) \leq \sigma(qb)$, and thus $\tau(b) \leq \sigma((ac)b) = \tau(cb)$ which implies the part (2) of the definition.

Assume that $b, r \in R \setminus 0$ are such that $\sigma(b) > \sigma(r)$. We firstly can follow that $\sigma(r) \geq \tau(r)$ by definition of τ, and $\tau(b) = \sigma(cb) \geq \sigma(b)$ by previous point, which implies that

$$\tau(b) \geq \sigma(b) > \sigma(r) \geq \tau(r)$$

which gives us point (1) and the desired result.

7.2.4

this one was taken care of in the linear algebra course

7.2.5

Explain why proof of the fact that $Z[i]$ is a Eucledian domain won't work on $Z[\sqrt{3}]$
here i've copied the exercise wrongly

We firstly follow that $Z[\sqrt{3}]$ is a subring of R, and thus it's got to be an integral domain. We can also state that there is a bijection between $Z[\sqrt{3}]$ and Z^2 which can also give us a plane, just as in $Z[i]$ case. We can also define $\sigma : Z[\sqrt{3}] \to R$ by setting

$$\sigma(a + b\sqrt{3}) = a^2 + b^2$$

we can follow that $\sigma(\zeta) = 0 \Leftrightarrow \zeta = 0$, but can we do the second part? We can see that

$$\sigma(\sqrt{3} * \sqrt{3}) = \sigma(3) = 3^2 + 0^2 = 9$$

$$\sigma(\sqrt{3}) * \sigma(\sqrt{3}) = 1 * 1 = 1 \neq 9$$

which gives us problems.

7.2.6

For each of the following rings R and elements α, determine whether α is irreductible in R. Justify your answer by either factoring α or proving that it is irreductible

(a) $R = Z[i]$ and $\alpha = 2 + 3i$

We can follow that we have a function $\sigma(x + yi) = x^2 + y^2$ is having a property $\sigma(ab) = \sigma(a)\sigma(b)$. We then follow that

$$\sigma(\alpha) = \sigma(2 + 3i) = 4 + 9 = 15 = 3 * 5$$

thus we can try to make up elements with sizes 3 and 5. The problem is that 3 is not a sum of squares, and thus we can follow that there is no element a of $Z[i]$ such that $\sigma(a) = 3$, which implies that the element is irreductible.

(b) $R = Z[i]$ and $\alpha = 4 + 3i$

We follow that

$$\sigma(\alpha) = \sigma(4 + 3i) = 16 + 9 = 25 = 5^2$$

we then can heck around with $Z[i]$ to get that

$$(2 - i) * (1 + 2i) = 2 + 4i - i + 2 = 4 + 3i$$

thus giving us the desired result.

(c) $R = F_2[x]$ and $\alpha = x^5 + x + 1$

Here we firstly note that the size function is deg, which has property $\deg(a * b) = \deg(a) + \deg(b)$, thus stating that our resulting elements are of order $1, 4$ or $2, 3$. We also note that both elements should have a non-zero constant value in order to result in a non-zero constant value in the result. There are only a finite amount of polynomials of both degrees, and thus we can try to go through all of them

$$(x+1)(x^4+1) = x^5 + x^4 + x + 1$$

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

we then note an interesting thing: polynomial multiplication in F_2 looks kinda similar to multiplication in a base 2. We follow that in base 2

$$\alpha = 2^5 + 2 + 1 = 35 = 5 * 7$$

and $5 = x^2 + 1$, $7 = x^2 + x + 1$. We then follow that

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

thus concluding that we were wrong on this one (but it's still pretty interesting how exactly this thing translates to binary). Thus let us go back to just calculating the things

$$(x+1)(x^4+1) = x^5 + x^4 + x + 1$$

$$(x+1)(x^4+x+1) = x^5 + x^2 + x + x^4 + x + 1 = x^5 + x^4 + x^2 + x + 1$$

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

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

after doing this thing for a while, I thought that maybe a better idea is to think about theproblem a bit. If we're multiplying $(x+1)$ by any polynomial with 4th power, then the fourth power will be in the resulting polynomial, which does not give us the desired result. Thus we can skip this thing to get to the powers $3, 2$:

$$(x^2+1)(x^3+1) = x^5 + x^2 + x^3 + 1$$

$$(x^2+1)(x^3+x+1) = x^5 + x^3 + x^2 + x^3 + x + 1 = x^5 + x^2 + x + 1$$

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

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

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

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

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

which gives us α, and thus the desired result.

(d) $R = F_2[x]$ and $\alpha = x^5 + x^2 + 1$ we've got only one polynomial to check, thus let us do this:

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

thus we've gone through all the applicable polynomials, which implies that there α is irreductible.

7.2.7

This one mirrors the proof of 3.51(c) since we haven't used degrees in that proof

7.3 Factorization in PID

7.3.1

Let R be a principal ideal domain, and let $a, bc \in R$. Prove that if a is irreductible, does not divide b, and $a|c$, $b|c$, then $ab|c$.

We can follow that there are nonzero $n, k \in R$ such that

$$an = c, bk = c$$

thus

$$an = bk \Rightarrow a|bk$$

since a does not divice b we follow that $a|k$. Thus there is $j \in R$ such that $aj = k$, and therefore

$$bk = baj = c$$

which implies that $ba = ab$ divides c, as desired.

7.3.2

Let R be a PID. Prove the 7.19 without the assumption that R is a Eucledian domain by assuming that $a \in R$ is non-zero non-unit, not a product of irreductibles, and following the following steps.

(a) Show that you can write $a = a_1b_1$ as a product of non-units such that b_1 is not a product of irreductibles and then that you can write $a = a_1a_2b_2$ as a product of non-units such that b_2 is not a product of irreductibles etc. In this way, for every n you get a product of non-units $a = a_1a_2...a_nb_n$ such that b_n is not a product of irreductibles.

