PMATH347S18 - Groups & Rings

Classnotes for Spring 2018

by

Johnson Ng

BMath (Hons), Pure Mathematics major, Actuarial Science Minor

University of Waterloo

Table of Contents

List of Definitions

List of Theorems

Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on:
  `https://japorized.github.io/TeX_notes`

1 Lecture 1 May 02nd 2018

1.1 Introduction

1.1.1 Numbers

The following are some of the number sets that we are already familiar with:

$$\mathbb{N} = \{1, 2, 3, ...\} \qquad \mathbb{Z} = \{.., -2, -1, 0, 1, 2, ...\}$$
$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \right\} \qquad \mathbb{R} = \text{ set of real numbers}$$
$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i = \sqrt{-1}\} = \text{ set of complex numbers}$$

For $n \in \mathbb{Z}$, let $\mathbb{Z}_n$ denote the set of integers modulo n, i.e.

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$$

where the $[r]$, $0 \leq r \leq n-1$, are the congruence classes, i.e.

$$[r] = \{z \in \mathbb{Z} : z \equiv r \mod n\}$$

These sets share some common properties, e.g. $+$ and $\times$. Let's try to break that down to make further observation.

Note that for $R = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_n$, R has 2 operations, i.e. addition and multiplication.

Addition If $r_1, r_2, r_3 \in R$, then

- (**closure**) $r_1 + r_2 \in R$
- (**associativity**) $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$

Also, if $R \neq \mathbb{N}$, then $\exists 0 \in R$ (the **additive identity**) such that

$$\forall r \in R \quad r + 0 = r = 0 + r.$$

Also, $\forall r \in R$, $\exists (-r) \in R$ such that

$$r + (-r) = 0 = (-r) + r.$$

Multiplication For $r_1, r_2, r_3 \in R$, we have

- (**closure**) $r_1 r_2 \in R$
- (**associativity**) $r_1(r_2 r_3) = (r_1 r_2) r_3$

Also, $\exists 1 \in R$ (a.k.a the **mutiplicative identity**), such that

$$\forall r \in R \quad r \cdot 1 = r = 1 \cdot r.$$

Finally, for $R = \mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, $\forall r \in R$, $\exists r^{-1} \in R$ such that

$$r \cdot r^{-1} = 1 = r^{-1} \cdot r.$$

Note that for $R = \mathbb{Z}_n$, where $n \in \mathbb{Z}$, not all $[r] \in \mathbb{Z}_n$ have a multiplicative inverse. For example, for $[2] \in \mathbb{Z}_4$, there is no $[x] \in \mathbb{Z}_4$ such that $[2][x] = [1]$.[1]

[1] This is best proven using techniques introduced in MATH135/145.

1.1.2 Matrices

For $n \in \mathbb{N} \setminus \{1\}$, an $n \times n$ matrix over $\mathbb{R}$ [2] is an $n \times n$ array that can be expressed as follows:

[2] $\mathbb{R}$ can be replaced by $\mathbb{Q}$ or $\mathbb{C}$.

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

where for $1 \leq i, j \leq n$, $a_{ij} \in \mathbb{R}$. We denote $M_n(\mathbb{R})$ as the set of all $n \times n$ matrices over $\mathbb{R}$.

As in Section 1.1.1, we can perform **addition and multiplication** on $M_n(\mathbb{R})$.

Matrix Addition Given $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}] \in M_n(\mathbb{R})$, we define matrix addition as

$$A + B = [a_{ij} + b_{ij}],$$

which immediately gives the **closure property**, since $a_{ij} + b_{ij} \in \mathbb{R}$ and hence $A + B \in M_n(\mathbb{R})$. Also, by this definition, we also immediately obtain the **associativity property**, i.e.

$$A + (B + C) = (A + B) + C.$$

We define the zero matrix as

$$0 = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

Then we have that 0 is the **additive identity**, i.e.

$$A + 0 = A = 0 + A.$$

Finally, $\forall A \in M_n(\mathbb{R})$, $\exists(-A) \in M_n(\mathbb{R})$ (the **additive inverse**) such that

$$A + (-A) = 0 - (-A) + A.$$

Note that in this case, we also have that that the operation is **commutative**, i.e.

$$A + B = B + A.$$

Matrix Multiplication Given $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}] \in M_n(\mathbb{R})$, we define the matrix multiplication as

$$AB = [d_{ij}] \text{ where } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \in \mathbb{R}.$$

Clearly, $AB \in M_n(\mathbb{R})$, i.e. it is **closed under matrix multiplication**. Also, we have that, under such a defintion, matrix multiplication is **associative**, i.e.

$$A(BC) = (AB)C.$$

Define the identity matrix, $I \in M_n(\mathbb{R})$, as follows:

$$I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Then we have that I is the **multiplicative identity**, since

$$AI = A = IA.$$

However, contrary to matrix addition, $\forall A \in M_n(\mathbb{R})$, it is not always true that $\exists A^{-1} \in M_n(\mathbb{R})$ such that

$$AA^{-1} = I = A^{-1}A.$$

This is especially true if the **determinant** of A is 0.

Also, we can always find some $A, B \in M_n(\mathbb{R})$ such that

$$AB \neq BA,$$

i.e. matrix multiplication is not always commutative.

The common properties of the operations from above: **closure, associativity, and existence of an inverse**, are not unique to just addition and multiplication. We shall see in the next lecture that there are other operations where these properties will continue to hold, e.g. **permutations**.