Since a is not a non-unit, and not irreductible, we follow taht there are a_1, b_1 such that

$$a = a_1b_1$$

We follow that if both of a_1, b_1 are irreductibles, then a is a product of irreductibles, which is a contradiction. Therefore we conclude that at least one of a_1, b_1 is not irreductible. We then follow that at least one of a_1, b_1 also has to be a product of non-irreductibles, otherwise we have that a is a product of irreductibles. By relabeling if necessary and proceeding with induction we get the desired result.

(b) Prove that the ideals $I_n = b_n R$ satisfy $I_1 \subseteq I_2 \subseteq I_3$...

We can follow that by construction of b_n we have that $b_{n+1}|b_n$, and thus $b_{n+1}R \subseteq b_n$, which implies this result.

(c) Let $J = I_1 \cup I_2$... be the union of all of the I_n. Prove that J is an ideal of R. Then since we have assumed that R is a PID, the ideal J is principal, so we can write $J = cR$ for some $c \in R$.

We can follow that any given $a_1, a_2 \in J$ are both contained in some I_n, and thus their sum is also in I_n. We can also follow that $a_1 c \in I_n$ by the fact that I_n is an ideal, thus making J an ideal.

(d) Since J is the union of the I_n, there is an index k so that $c \in I_k$. Prove that $I_k = I_{k+1} = I_{k+2} = ...$

We know that $cR = J$, $cR \subseteq I_k$ and $I_k \subseteq J$, which implies that $I_k = J$. By similar reasoning we have the rest.

(e) Use $I_k = I_{k+1}$ to deduce that $a_{k+1}bk + 1R = b_{k+1}R$, and from this, deduce that $a_{k+1} \in R^*$.

We can follow that $I_{k+1} = b_{k+1}R$ by definition, and $b_k = a_{k+1}b_{k+1}$ by its definition, thus implying that

$$b_k R = a_{k+1}b_{k+1}R = I_k = I_{k+1} = b_{k+1}R$$

thus we have that there is $c \in R$ such that

$$a_{k+1}cb_{k+1} = b_{k+1}$$

we then follow that $a_{k+1}c = 1$ by cancellation property, that implies in turn that $a_{k+1} \in R^*$.

7.3.3

Let $R = Z[\sqrt{-3}]$ be the ring that we studies in Example 7.21.

(a) Prove that ± 1 are the only units in R.

± 1 are obviously units here, as can be proven trivially.

If we take a number q that is in Z and not equal to ± 1, then we follow that if we multipy it by another member of Z, then we're not getting 1 (ddue to basic properties of Z). If we multiply them by any $a + b\sqrt{-3}$ with non-zero b, then we're getting non-zero b in the result as well, thus proving that no member of Z is a unit.

If $q \notin Z$, then we follow by previous point that its supposed multiplicative inverse cannot be in Z by previous point. If $q = b\sqrt{-3}$, then we follow that by multiplicating this thing by some $b'\sqrt{-3}$ will give us $-3bb'$, which cannot be equal to 1 with $b, b' \in Z$.

Multiplication by $a' + b'\sqrt{3}$ with nonzero a' will give us nonzero $\sqrt{-3}$ in the result, so it won't do. Thus the only other case happens if $q = a + b\sqrt{-3}$ with $a, b \neq 0$. Multiplicating this q by any $a' + b'\sqrt{-3}$ with zero a or b will give us previous point, thus we need to assume that $a', b' \neq 0$. We follow that

$$(a + b\sqrt{-3})(a' + b'\sqrt{-3}) = 1$$

we then follow that

$$(a - b\sqrt{-3})(a' - b'\sqrt{-3}) = 1$$

and mmultyplying them we get

$$(a^2 + 3b^2)(a'^2 + 3b'^2) = 1$$

we then follow that $(a^2 + 3b^2)$ for nonzero a, b is greater or equal to 4, thus implying that there is no way to pick such numbers, thus impying the desired result

(b) Prove that $1 + \sqrt{-3}$ *and* $1 - \sqrt{-3}$ *are irreductible elements of* R.

Suppose that there are non-units $q, w \in R$ such that

$$qw = 1 + \sqrt{-3}$$

we follow that

$$(a + b\sqrt{-3})(a' + b'\sqrt{-3}) = 1 + \sqrt{-3}$$

and therefore

$$(a - b\sqrt{-3})(a' - b'\sqrt{-3}) = 1 - \sqrt{-3}$$

and thus

$$(a^2 + 3b^2)(a'^2 + 3b'^2) = 1^2 + 3 = 4$$

$$(a^2 + 3b^2)(a'^2 + 3b'^2) = 4$$

and then we're going with pretty much the same deriviation as in the example.

(c) Prove that 2 *is ireeductible in* R

Skip

(d) Use previous point to dedufe that R *is not a UFD*

Directly follows from definitions and trivial deriviations

7.4 The Chinese Remainder Theorem

7.4.1

Solve the following simultanenous congruences:

(a) $x \equiv 3(mod 7)$ *abd* $x \equiv 5(\mod 11)$

$38 + 77n$ for $n \in Z$.

(b) $x \equiv 31(mod 117)$ *abd* $x \equiv 41(\mod 119)$

$13726 + 117 * 119 * n$ for $n \in Z$.

Next one is 423, and the rest is skipped

7.4.2

Let R be a commutative ring

(a) Suppose that $a, b \in R$ have the property that $aR + bR = R$. Prove that for all $m, n \geq 1$ we have

$$a^m R + b^n R = R$$

We follow that there are $v, w \in R$ such that

$$a^2 v + baw = a$$

and thus we have that

$$1 = av + bw = (a^2 v + baw)v + bw = a^2 v^2 + bawv + bw = a^2 v^2 + b(aw^2 + w)$$

and therefore we follow that $a^2 R + bR = R$. By induction we can prove that $a^m R + bR = R$, which would imply the desired result

Next one is also proven by induction

7.4.3

Let R be a PID

(a) Let $a, b \in R$. Prove that

$$aR + bR = R \Leftrightarrow aR \cap bR = abR$$

Assume the former. We follow that if $x \in abR$ then there is $q \in R$ such that $x = abq$, and thus $x \in aR, x \in bR$, which implies that

$$abR \subseteq aR \cap bR$$

If $x \in aR \cap bR$, then we follow that there are $u, w \in R$ such that $au = bw = x$. Since $aR + bR = R$ we follow also that there are $q, e \in R$ such that

$$aq + be = 1$$

and thus

$$u = u * 1 = u(aq + be) = auq + bue = bwq + bue = b(wq + ue)$$

and thus we have that

$$x = au = ab(wq + ue) \in abR$$

which gives us the forward implication.

Since R is a PID we follow that there is $d \in R$ such that

$$aR + bR = dR$$

thus there are $u, w \in R$ such that

$$au + bw = d$$

We then follow that by one of the previous exercises $d|a$ and $d|b$. Therefore there are $n, j \in R$ such that

$$dn = a$$

$$dk = b$$

and thus we follow that

$$dnk = ak = bn \in aR \cap bR = abR$$

therefore we have that there is $q \in R$ such that

$$dnk = abq$$

and thus

$$dnk = dndkq$$

since R is a PID we follow that it's an integral domain, and thus we can cancel out the terms to obtain

$$dnk = dndkq$$

$$1 * (dnk) = (dnk) * dq$$

$$1 = dq$$

which implies that $d \in R^*$, and thus $dR = R$, which gives us the desired result.

(b) Let $c_1, ..., c_n \in R$, and suppose that $c_iR + c_jR = R$ for all $i \neq j$. Prove that

$$c_1R \cap c_2R... \cap c_nR = c_1c_2...c_nR$$

As before, we can follow that $c_1c_2...c_nR \subseteq c_1R \cap c_2R... \cap c_nR$ by a straightforward application of the definition.

Now the proof of 7.25 (particularly the IH part) gives us that

$$c_1c_2...c_nR + c_{n+1}R = R$$

namely throught the deriviation that

$$c_1R + c_3R = R$$

$$c_2R + c_3R = R$$

$$c_1u_1 + c_3w_1 = 1$$

$$c_2u_2 + c_3w_2 = 1$$

$$(c_1u_1 + c_3w_1)(c_2u_2 + c_3w_2) = 1$$

$$c_1c_2u_1u_2 + c_3c_1u_1w_2 + c_3... = c_1c_2u_1u_2 + c_3(...) = 1$$

thus we fllow that

$$c_1R \cap c_2R \cap c_3R = (c_1R \cap c_2R) \cap c_3R = c_1c_2R \cap c_3R = c_1c_2c_3R$$

which by induction givesus the desired result.

(c) Prove that (a) may be false if R is not a PID by giving a counterexample for the ring $F[x, y]$ where F is a field.

Let us look at $xF[x, y]$ and $yF[x, y]$. We follow that if $q \in xF[x, y] \cap yF[x, y]$, then every sum element of q is a multiple of x and y, and thus xy, thus implying that $q \in xyR$, and the reverse inclusion is also trivial. However, we have that

$$1 \notin xF[x, y] + yF[x, y]$$

which implies the desired result.

7.4.4

Prove the generalized version of the CRT

We're going to try to replicate the proof of the version 2 here, but with additional points. Thus we firstly need to prove the version for 2 ideals.

Let us denote $I = I_1 \cap I_2$. We follow that since $I_1 + I_2 = R$, that there are $i \in I_1, j \in I_2$ such that

$$i + j = 1$$

there is an obvious map

$$\psi : R \to R/I_1 \times R/I_2, \psi(r) = (r \mod I_1, r \mod I_2)$$

we then follow that if $x \in I = I_1 \cap I_2$, then $\psi(x) = (x \mod I_1, x \mod I_2) = (0, 0)$, thus implying that $I \subseteq \ker(\psi)$. (by mod here we mean standart addition of the cosets, the same as in the chapter).

Now assume that $r \in \ker(\psi)$. We follow that $r + I_1 = I_1$ and $r + I_2 = I_2$, thus we have that $r \in I_1$ and $r \in I_2$, and thus $r \in I$. Therefore we conclude that $I \subseteq \ker(\psi)$, and thus $\ker(\psi) = I$.

Thus we have an injective homomorphism

$$\phi : R/I \to R/I_1 \times R/I_2$$

we've aasumed in the beginning that $i + j = 1$, and thus we have that $i = 1 - j$, and $j = 1 - i$. We follow that

$$\phi(1 - j) = \phi(i) = (i + I_1, 1 - j + I_2) = (0, 1)$$

and similar for the other case, which implies that ψ is surjective, as desired.

Now for the inductive step. We're going to state it only for the case of 3, which can be generalized further. We follow that there are $i_1 \in I_1, i_2 \in I_2, i_{3,1}, i_{3,b2} \in I_3$ such that

$$i_1 + i_{3,1} = 1$$

$$i_2 + i_{3,2} = 1$$

thus giving us that

$$(i_1 + i_{3,1})(i_2 + i_{3,2}) = 1$$

$$i_1 i_2 + i_1 i_{3,2} + i_{3,1} i_2 + i_{3,1} i_{3,2} = 1$$

we follow that

$$i_1 i_{3,2} + i_{3,1} i_2 + i_{3,1} i_{3,2} \in I_3$$

and

$$i_1 i_2 \in I_1 \cap I_2$$

which implies that there are $q \in I_1 \cap I_2, r \in I_3$ such that

$$q + r = 1$$

thus givin us the fact that

$$I_1 \cap I_2 + I_3 = R$$

this is the point where our previous proof will kick in, and by the same deriviation as in the original proof, we get the desired result.

Skipping the rest of the exercises

7.5 Field of Fractions

7.5.1

Prove the following results, which are needed to complete the proof of Theorem 7.30

(a) Prove that the relation $(a, b) \equiv (a', b')$ defined by $ab' = a'b$ is an equivalence relation.

Firstly it's obvious that

$$ab = ab$$

thus giving us the reflexivily. Symmetry is also kinda trivial. If

$$(a_1, b_1) \equiv (a_2, b_2), (a_2, b_2) \equiv (a_3, b_3)$$

then we follow that

$$a_1 b_2 = a_2 b_1, a_2 b_3 = a_3 b_2$$

we thus can multiply both equations to get

$$a_1b_2a_2b_3 = a_2b_1a_3b_2$$

since R is an indegral domain, we follow that we can cancel and thus

$$a_1a_2b_3 = a_2b_1a_3$$

$$a_1b_3 = b_1a_3$$

thus implying that

$$(a_1, b_1) \equiv (a_3, b_3)$$

which is the desired conclusion.