2 Lecture 2 May 04th 2018

2.1 Introduction (Continued)

2.1.1 Permutations

Definition 1 (Injectivity)

Let $f : X \to Y$ be a function. We say that f is ***injective*** *(or* ***one-to-one****) if $f(x_1) = f(x_2)$ implies $x_1 = x_2$.*

Definition 2 (Surjectivity)

Let $f : X \to Y$ be a function. We say that f is ***surjective*** *(or* ***onto****) if $\forall y \in Y \; \exists x \in X \; f(x) = y$.*

Definition 3 (Bijectivity)

Let $f : X \to Y$ be a function. We say that f is ***bijective*** *if it is both* ***injective*** and ***surjective***.

Definition 4 (Permutations)

Given a non-empty set L, a permutation of L is a bijection from L to L. The set of all permutations of L is denoted by S_L.

Example 2.1.1

Consider the set $L = \{1, 2, 3\}$*, which has the following* 6 *different permutations:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Note

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

indicates the bijection $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ *with* $\sigma(1) = 1$, $\sigma(2) = 3$ *and* $\sigma(3) = 2$.

For $n \in \mathbb{N}$, we denote $S_n := S_{\{1,2,\dots,n\}}$, the set of all permutations of $\{1, 2, \dots, n\}$. Example 2.1.1 shows the elements of the set S_3.

Definition 5 (Order)

The order of a set A*, denoted by* $|A|$*, is the cardinality of the set.*

Example 2.1.2

We have seen that the order of S_3, $|S_3|$ *is* $6 = 3!$.

Proposition 1

$|S_n| = n!$

Proof

$\forall \sigma \in S_n$*, there are* n *choices for* $\sigma(1)$, $n-1$ *choices for* $\sigma(2)$*, ...,* 2 *choices for* $\sigma(n-1)$*, and finally* 1 *choice for* $\sigma(n)$. $\square$

Do elements of S_n *share the same properties as what we've seen in the numbers?* Given $\sigma, \tau \in S_n$, we can compose the 2 together to get a third element in S_n, namely $\sigma\tau$ (wlog), where $\sigma\tau : \{1, \dots, n\} \to \{1, \dots, n\}$ is given by $\forall x \in \{1, \dots, n\}$, $x \mapsto \sigma(\tau(x))$.

It is important to note that $\because$ σ, τ are **both bijective**, $\sigma\tau$ is also bijective. Thus, together with the fact that $\sigma\tau : \{1, ..., n\} \to \{1, ..., n\}$, we have that $\sigma\tau \in S_n$ by definition of S_n.

$\therefore \forall \sigma, \tau \in S_n,\ \sigma\tau, \tau\sigma \in S_n$, but $\sigma\tau \neq \tau\sigma$ in general. The following is an example of the stated case:

Example 2.1.3

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \textit{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Compute $\sigma\tau$ and $\tau\sigma$ to show that they are not equal.

Solution

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

Perhaps what is interesting is the question of: **when does commutativity occur?** One such case is when σ and τ have support sets that are disjoint[1].

[1] This is proven in A1

On the other hand, the associative property holds[2], i.e.

$$\forall \sigma, \tau, \mu \in S_n \quad \sigma(\tau\mu) = (\sigma\tau)\mu$$

[2]

Exercise 2.1.1
Prove this as an exercise.

The set S_n also has an identity element[3], namely

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

[3]

Exercise 2.1.2
Verify that the given identity element is indeed the identity, i.e.

$$\forall \sigma \in S_n \quad \sigma\varepsilon = \sigma = \varepsilon\sigma.$$

Finally, $\forall \sigma \in S_n$, since σ is a bijection, we have that its inverse function, σ^-1 is also a bijection, and thus satisfies the requirements to be in S_n. We call $\sigma^{-1} \in S_n$ to be the **inverse permutation** of σ, such that

$$\forall x, y \in \{1, ..., n\} \quad \sigma^{-1}(x) = y \iff \sigma(y) = x.$$

It follows, immediately, that

$$\sigma\left(\sigma^{-1}(x)\right) = x \wedge \sigma^{-1}\left(\sigma(y)\right) = y.$$

$\therefore$ We have that

$$\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma.$$

Example 2.1.4

Find the inverse of

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

Solution

By rearranging the image in ascending order, using them now as the object and their respective objects as their image, construct

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

It can easily (although perhaps not so prettily) be shown that

$$\sigma\tau = \varepsilon = \tau\sigma.$$

With all the above, we have for ourselves the following proposition:

Proposition 2 (Properties of S_n)

We have[4]

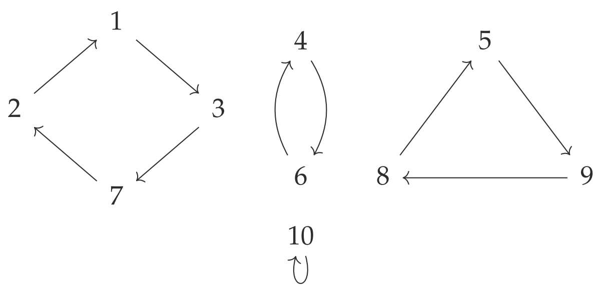
1. $\forall \sigma, \tau \in S_n \;\; \sigma\tau, \tau\sigma \in S_n$.
2. $\forall \sigma, \tau, \mu \in S_n \;\; \sigma(\tau\mu) = (\sigma\tau)\mu$.
3. $\exists \varepsilon \in S_n \;\; \forall \sigma \in S_n \;\; \sigma\varepsilon = \sigma = \varepsilon\sigma$.
4. $\forall \sigma \in S_n \;\; \exists! \sigma^{-1} \in S_n \;\; \sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$.