(b) If $(a_1', b_1') \equiv (a_1, b_1)$ and $(a_2', b_2') \equiv (a_2, b_2)$, prove that their multiplication is well-defined

We can follow that we need to prove that

$$(a_1'a_2', b_1'b_2') \equiv (a_1a_2, b_1b_2)$$

by definition of the multiplication. Thus we need to prove that

$$a_1'a_2'b_1b_2 = a_1a_2b_1'b_2'$$

by definition of $\equiv$. By our assumptions we have that

$$a_1'b_1 = a_1b_1'$$

$$a_2'b_2 = a_2b_2'$$

Thus we have

$$a_1'a_2'b_1b_2 = a_1a_2b_1'b_2'$$
$$a_1'b_1a_2'b_2 = a_1b_1'a_2b_2'$$
$$(a_1'b_1)(a_2'b_2) = a_1b_1'a_2b_2'$$
$$(a_1b_1')(a_2b_2') = a_1b_1'a_2b_2'$$
$$a_1b_1'a_2b_2' = a_1b_1'a_2b_2'$$

(which you can chain, or use the same thing as in the proof for the addition to get a solid proof).

(c) Prove that the map λ defined by 7.23 is a field homomorphism from F to K.

We can follow that

$$\lambda(1,1) = \phi(1) * \phi(1)^{-1} = \phi(1) * \phi(1) = 1 * 1 = 1$$

where we follow that $\phi(1) = 1$ by the fact that it's a homomorphism (with 1's in their respective rings/fields).

We also have

$$\lambda((a,b)+(c,d)) = \lambda((ad+bc,bd)) =$$
$$= \phi(ad+bc) * \phi(bd)^{-1}$$
$$\lambda(a,b) + \lambda(c,d) = \phi(a) * \phi(b)^{-1} + \phi(c) * \phi(d)^{-1} =$$
$$= \phi(a) * \phi(b)^{-1} * 1 + \phi(c) * \phi(d)^{-1} * 1 = \phi(a) * \phi(b)^{-1} * 1 + \phi(c) * \phi(d)^{-1} * 1 =$$
$$= \phi(a) * \phi(b)^{-1} * \phi(d) * \phi(d)^{-1} + \phi(c) * \phi(d)^{-1} * \phi(b) * \phi(b)^{-1} =$$
$$= \phi(ad) * \phi(b)^{-1} * \phi(d)^{-1} + \phi(cb) * \phi(d)^{-1} * \phi(b)^{-1} =$$
$$= (\phi(ad) + \phi(cb)) * \phi(b)^{-1} * \phi(d)^{-1} = (\phi(ad+cb)) * \phi(bd)^{-1}$$

which states that addition is fine, and we also have that

$$\lambda((a,b) * (c,d)) = \lambda((ac,bd)) = \phi(ac) * \phi(bd)^{-1}$$

$$\lambda((a,b)) * \lambda((c,d)) = \phi(a) * \phi(b)^{-1} * \phi(c) * \phi(d)^{-1} = \phi(ac) * \phi(bd)^{-1}$$

which provess that multiplication is also fine, thus proving that λ is indeed a homomorphism, as desired

7.5.2

Let F be a field. An informal definition of the projective line is that it is the union

$$P^1(F) = F \cup \{\infty\}$$

of the field F and one extra point "at infinity". Then for $\alpha \in F$, we define an evaluation map

$$E_\alpha : F(X) \to P^1(F)$$

as follows. For rational functions $\phi \in F(X)$, we write $\phi(X) = f(X)/g(X)$ as a ration of polynomials having no common factors in $F[X]$, and then we set

$$E_\alpha(\phi) = \begin{cases} f(\alpha)/g(\alpha) \text{ if } g(\alpha) \neq 0 \\ \infty \text{ if } g(\alpha) = 0 \end{cases}$$

(a) Prove that $E_\alpha(\phi)$ is well-defined; i.e. that is does not depend on the choice of f and g.

Let $\phi \in F(X)$. We know that $F(X)$ is a field of fractions, and thus assume that $(f_1, g_1), (f_2, g_2)$ are both representations of ϕ. We follow that by definition

$$f_1 g_2 = f_2 g_1$$

We know also that $F[X]$ is PID, and thus a UFD. Therefore we follow that we can deconstruct f_1, g_1 into irreductible polynomials, and then remove common factors, (or the factors that differ by multiplication by a unit). Thus we can get $f, g \in F[X]$ with such property. Since we've removed common factors, we follow that there is a product of those factors q, and thus we have that

$$f_1 = fq, g_1 = gq$$

and thus we have that

$$f_1 gq = fqg_1$$

and since $F[X]$ is an integral domain we follow that

$$f_1 g = fg_1$$

thus concluding that

$$(f_1, g_1) \sim (f, g)$$

thansitivity of $\sim$ implies that

$$(f_2, g_2) \sim (f, g)$$

Now we've proven that two representations of a rational "function" can be mapped into one single pair of polynomials, that have no common factors, but we don't have that outputting pair is unique. And it does not have to be, since we can differ for example factors of polynomials in R by a unit, and get different pair. Thus we still need to prove that if (f, g) and (f', g') are both polynomials, that have no common factors that are equivalent to each other, then their quotient at α is the same.