[4] These properties show that S_n is a group, which will be defined later.

Consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 9 & 4 & 2 & 5 & 8 & 10 \end{pmatrix} \in S_{10}$$

If we represent the action of σ geometrically, we get



We observe that σ can be **decomposed** into one 4-cycle, $\begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix}$, one 2-cycle, $\begin{pmatrix} 4 & 6 \end{pmatrix}$, one 3-cycle, $\begin{pmatrix} 5 & 9 & 8 \end{pmatrix}$, and one 1-cycle, $\begin{pmatrix} 10 \end{pmatrix}$.

Note that these cycles are (pairwise) **disjoint**, and we can write[5]

$$\sigma = \begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 5 & 9 & 8 \end{pmatrix}$$

Note that we may also write

$$\begin{aligned} \sigma &= \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 5 & 9 & 8 \end{pmatrix} \begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 6 & 4 \end{pmatrix} \begin{pmatrix} 9 & 8 & 5 \end{pmatrix} \begin{pmatrix} 7 & 2 & 1 & 3 \end{pmatrix} \end{aligned}$$

It is interesting to note that the cycles can rotate their "elements" in a **cyclic** manner, i.e.

$$\begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 7 & 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 7 & 3 \end{pmatrix}.$$

Although the decomposition of the cycle notation is not unique (i.e. you may rearrange them), each individual cycle is unique, and is proven below[6].

[5] We generally do not include the 1-cycle and assume that by excluding them, it is known that any number that is supposed to appear loops back to themselves.

[6] See bonus question of A1. Proof will be included in the notes once the assignment is over.

Theorem 3 (Cycle Decomposition Theorem)

If $\sigma \in S_n$, $\sigma \neq \varepsilon$, then σ is a product of (one or more) disjoint cycles of length at least 2. This factorization is unique up to the order of the factors.

Note (Convention)

Every permutation in S_n can be regarded as a permutation of S_{n+1} by fixing the permutation of $n+1$. Therefore, we have that

$$S_1 \subseteq S_2 \subseteq \ldots \subseteq S_n \subseteq S_{n+1} \subseteq \ldots$$

3 Lecture 3 May 07th 2018

3.1 Groups

3.1.1 Groups

Definition 6 (Groups)

Let G be a set and $*$ an operation on $G \times G$. We say that $G = (G, *)$ is a ***group*** *if it satisfies*[1]

1. ***Closure***: $\forall a, b \in G \quad a * b \in G$
2. ***Associativity***: $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$
3. ***Identity***: $\exists e \in G \;\; \forall a \in G \quad a * e = a = e * a$
4. ***Inverse***: $\forall a \in G \;\; \exists b \in G \quad a * b = e = b * a$

[1] If you wonder why the uniqueness is not specified for **Identity** and **Inverse**, see Proposition 4.

Definition 7 (Abelian Group)

A group G is said to be abelian if $\forall a, b \in G$, we have $a * b = b * a$.

Proposition 4 (Group Identity and Group Element Inverse)

Let G be a group and $a \in G$.

1. *The identity of G is unique.*
2. *The inverse of a is unique.*

Proof

1. *If $e_1, e_2 \in G$ are both identities of G, then we have*

$$e_1 \overset{(1)}{=} e_1 * e_2 \overset{(2)}{=} e_2$$

where (1) is because e_2 is an identity and (2) is because e_1 is an identity.

2. *Let $a \in G$. If $b_1, b_2 \in G$ are both the inverses of a, then we have*

$$b_1 = b_1 * e = b_1 * (a * b_2) \overset{(1)}{=} e * b_2 = b_2$$

where (1) is by associativity.

Example 3.1.1

The sets $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all abelian, where the additive identity is 0, and the additive inverse of an element r is $(-r)$.

Note

$(\mathbb{N}, +)$ is not a group for neither does it have an identity nor an inverse for any of its elements.

Example 3.1.2

*The sets $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are **not** groups, since 0 has no multiplicative inverse in $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$.*

We may define that for a set S, let $S^* \subseteq S$ contain all the elements of S that has a multiplicative inverse. For example, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Then, $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are groups and are in fact abelian, where the multiplicative identity is 1 and the multiplicative of an element r is $\frac{1}{r}$.

Example 3.1.3

The set $\left(M_n(\mathbb{R}), +\right)$ is an abelian group, where the additive identity is the zero matrix, $0 \in M_n(\mathbb{R})$, and the additive inverse of an element $M =$

$[a_{ij}] \in M_n(\mathbb{R})$ is $-M = [-a_{ij}] \in M_n(\mathbb{R})$.

Consider the set $M_n(\mathbb{R})$ under the matrix mutiplication operation that we have introduced in Lecture 1 May 02nd 2018. We found that the identity matrix is

$$I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \in M_n(\mathbb{R}).$$

But since not all elements of $M_n(\mathbb{R})$ have a multiplicative inverse[2], $(M_n(\mathbb{R}), \cdot)$ is not a group.

[2] The multiplicative inverse of a matrix does not exist if its determinant is 0.

We can try to do something similar as to what we did before: by excluding the elements that do not have an inverse. In this case, we exclude elements whose determinant is 0. We define the following set

Definition 8 (General Linear Group)

The general linear group of degree n over $\mathbb{R}$ is defined as

$$GL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}) \, : \, \det M \neq 0\}$$

Note that $\because \det I = 1 \neq 0$, we have that $I \in GL_n(\mathbb{R})$.
Also, $\forall A, B \in GL_n(\mathbb{R})$, we have that $\because \det A \neq 0 \wedge \det B \neq 0$,

$$\det AB = \det A \det B \neq 0,$$

and therefore $AB \in GL_n(\mathbb{R})$. Finally, $\forall M \in GL_n(\mathbb{R})$, $\exists M^{-1} \in GL_n(\mathbb{R})$ such that

$$MM^{-1} = I = M^{-1}M$$

since $\det M \neq 0$. $\therefore (GL_n(\mathbb{R}), \cdot)$ is a group.

Since we have introduced permutations in Lecture 2 May 04th 2018, we shall formalize the purpose of its introduction below.

Example 3.1.4

Consider S_n, the set of all permutations on $\{1, 2, ..., n\}$. By Proposition 2, we know that S_n is a group. We call S_n the ***symmetry group of degree n****. For $n \geq 3$, the group S_n is not abelian*[3].

[3] Let us make this an exercise.

Exercise 3.1.1
For $n \geq 3$, prove that the group S_n is not abelian.

NOW THAT we have a fairly good idea of the basic concept of a group, we will now proceed to look into handling multiple groups. One such operation is known as the **direct product**.

Example 3.1.5

Let G and H be groups. Their direct product is the set $G \times H$ with the component-wise operation defined by

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

where $g_1, g_2 \in G$, $h_1, h_2 \in H$, $*_G$ is the operation on G, and $*_H$ is the operation on H.

The ***closure*** *and* ***associativity*** *property follow immediately from the definition of the operation. The identity is $(1_G, 1_H)$ where 1_G is the identity of G and 1_H is the identity of H. The inverse of an element $(g_1, h_1) \in G \times H$ is (g_1^{-1}, h_1^{-1}).*

By induction, we can show that if $G_1, G_2, ..., G_n$ are groups, then so is $G_1 \times G_2 \times \ldots \times G_n$.

To facilitate our writing, use shall use the following notations:

Notation

Given a group G and $g_1, g_2 \in G$, we often denote its identity by 1, and write $g_1 * g_2 = g_1 g_2$. Also, we denote the unique inverse of an element $g \in G$ as g^{-1}.

We will write $g^0 = 1$. Also, for $n \in \mathbb{N}$, we define

$$g^n = \underbrace{g * g * \ldots * g}_{n \text{ times}}$$

and

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

With the above notations,

Proposition 5

Let G be a group and $g, h \in G$. We have

1. $(g^{-1})^{-1} = g$
2. $(gh)^{-1} = h^{-1}g^{-1}$
3. $g^n g^m = g^{n+m}$ *for all* $n, m \in \mathbb{Z}$
4. $(g^n)^m = g^{nm}$ *for all* $n, m \in \mathbb{Z}$

Exercise 3.1.2
Prove Proposition 5 as an exercise.

Warning

In general, it is not true that if $g, h \in G$, then $(gh)^n = g^n h^n$. For example,

$$(gh)^2 = ghgh \quad \text{but} \quad g^2h^2 = gghh.$$

The two are only equal if and only if G is abelian.

4 Lecture 4 May 09 2018

4.1 Groups (Continued)

4.1.1 Groups (Continued)

Proposition 6 (Cancellation Laws)

Let G be a group and $g, h, f \in G$. Then

1. (a) (**Right Cancellation**) $gh = gf \implies h = f$
   (b) (**Left Cancellation**) $hg = fg \implies h = f$
2. *The equation $ax = b$ and $ya = b$ have unique solution for $x, y \in G$.*

Proof

1. (a) *By left multiplication and associativity,*

$$gh = gf \iff g^{-1}gh = g^{-1}gf \iff h = f$$

   (b) *By right multiplication and associativity,*

$$hg = fg \iff hgg^{-1} = fgg^{-1} \iff h = f$$

2. *Let $x = a^{-1}b$. Then*

$$ax = a(a^{-1}b) = (aa^{-1})b = b.$$

If $\exists u \in G$ that is another solution, then

$$au = b = ax \implies u = x$$

by Left Cancellation. The proof for $ya = b$ is similar by letting $y = ba^{-1}$.

$\square$

4.1.2 Cayley Tables

For a finite group, defining its operation by means of a table is sometimes convenient.

Definition 9 (Cayley Table)

Let G be a group. Given $x, y \in G$, let the product xy be an entry of a table in the row corresponding to x and column corresponding to y. Such a table is called a ***Cayley Table****.*

Note

By Cycle Decomposition Theorem 6, the entries in each row (and respectively, column) of a Cayley Table are all distinct.

Example 4.1.1

Consider the group $(\mathbb{Z}_2, +)$. Its Cayley Table is

$\mathbb{Z}_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

where note that we must have $[1] + [1] = [0]$; otherwise if $[1] + [1] = [1]$ then $[1]$ does not have its additive inverse, which contradicts the fact that it is in the group.