Since $(f, g) \sim (f', g')$ we have that

$$fg' = f'g$$

and therefore we have

$$(fg')(\alpha) = (f'g)(\alpha)$$

or in other words

$$E_\alpha(fg') = E_\alpha(f'g)$$

evaluation of $F[X]$ is a ring homomorphism, thus giving us that

$$E_\alpha(fg') = E_\alpha(f)E_\alpha(g') = E_\alpha(fg') = E_\alpha(f')E_\alpha(g)$$

or in other words

$$f(\alpha)g'(\alpha) = f'(\alpha)g(\alpha)$$

we then can follow that if $g'(\alpha), g(\alpha) \neq 0$, then

$$f(\alpha)g(\alpha)^{-1} = f'(\alpha)g'(\alpha)^{-1}$$

which gets us the desired result. If $g(\alpha) = 0$ and $g'(\alpha) \neq 0$, then we follow that there is $q \in F[X]$ such that

$$g = q(x - \alpha)$$

by exercise 5.1. Since $g'(\alpha) \neq 0$ we follow that $(x - \alpha)$ is not a factor of g'. But we have that

$$fg'(\alpha) = f'g(\alpha) = 0$$
$$f(\alpha)g'(\alpha) = 0$$
$$f(\alpha) = 0$$

thus implying that f is also factored by $(x - \alpha)$, thus implying that f and g have common factors, which is false. And in conclusion we have that if $g(\alpha) = g'(\alpha) = 0$, then $E_\alpha(\phi) = \infty$, which implies the desired result.

Skip this one

7.5.3

This exercise describes a generalization of the construction of the field of fractions. Let R be a ring. A subset $S \subseteq R$ is said to be multiplicatively closed if it has the following properties:

$$1 \in S \text{ and } 0 \notin S$$

and

$$\text{If } a, b \in S \text{ then } ab \in S$$

We define an equivalence relation $\sim_S$ on the set of paints $(a, b) \in R \times S$ by

$$(a, b) \sim_S (a', b') \iff cab' = ca'b \text{ for some } c \in S$$

and we write R_S for the set of equivalence classes. We define addition and multiplication on R_S exactly as we did for the field of fractions.

Little note: for this chapter we assume that rings are all associative, and also we are not assuming that R_S is a afield, only indicating that it is a ring.

(a) Prove that $\sim_S$ is an equivalence relation

We follow that for $(a, b), (a', b'), (a'', b'') \in R \times S$ we have

$$ab = ab \Rightarrow (a, b) \sim_S (a, b)$$

thus giving us reflexivity. We also follow that if

$$(a, b) \sim_S (a', b')$$

then there is $c \in S$ such that

$$cab' = ca'b \Rightarrow (a', b') \sim_S (a, b)$$

thus giving us symmetry. We also have that if

$$(a,b) \sim_S (a',b') \wedge (a',b') \sim_S (a'',b'')$$

then there are $c, c' \in S$ such that

$$cab' = ca'b \wedge c'a'b'' = c'a''b'$$

and therefore we can just as before multiply both sides to get

$$cab'c'a'b'' = ca'bc'a''b'$$

$$cb'c'a'(ab'') = ca'c'b'(a''b)$$

setting $q = cb'c'a'$ we get

$$q(ab'') = q(a''b)$$

thus proving that

$$(a,b) \sim_S (a'',b'')$$

thus giving us transitivity and the desired result.

(b) Prove that addition and multiplication on R_S are well-defined.

Let $(a_1,b_1),(a_1',b_1'),(a_2,b_2),(a_2',b_2') \in R \times S$ be such that

$$(a_1,b_1) \sim_S (a_1',b_1'), (a_2,b_2) \sim_S (a_2',b_2')$$

We follow that

$$(a_1,b_1) + (a_2,b_2) = (a_1b_2 + a_2b_1, b_1b_2)$$

$$(a_1',b_1') + (a_2',b_2') = (a_1'b_2' + a_2'b_1', b_1'b_2')$$

thus we need to show that there is $c \in S$ such that

$$c(a_1b_2 + a_2b_1)(b_1'b_2') = c(a_1'b_2' + a_2'b_1')(b_1b_2)$$

we then pull the same trick as in the book

$$0 = 0$$

$$(c_1a_1b_1' - ca_1'b_1) = (c_2a_2'b_2 - c'a_2b_2')$$

$$c_1(a_1b_1' - a_1'b_1) = c_2(a_2'b_2 - a_2b_2')$$

we then multiply lhs by c_2 and rhs by c_1 (which we can do since both are still zero)

$$c_1c_2(a_1b_1' - a_1'b_1) = c_1c_2(a_2'b_2 - a_2b_2')$$

we then set $c = c_1c_2$ and get that

$$cb_2b_2'(a_1b_1' - a_1'b_1) = cb_1b_1'(a_2'b_2 - a_2b_2')$$

$$ca_1b_2b_1'b_2' - ca_1'b_2'b_1b_2 = ca_2'b_1'b_1b_2 - ca_2b_1b_1'b_2'$$

$$ca_1b_2b_1'b_2' + ca_2b_1b_1'b_2' = ca_1'b_2'b_1b_2 + ca_2'b_1'b_1b_2$$

$$(ca_1b_2 + ca_2b_1)(b_1'b_2') = (ca_1'b_2' + ca_2'b_1')(b_1b_2)$$

$$c(a_1b_2 + a_2b_1)(b_1'b_2') = c(a_1'b_2' + a_2'b_1')(b_1b_2)$$

which is precisely the desired result.

We could've also simplified this proof by firstly stating that if

$$(a_1, b_1) \sim_S (a_1', b_1'), (a_2, b_2) \sim_S (a_2', b_2')$$

then there are $c_1, c_2 \in S$ such that

$$c_1a_1b_1' = c_1a_1'b_1, c_2a_2b_2' = c_2a_2'b_2$$

and therefore we follow that

$$c_1c_2a_1b_1' = c_1c_2a_1'b_1, c_1c_2a_2b_2' = c_1c_2a_2'b_2$$

and thus there is a single $c = c_1c_2 \in S$ (product is in S since it's multiplicatively closed) such that

$$ca_1b_1' = ca_1'b_1, ca_2b_2' = ca_2'b_2$$

For multiplication we gotta prove that

$$(a_1, b_1) * (a_2, b_2) = (a_1a_2, b_1b_2)$$

$$(a_1', b_1') * (a_2', b_2') = (a_1'a_2', b_1'b_2')$$

By our assumptions and previous paragraph we have that there is $c \in S$ such that

$$ca_1'b_1 = ca_1b_1'$$

$$ca_2'b_2 = ca_2b_2'$$

which then workd out in the same manner, as our proof for intergal domains

(c) Prove that R_S with the indicated addition and multiplication is a ring. The ring R_S is called the localization of R in S.