If we replace 1 by $[0]$ and -1 by $[1]$, the Cayley Tables of $\mathbb{Z}_2$ and $\mathbb{Z}^*$ are the same. In thie case, we say that $\mathbb{Z}_2$ and $\mathbb{Z}^*$ are **isomorphic**, which we denote by $\mathbb{Z}_2 \cong \mathbb{Z}^*$.

Example 4.1.2

Consider the group $\mathbb{Z}^* = \{1. -1\}$. Its Cayley Table (under multiplication) is

$\mathbb{Z}^*$	1	-1
1	1	-1
-1	-1	1

Example 4.1.3

Given $n \in \mathbb{N}$, the **Cyclic Group** *of order n is defined by*

$$C_n = \{1, a, a^2, ..., a^{n-1}\} \quad \text{with } a^n = 1.$$

We write $C_n = \langle a : a^n = 1 \rangle$ and a is called a generator of C_n. The Cayley Table of C_n is

C_n	1	a	a^2	$\dots$	a^{n-2}	a^{n-1}
1	1	a	a^2	$\dots$	a^{n-2}	a^{n-1}
a	a	a^2	a^3	$\dots$	a^{n-1}	1
a^2	a^2	a^3	a^4	$\dots$	1	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
a^{n-2}	a^{n-2}	a^{n-1}	1	$\dots$	a^{n-4}	a^{n-3}
a^{n-1}	a^{n-1}	1	a	$\dots$	a^{n-3}	a^{n-2}

Proposition 7

Let G be a group. Up to isomorphism, we have

1. *if $|G| = 1$, then $G \cong \{1\}$.*
2. *if $|G| = 2$, then $G \cong C_2$.*
3. *if $|G| = 3$, then $G \cong C_3$.*
4. *if $|G| = 4$, then either $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$.*

K_n is known as the **Klein n-group**

Proof

1. *If $|G| = 1$, then it can only be $G = \{1\}$ where 1 is the identity element.*
2. $|G| = 2 \implies G = \{1, g\}$ *with $g \neq 1$. The Cayley Table of G is thus*

G	1	g
1	1	g
g	g	1

where we note that $g^2 = 1$; otherwise if $g^2 = g$, then we would have $g = 1$ by Cycle Decomposition Theorem 6, which contradicts the fact that $g \neq 1$. Comparing the above Cayley Table with that of C_2, we see that $G = \langle g : g^2 = 1 \rangle \cong C_2$.

3. $|G| = 3 \implies G = \{1, g, h\}$ *with* $g \neq 1 \neq h$ *and* $g \neq h$. *We can then start with the following Cayley Table:*

G	1	g	h
1	1	g	h
g	g		
h	h		

We know that by Cycle Decomposition Theorem 6, $gh \neq g$ and $gh \neq h$. Thus $gh = 1$. Similarly, we get that $hg = 1$.

<u>*Claim:*</u> *Entries in a row (or column) must be distinct. Suppose not. Then say $g^2 = 1$. But since $gh = 1$, by Cycle Decomposition Theorem 6, we have that $h = g$, which is a contradiction.*

With that, we can proceed to fill in the rest of the entries: with $g^2 = h$ and $h^2 = g$. Therefore,

G	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

Recall that the Cayley Table for C_3 is:

C_3	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

$\therefore G \cong C_3$ *(by identifying $g = a$ and $h = a^2$).*

4. ***Proof will be added once assignment 1 is over***

4.2 Subgroups

4.2.1 Subgroups

Definition 10 (Subgroup)

Let G be a group and $H \subseteq G$. If H itself is a group, then we say that H is a subgroup of G

5 Lecture 5 May 11th 2018

5.1 Subgroups (Continued)

5.1.1 Subgroups (Continued)

Note (Recall: definition of a subgroup)
Let G be a group and $H \subseteq G$. If H itself is a group, then we say that H is a subgroup of G.

Note
Since G is a group, $\forall h_1, h_2, h_3 \in H \subseteq G$, we have $h_1(h_2h_3) = (h_1h_2)h_3$. So H is a subgroup of G if it satisfies the following conditions, which we shall hereafter refer to as the Subgroup Test.

Subgroup Test

1. $h_1h_2 \in H$
2. $1_G \in H$
3. $\exists h_1^{-1} \in H$ *such that* $h_1h_1^{-1} = 1_G$

Note that the identity in H must also be the identity in G. This is because if $h_1, h_1^{-1} \in H$, then $h_1h_1^{-1} = 1_H$, but $h_1, h_1^{-1} \in G$ as well, and so $h_1h_1^{-1} = 1_G$. Thus $1_H = 1_G$.

Example 5.1.1

Given a group G, it is clear that $\{1\}$ and G are both subgroups of G.

Example 5.1.2

We have the following chain of groups:

$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$$

Recall that the general linear group is defined as:

$$GL_n(\mathbb{R}) = (GL_n(\mathbb{R}), \cdot) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$$

Definition 11 (Special Linear Group)

The special linear group of order n of $\mathbb{R}$ is defined as

$$SL_n(\mathbb{R}) = (SL_n(\mathbb{R}), \cdot) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$$

Example 5.1.3

Clearly, $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. Note that the identity matrix I must be in $SL_n(\mathbb{R})$ since $\det I = 1$. Also, $\forall A, B \in SL_n(\mathbb{R})$, we have that

$$\det AB = \det A \det B = 1$$

$\therefore AB \in SL_n(\mathbb{R})$. Also, since $\det A^{-1} = \frac{1}{\det A} = 1$, we also have that $A^{-1} \in SL_n(\mathbb{R})$. We see that $SL_n(\mathbb{R})$ satisfies the Subgroup Test, and hence it is a subgroup of $GL_n(\mathbb{R})$.

Definition 12 (Center of a Group)

Given a group G, the the center of a group G is defined as

$$Z(G) = \{z \in G : \forall g \in G \;\; zg = gz\}$$

Example 5.1.4

For a group G, $Z(G)$ is an abelian subgroup of G.

Proof

Clearly, $1_G \in Z(G)$. Let $y, z \in G$. $\forall g \in G$, we have that

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz)$$

Therefore $yz \in Z(G)$ and so $Z(G)$ is closed under its operation. Also, $\forall h \in G$, we can write $h = (h^{-1})^{-1} = g^{-1}$. Since $z \in Z(G)$, we have *that* $\forall g \in G$,

$$\begin{aligned} zg = gz \iff (zg)^{-1} = (gz)^{-1} &\iff g^{-1}z^{-1} = z^{-1}g^{-1} \\ &\iff hz^{-1} = z^{-1}h \end{aligned}$$

Therefore $z^{-1} \in Z(G)$. *By the* **Subgroup Test**, *it follows that* $Z(G)$ *is a subgroup of* G.

Finally, since $Z(G) \subseteq G$, *by its definition, we have that* $\forall x, y \in Z(G)$, $x, y \in G$ *as well, and we have that* $xy = yx$. *Therefore,* $Z(G)$ *is abelian.* □

Proposition 8 (Intersection of Subgroups is a Subgroup)

Let H *and* K *be subgroups of a group* G. *Then their intersection*

$$H \cap K = \{g \in G : g \in H \wedge g \in K\}$$

is also a subgroup of G.

Proof

Since H *and* K *are subgroups, we have that* $1 \in H$ *and* $1 \in K$ *and hence* $1 \in H \cap K$. *Let* $a, b \in H \cap K$. *Since* H *and* K *are subgroups, we have that* $ab \in H$ *and* $ab \in K$. *Therefore,* $ab \in H \cap K$. *Similarly, since* $a^{-1} \in H$ *and* $a^{-1} \in K$, $a^{-1} \in H \cap K$. *By the* **Subgroup Test**, $H \cap K$ *is a subgroup of* G. □

Proposition 9 (Finite Subgroup Test)

If H *is a finite nonempty subset of a group* G, *then* H *is a subgroup if and only if* H *is closed under its operation.*

This result says that if H is a finite nonempty subset, then we only need to prove that it is closed under its operation to prove that it is a subgroup. The other two conditions in the **Subgroup Test** are automatically implied.

Proof

The forward direction of the proof is trivially true, since H *must satisfy the closure property for it to be a subgroup.*

For the converse, since $H \neq \emptyset$, let $h \in H$. Since H is closed under its operation, we have that

$$h, h^2, h^3, \ldots$$

are all in H. Since H is finite, not all of the h^n's are distinct. Then, $\forall n \in \mathbb{N}$, there must $\exists m \in \mathbb{N}$ such that $h^n = h^{n+m}$. Then by Cancellation Laws, $h^m = 1$ and so $1 \in H$. Also, because $1 = h^{m-1}h$, we have that $h^{-1} = h^{m-1}$, and thus the inverse of h is also in H. Therefore, H is a subgroup of G as requried. $\square$

6 Lecture 6 May 14th 2018

6.1 Subgroups (Continued 2)

6.1.1 Alternating Groups

Recall that $\forall \sigma \in S_n$, with $\sigma \neq \varepsilon$, σ can be uniquely decomposed (up to the order) as disjoint cycles of length at least 2. We will now present a related concept.

Definition 13 (Transposition)

A ***transposition*** *$\sigma \in S_n$ is a cycle of length 2, i.e. $\sigma = \begin{pmatrix} a & b \end{pmatrix}$, where $a, b \in \{1, \ldots, n\}$ and a neqb.*

Example 6.1.1

We have that[1]

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

Also, we can show that[2]

$$\begin{pmatrix} 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \tag{6.1}$$

Observe that the factorization into transpositions are **not unique or disjoint**. However, the following property is true.

Theorem 10 (Parity Theorem)

[1] If we apply the permutations on the right hand side, we have that

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ & & \downarrow & & \\ 1 & 2 & 3 & 5 & 4 \\ & & \downarrow & & \\ 1 & 4 & 3 & 5 & 2 \\ & & \downarrow & & \\ 2 & 4 & 3 & 5 & 1 \end{array}$$

[2]

Exercise 6.1.1
Show that Equation 6.1 is true.

Exercise 6.1.2
Play around with the same idea and create a few of your own transpositions. Note that you will only be able to get an odd number of tranpositions (why?).

If a permutations σ has 2 factorizations

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_r = \mu_1 \mu_2 \dots \mu_s,$$

where each γ_i and μ_j are transpositions, then $r \equiv s \mod 2$.

Proof

This is the bonus question in A2. Proof shall be included after the end of the assignment.

Definition 14 (Odd and Even Permutations)

A permutation σ is even (or odd) if it can be written as a product of an even (or odd) number of transpositions. By Parity Theorem 10, a permutation must either be even or odd, but not both.