We firstly follow that the identitiies proof is the same as in the usual field of fractions, same goes for distributivity. For identity we need to prove that $(0, 1) \not\sim_S (1, 1)$, thus firstly assume that $(0, 1) \sim_S (1, 1)$. Then we have that there is $c \in S$ such that

$$0 * 1 * c = 1 * 1 * c \Rightarrow 0 = 1$$

which is not true by the assumption that R is a ring.

The fact that R_S under plus is commutative follows directly from the definition, we follow that for $(a, b) \in R_S$ we have that

$$(a, b) + (-a, b) = (ab - ba, bb) = (0, ab) = (0, 1)$$

thus proving inverses for the addition. We also follow that

$$((a_1, b_1)+(a_2, b_2))+(a_3, b_3) = (a_1b_2+a_2b_1, b_1b_2)+(a_3, b_3) = (a_1b_2b_3+a_2b_1b_3+a_3b_1b_2, b_1b_2b_3)$$

$$(a_1, b_1)+((a_2, b_2)+(a_3, b_3)) = (a_1, b_1)+(a_2b_3+a_3b_2, b_2b_3) = (a_1b_2b_3+a_2b_3b_1+a_3b_2b_1, b_1b_2b_3)$$

thus giving us the associativity and proving that R is indeed an abelian group under $+$.

The only thing that is left for the ring properties is associativity, which is also trivial:

$$((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) = (a_1a_2a_3, b_1b_2b_3) = (a_1, b_1) * ((a_2, b_2) * (a_3, b_3))$$

One note: we see that in all of the given proofs we have denominators being products of elements of S, which by assumption of S give us the fact that they aren't 0.

Here we are also note why this thing is a ring, and not a field: R_S is a cartesian of R and S, which implies that if $q \in R \setminus S$ and $q \neq 0$, then $(q, 1) \neq 0$ for example may not have an inverse in R_S since $(1, q) \notin R_S$. If $R \setminus S = \{0\}$ however, then

$$(a, b) * (b, a) = (ab, ab)$$

but here we can have a problem that there might be the case that $ab = 0$ since R is not an integral domain, which would imply that $(ab, ab) \notin R_S$.

(d) Suppose that R is an integral domain and that S is multiplicatively closed. Prove that R_S is a subring of the field of fractions of R.

If R is an integral domain, then we follow that there is indeed a field of fractions. R_S in this case by the way it's defined is indeed a subset of a field of fractions, with the same addition and multiplication functions, and as proven in the previous point it is a ring, thus making it a subring of the field of fractions.

(e) Let I be an ideal of R and let

$$S = R \setminus I$$

Prove that S is multiplicatively closed if and only if I is a prime ideal.

Here we're gonna assume that I is given as an ideal, and then multiplicative closuse of S is followed directly, as indicated in the definition in the book.

(f) Let $b \in R$ be an element, and let

$$\langle b \rangle = \{1, b^1, b^2, ...\}$$

be the set of powers of b. Prove that $\langle b \rangle$ is multiplicatively closed if and only if b is not nilpotent.

Suppose that $\langle b \rangle$ is multiplicatively closed. We follow that there are no $q, w \in \langle b \rangle$ such that $qw = 0$ since $qw \in \langle b \rangle$ and $0 \notin \langle b \rangle$. Thus we conclude that there are no $m, n \in Z$ such thaht $b^m b^n = 0$, and thus b is not nilpotent, as desired.

If b is not nilpotent, then we follow that there is no $m \in Z$ such that $b^m = 0$. We follow that $1 \in \langle b \rangle$, $0 \notin \langle b \rangle$, and if $b^m, b^n \in \langle b \rangle$ for some $m, n \in Z$ then $b^m b^n \in \langle b \rangle$, as desired.

Skipping the rest due to triviality

7.6 Multivariate and Symmetric Polynomials

7.6.1

Let F be a field, let $F(x, y)$ be the 2-variable field of rational functions as described in Definition 7.34. For $(b, c) \in F^2$, we might try to define an evaluation-at-(b, c) map

$$E_{b,c} : F(x, y) \to F, \frac{f(x, y)}{g(x, y)} \to \frac{f(b, c)}{g(b, c)}$$

but just as in the 1-variable case, things may go wrong if we get 0 in the denominator. In this exercise we look at what might happen for the functiion

$$\phi(x, y) = \frac{x}{x^2 + y^2} \in F(x, y)$$

(a) If $F = R$, prove that $E_{b,c}(\phi)$ is well-defined except at the one point $(0, 0)$

We can easily follow that $x^2 + y^2 = 0 \Leftrightarrow x = 0 \wedge y = 0$ by various methods.

(b) If $F = C$, for which points $(b, c) \in C^{@}$ is $E_{b,c}\phi$ is not defined?

We have that

$$x^2 + y^2 = 0$$
$$y^2 = -x^2$$
$$y = \pm\sqrt{-x^2}$$

which is as much as I can define in this case

Chapter 8

Fields - Part 2

8.1 Algebraic Numbers and Transcendental Numbers

8.1.1

Let F be a field, let $f(x) \in F[x]$ be a non-zero polynomial, and let α be a root of $f(x)$ in some extension field of F. Prove that

$$[F(\alpha) : F] = \deg(f) \Rightarrow f(x) \text{ is irreductible in } F[x]$$

By definition we have that

$$[F(\alpha) : F] = \dim_F(F(\alpha))$$

and thus

$$\dim_F(F(\alpha)) = \deg(f) = \dim_F F[x]/f(x)F[x]$$

By the same reasoning as in proof of 8.6(b) we have that there is a well-defined surjective ring homomorphism

$$F[x]/f(x)F[x] \to F(a)$$

which is also a linear map between two F-spaces. Since this map is a linear map of spaces with the same dimension, we follow that surjectivity here implies bijectivity (see LADR for clarifications), thus making this map an isomorphism, which implies that $F[x]/f(x)F[x]$ is a field, for which by 7.16 we follow that $f(x)$ is irreductible, as desired.