Theorem 11 (Alternating Group)

For $n \geq 2$, let A_n denote the set of all even permutations in S_n. Then

1. $\varepsilon \in A_n$
2. $\forall \sigma, \tau \in A_n \;\; \sigma\tau \in A_n$ *and* $\exists \sigma^{-1} \in A_n$ *such that* $\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$
3. $|A_n| = \frac{1}{2} n!$

Note

From items 1 and 2, we know that A_n is a subgroup of S_n. A_n is called the ***alternating subgroup of degree*** n.

Proof

1. *We have that* $\varepsilon = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$. *Thus ε is even and so $\varepsilon \in A_n$.*

2. $\forall \sigma, \tau \in A_n$, *we may write*

$$\begin{aligned} \sigma &= \sigma_1 \sigma_2 \ldots \sigma_r \quad \text{and} \\ \tau &= \tau_1 \tau_2 \ldots \tau_s, \end{aligned}$$

where σ_i, τ_j *are transpositions, and* r, s *are even integers. Then*

$$\sigma\tau = \sigma_1 \sigma_2 \ldots \sigma_r \tau_1 \tau_2 \ldots \tau_s$$

is a product of $(r + s)$ *transpositions, and thus* $\sigma\tau$ *is even. Thus* $\sigma\tau \in A_n$.

For the inverse, note that since σ_i *is a transposition, we have that* $\sigma_i^2 = \varepsilon$ *and thus* $\sigma_i^{-1} = \sigma_i$. *It follows that*

$$\begin{aligned} \sigma^{-1} &= (\sigma_1 \sigma_2 \ldots \sigma_r)^{-1} \\ &= \sigma_r^{-1} \sigma_{r-1}^{-1} \ldots \sigma_2^{-1} \sigma_1^{-1} \\ &= \sigma_r \sigma_{r-1} \ldots \sigma_2 \sigma_1 \end{aligned}$$

which is an even permutation and

$$\sigma\sigma^{-1} = \sigma_1 \sigma_2 \ldots \sigma_r \sigma_r \ldots \sigma_2 \sigma_1 = \varepsilon.$$

Thus $\exists \sigma^{-1} \in A_n$ *such that it is the inverse of* σ.

3. *Let* O_n *denote the set of odd permutations in* S_n. *Then we have* $S_n = A_n \cup O_n$, *and by the Parity Theorem, we have that* $A_n \cap O_n = \emptyset$. *Since* $|S_n| = n!$, *to prove that* $|A_n| = \frac{1}{2} n!$, *it suffices to show that* $|A_n| = |O_n|$.

Let $\gamma = \begin{pmatrix} 1 & 2 \end{pmatrix}$ *and* $f : A_n \to O_n$ *such that* $f(\sigma) = \gamma\sigma$. *Since* σ *is even,* $\gamma\sigma$ *is odd, and so* f *is well-defined.*

Also, if $\gamma\sigma_1 = \gamma\sigma_2$, *then by Cancellation Laws,* $\sigma_1 = \sigma_2$, *and hence* f *is injective.*

Finally, $\forall \tau \in O_n$, *we have that* $\gamma\tau = \sigma \in A_n$. *Note that*

$$f(\sigma) = \gamma\sigma = \gamma\gamma\tau = \tau.$$

Therefore, f *is surjective.*

It follows that $|A_n| = |O_n|$. □

For the proof of 3, we know that $|S_n| = n!$, which is twice of the suggested order of A_n. Since we took out the even permutations of S_n, we just need to make the rest of the permutations, the odd permutations, into a set and prove that A_n and this new set has the same size. One way to show this is by creating a bijection between the two.

Also, note that the set of all odd permutations of S_n is not a group, since

- there is no identity element in this set; and
- this set is not closed under map composition.

We have shown that ε is an even permutation, and so by the Parity Theorem, it cannot be an odd permutation, and there is only one identity in S_n. The set is not closed under map composition since if we compose two odd permutations, we would get an even permutation, which does not belong to this set.

6.1.2 Order of Elements

Notation

If G is a group and $g \in G$, we denote

$$\langle\, g \,\rangle = \{g^k : k \in \mathbb{Z}\}.$$

Note that $1 = g^0 \in \langle\, g \,\rangle$.

If $x = g^m, y = g^n \in \langle\, g \,\rangle$ *where* $m, n \in \mathbb{Z}$, *then*

$$xy = g^m g^n = g^{m+n} \in \langle\, g \,\rangle$$

and we have $\exists x^{-1} = g^{-m} \in \langle\, g \,\rangle$ *such that*

$$xx^{-1} = g^m g^{-m} = g^0 = 1.$$

Along with the **Subgroup Test**, we have the following proposition:

Proposition 12 (Cyclic Group as A Subgroup)

If G is a group and $g \in G$, then $\langle\, g \,\rangle$ is a subgroup of G.

Definition 15 (Cyclic Groups)

Let G be a group and $g \in G$. Then we call $\langle\, g \,\rangle$ the ***cyclic subgroup*** *of G generated by g. If $G = \langle\, g \,\rangle$ for some $g \in G$, then we say that G is a* ***cyclic group****, and g is a* ***generator*** *of G.*

7 Lecture 7 May 16th 2018

7.1 Subgroups (Continued 3)

7.1.1 Order of Elements (Continued)

Example 7.1.1

Consider $(\mathbb{Z}, +)$ *. Note that* $\forall k \in \mathbb{Z}$*, we can write* $k = k \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{k \text{ times}}$*. So we have that* $(\mathbb{Z}, +) = \langle\ 1\ \rangle$*. Similarly, we would have* $(\mathbb{Z}, +) = \langle\ -1\ \rangle$*.*

However, observe that $\forall n \in \mathbb{Z}$ *with* $n \neq \pm 1$*, there is no* $k \in \mathbb{Z}$ *such that* $k \cdot n = 1$*. Therefore,* ± 1 *are the only generators of* $\mathbb{Z}$*.*

Let G be a group and $g \in G$. Suppose $\exists k \in \mathbb{Z}$ with $k \neq 0$ such that $g^k = 1$. Then $g^{-k} = (g^k)^{-1} = 1$. Thus wlog, we can assume that $k \geq 1$. By the **Well Ordering Principle**, $\exists n \in \mathbb{N}$ such that n is the smallest, such that $g^n = 1$.