8.1.2

Prove that each of the following numbers is algebraic over Q by finding a polynomial in $Q[x]$ for which it is a root:

(a) $\sqrt[n]{c}$ where $c \in Q$ and $n \geq 1$.

We can say that

$$f(x) : x^n - c$$

is such a polynomial.

(b) $\sqrt{2} + \sqrt{3}$

We can follow that

$$(\sqrt{2} + \sqrt{3})^2 = 2\sqrt{6} + 5$$

thus

$$((\sqrt{2} + \sqrt{3})^2 - 5)/2 = \sqrt{6}$$

and therefore

$$(((\sqrt{2} + \sqrt{3})^2 - 5)/2)^2 = 6$$
$$(((\sqrt{2} + \sqrt{3})^2 - 5)/2)^2 - 6 = 0$$

then we sub $\sqrt{2} + \sqrt{3}$ for x and get

$$((x^2 - 5)/2)^2 - 6 = 0.25(x^2 - 5)^2 - 6 = 0.25(x^4 - 10x^2 + 25) - 6 = \frac{1}{4}x^4 - \frac{10}{4}x^2 + \frac{1}{4}$$

which is the desired polynomial.

(c) $\sqrt[3]{2} + \sqrt{3}$.

We can follow that

$$(\sqrt[3]{2} + \sqrt{3})^0 = 1$$
$$(\sqrt[3]{2} + \sqrt{3})^1 = \sqrt[3]{2} + \sqrt{3}$$
$$(\sqrt[3]{2} + \sqrt{3})^2 = (\sqrt[3]{2})^2 + 2\sqrt[3]{2}\sqrt{3} + 3$$
$$(\sqrt[3]{2} + \sqrt{3})^3 = 2 + 3\sqrt[3]{2}^2\sqrt{3} + 9\sqrt[3]{2} + 3\sqrt{3}$$

and so on. In general we can later create a matrix with coefficients in

$$1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt{3}, \sqrt{3}\sqrt[3]{2}, \sqrt{3}(\sqrt[3]{2})^2$$

from powers to coefficients, to get a surjective matrix with nonzero kernel, which would in turn give us the desired polynomial (we need to go for at least 6th power here, and that's too tedious).

8.1.3

This exercise sketches a proof of the following resut, which says that if a number is the root of a polynomial in $Q[x]$, then it cannot be too closely approximated by rational numbers.

Let $f(x) \in Q[x]$ be a polynomial of degree $d \geq 1$. There is a positive constant $C_f > 0$ such that if $\alpha \in C \setminus Q$ is a non-rational root if $f(x)$, then

$$|p/q - \alpha| \geq C_f/q^d \text{ for all } p/q \in Q$$

Skipping the rest due to the fact that this exercise is wrong, and fixing it is a mess

8.2 Polynomial Roots and Multiplicative Subgroups

8.2.1

Suppose that R is a commutative ring that is not an integral domain. Prove that threre is a polynomial $f(x) \in R[x]$ that has more distinct roots in R than its degree.

Let $a, b \in R$ be nonzero and such that $ab = 0$. We can follow that

$$(x-a)(x-b) = x^2 - bx - ax + ab = x^2 + (-a-b)x + ab = x^2 + (-a-b)x$$

We then follow that roots for this polynomial are $a, b, 0$, which gives us the desired result.

8.2.2

Let R be a ring, let $a_1, ..., a_n \in R$, and define a set of polynomials

$$K_a = \{f(x) \in R[x] : f(a_1) = ... = f(a_n) = 0\}$$

(a) Prove that K_a is an ideal of $R[x]$.

Let $f, g \in K_a$. We follow that

$$(f+g)(a_j) = f(j) + g(j) = 0 + 0 = 0$$

and if $q \in R$ then

$$(fq)(a_j) = f(j)q(j) = 0 * q(j) = 0$$

thus proving to us that K_a is indeed an ideal, as desired.

(b) Suppose that R is an integral domain, and that $a_1, ..., a_n$ are distinct. Prove that K_a is the principal ideal of $R[x]$ generated by the polynomial $(x-a_1)...(x-a_n)$.

Firstly we follow that

$$(x-a_1)...(x-a_n) \in K_a$$

which is pretty evident. Then we follow that if $f \in K_a$ then it can be destructed as

$$(x-a_1)...(x-a_n)g(x)$$

by theorem 8.8(b), which implies the desired result.

8.2.3

Let H be the ring of quaternions.

(a) It was noted that the quadratic polynomial $x^2 + 1$ has more than two roots in H. Explain which step of the proof Theorem 8.8 goes wrong for H.

Theorem 8.8 is not applicable to H due to the fact that H is a non-commutative ring. For the case of (a) we can follow that

$$x^k - a^k = (x-a)\sum_{i=0}^{k-1} x^{k-i-1}a^i$$

is wrong:

$$i^2 - j^2 = (-1) - (-1) = 0$$

$$(i-j)(i+j) = i^2 + ij - ji + j^2 = (-1) + k + k + (-1) = k - 2$$

(b) Prove that $x^2 + 1$ has infinitely many roots in H.

We can follow that for some $h \in H$ we have that

$$h = q + xi + yj + zk$$

for some $q, x, y, z \in R$, and thus we have that

$$h^2 = (q + xi + yj + zk)^2 = (q + xi + yj + zk)(q + xi + yj + zk) =$$

$$= (q^2 + qxi + qyj + qzk) + (qxi - x^2 + xyij + xzik) +$$
$$+ (qyj + xyji - y^2 + yzjk) + (qzk + zxki + zykj - z^2) =$$

$$= (q^2 + qxi + qyj + qzk) + (qxi - x^2 + xyk - xzj) +$$
$$+ (qyj - xyk - y^2 + yzi) + (qzk + zxj - zyi - z^2) =$$

$$= (q^2 - x^2 - y^2 - z^2) + i(qx + qx + yz - zy) + j(qy - xz + qy + zx) + k(qz + xy - xy + qz) =$$

$$= (q^2 - x^2 - y^2 - z^2) + (2qx)i + (2qy)j + (2qz)k$$

We then follow that if we set $q = 0$, then $(2qx)i = (2qy)j = (2qz)k = 0$. Thus we only need to find some $x, y, z \in R$ so that

$$-x^2 - y^2 - z^2 = -1$$

in order to find appropriate root. For example we can set $x = 0$ and get

$$-y^2 - z^2 = -1$$

$$-y^2 = -1 + z^2$$

$$y^2 = 1 - z^2$$

$$y = \sqrt{1 - z^2}$$

we then follow that for any $z \in [-1, 1]$ there is an appropriate y, which gives us that

$$(\sqrt{1 - z^2}j + zk)^2 = -1$$

which gives us the desired result.

(c) Describe all the roots of $x^2 + 1$ in H

This can be easily derived from our previous formula for the square.

(d) Skip

8.2.4

Let F be a finite field of order q, and assume that q is odd.

(a) Let $a, b \in F^*$. If $a^2 = b^2$, prove that either $a = b$ or $a = -b$.

Here we only use the assumption that F is an integral domain. Namely we have that

$$a^2 = b^2 \Leftrightarrow a^2 - b^2 = 0 \Rightarrow (a - b)(a + b) = 0 \Rightarrow a = b \vee a = -b$$

as desired.

(b) Show by the way of example that (a) is not true for the rings $Z/8Z$ and $Z/15Z$

We follow that

$$4^2 = 16 \equiv 0 = 0^2$$

and

$$11^2 = 121 \equiv 1 \equiv 196 = 14^2$$

as desired.

(c) Let

$$R = \{a^2 : a \in F^*\}, N = F^* \setminus R$$

be, respectively, the set of squares and non-squares in F^*. Prove that R and N each contain exactly $(q - 1)/2$ elements.

Since F^* is a finite subset of itself, and F is a finite field, we follow that F^* is a cyclic group under multiplication. This gives us the fact that there is w such that for each $a \in F^*$ there is $n \in N$ such that

$$a = w^n$$

thus we then follow that either n is odd or even, which in conjuction with the fact that $|F^*| = q - 1$ gives us the desired result.

(d) Let $f(x)$ be the polynomial

$$f(x) = x^{(q-1)/2} - 1$$

Prove that R is exactly the set of roots of $f(x)$ in F.

We follow that if $a^2 \in R$ then

$$(a^2)^{(q-1)/2} = a^{q-1}$$

since $a \in F^*$ we follow that its order j (which is finite since F^* is finite) divideds the order of F^*, and thus

$$a^{q-1} = a^{jk} = e^k = 1$$

which gives us that all elements of R are roots of the given polynomial. Since

$$|R| = (q-1)/2$$

we follow that f is fully destructed by elements of R, which implies that R is a comlete set of roots of f, as desired.

(e) Let $c \in F^*$. Prove that

$$c^{(q-1)/2)} \equiv \begin{cases} c \in R \Rightarrow 1 \\ c \in N \Rightarrow -1 \end{cases}$$

Presuming that there is a typo and the author meant R instead of Q.

We follow that if $x \in F^*$ then

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

we also follow that

$$(x^{(q-1)/2} - 1)(x^{(q-1)/2} + 1) = x^{q-1} - 1$$

The fact that $(x^{(q-1)/2} - 1)$ destructs by R is the previous point, which gives us the desired resut.

(f) Let $a_1, a_2 \in R$ and $b_1, b_2 \in N$. Prove that

$$a_1 a_2 \in R, b_1 b_2 \in R$$

We can follow that for $a_1, a_2 \in R$ there are even $m, n \in N$ such that

$$a_1 = w^m, a_2 = w^n$$

thus

$$a_1 a_2 = w^{mn}$$

since mn is even, we follow that it's in R, as desired. Similar reasoning holds for b, but in it we follow that sum of odd numbers is even.

8.2.5

Let F be a finite field with q elements, and let $m|q-1$.

(a) Prove that F^* has a unique subgroup of order m.

F^* is a cyclic group, and exercise 2.27(b) implies the desired result.

(b) Let $\alpha \in F^*$. Prove that the following are equivalent:

(i) α is an mth power in F (i.e. there's $\beta \in F^*$ such that $\beta^m = \alpha$).

(ii) $\alpha^{(q-1)/m} = 1$

Assuming (i) we follow that

$$\alpha^{(q-1)/m} = \beta^{q-1} = 1$$

by Lagrange or whatever

Assuming (ii) we follow that there is an element β that generates F^*, and $n \in Z$ such that

$$\alpha = \beta^n$$

thus

$$\alpha^{(q-1)/m} = \beta^{n(q-1)/m} = 1$$

thus we follow that

$$(q-1)|n(q-1)/m$$

thus there is $i \in Z$ such that

$$i(q-1) = n * (q-1)/m$$

thus $n/m \in Z$ (there's gotta be a better way to phrase this) and thus $m|n$. Therefore there is $j \in Z$ such that $n = mj$, and therefore

$$\alpha = \beta^n = \beta^{mj} = (\beta^j)^m$$

as desired.

(c) Suppose that q is odd. Prove that

$$-1 \textit{ is a square in } F^* \Leftrightarrow q \equiv 1 \mod 4$$

Suppose that -1 is a square. We follow then that there is $\beta \in F^*$ such that

$$\beta^2 = -1$$

thus

$$(-1)^{(q-1)/2} = 1$$

and therefore there is $j \in Z$ such that

$$(q-1)j = (q-1)/2$$

$$2(q-1)j = (q-1)$$

$$2(q-1)j + 1 = q$$

Since q is odd we follow that $q-1$ is even. Since F is a field, it's a ring, and by our standarts it's got to have at least two elements, and therefore $q \geq 3 \Rightarrow q-1 \geq 2$. Thus there is $l \in N$ such that $q-1 = 2l$. Thus

$$q = 2(q-1)j + 1 = 2 * 2 * l * j + 1$$

modding both sides by 4 gives the desired result.