With that, we may have the following definition:

Definition 16 (Order of an Element)

Let G *be a group and* $g \in G$*. If* n *is the smallest positive integer such that* $g^n = 1$*, we say that the order of* g *is* n*, denoted by* $o(g) = n$*.*

If no such n *exists, then we say that* g *has infinite order and write* $o(g) = \infty$*.*

Proposition 13 (Properties of Elements of Finite Order)

Let G be a group with $g \in G$ where $o(g) = n \in \mathbb{N}$. Then

1. $g^k = 1 \iff n | k$;
2. $g^k = g^m \iff k \equiv m \mod n$; *and*
3. $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$ *where each g^i is distinct from others.*[1]

[1] This also means that the order of the group is the same as the order of the generator.

Proof

1. $(\impliedby)$ *If $n|k$, then $k = nq$ for some $q \in \mathbb{Z}$. Then*

$$g^k = g^{nq} = (g^n)^q = 1^q = 1$$

$(\implies)$ *Suppose $g^k = 1$. Since $k \in \mathbb{Z}$, the* **Division Algorithm**, *we can write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Note $g^n = 1$. Thus*

$$g^r = g^{k-nq} = g^k (g^n)^{-q} = 1 \cdot 1 = 1.$$

Since $0 \leq r < n$, we must have that $r = 0$. Thus $n|k$.

2. $(\implies)$ $g^k = g^m \implies g^{k-m} = 1 \overset{\text{by } 1}{\implies} n|(k-m) \iff k \equiv m \mod n$

$(\impliedby)$ $k \equiv m \mod n \implies \exists q \in \mathbb{Z} \enspace k = qnm$. *The result follows from 1.*

3. $(\supseteq)$ *is clear by definition of* $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

To prove $(\subseteq)$, let $x = g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. By the **Division Algorithm**, *$k = nq + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then*

$$x = g^k = g^{nq+r} = g^{nq} g^r \overset{\text{by } 1}{=} g^r.$$

Since $0 \leq r < n$, we have that $x \in \{1, g, g^2, ..., g^{n-1}\}$. Thus $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$.

It remains to show that all the elements in $\langle g \rangle$ are distinct. Suppose $g^k = g^m$ for some $k, m \in \mathbb{Z}$ with $0 \leq k, m < n$. By 2, we have that $k \equiv m \mod 2$. Therefore, $k = m$.

We can also use 1 by the fact that $g^{k-m} = 1$ from assumption to complete the uniqueness proof.

$\square$

Proposition 14 (Property of Elements of Infinite Order)

Let G be a group, and $g \in G$ such that $o(g) = \infty$. Then

1. $g^k = 1 \iff k = 0$;
2. $g^k = g^r \iff k = m$;
3. $\langle\, g \,\rangle = \{..., g^{-2}, g^{-1} 1, g, g^2, ...\}$ *where each g^i is distinct from others.*

Proof

It suffices to prove 1, since 2 easily becomes true with 1, and 2 $\implies$ 3.

1. $(\impliedby)$ $g^0 = 1$

   $(\implies)$ *Suppose for contradiction that $g^k = 1$ for some $k \in \mathbb{Z}$ $k \neq 0$. Then $g^{-k} = (g^k)^{-1} = 1$. Then we can assume that $k \geq 1$. This, however, implies that $o(g)$ is finite, which contradicts our assumption. Thus $k = 0$.*

2. $$g^k = g^m \iff g^{k-m} = 1 \overset{by\ 1}{\iff} k - m = 0 \iff k = m$$

$\square$

Proposition 15 (Orders of Powers of the Element)

Let G be a group, and $g \in G$ with $o(g) = n \in \mathbb{N}$. We have that

$$\forall d \in \mathbb{N} \;\; d \mid n \implies o(g^d) = \frac{n}{d}$$

Proof

Let $k = \frac{n}{d}$. Note that $(g^d)^k = g^n = 1$. It remains to show that k is the smallest such positive integer. Suppose $\exists r \in \mathbb{N}$ $(g^d)^r = 1$. Since $o(g) = n$, then $n \mid dr$. Then $\exists q \in \mathbb{Z}$ $dr = nq$ by definition of divisibility.

$\because n = dk$ *and* $d \neq 0$*, we have*

$$dr = dkq \overset{d \neq 0}{\Longrightarrow} r = kq \implies r > k \quad \because r, k \in \mathbb{N} \implies q \in \mathbb{N}$$

□

7.1.2 Cyclic Groups

Recall the definition of a cyclic groups.

Definition 17 (Cyclic Groups)

*Let G be a group and $g \in G$. Then we call $\langle\, g \,\rangle$ the **cyclic subgroup** of G generated by g. If $G = \langle\, g \,\rangle$ for some $g \in G$, then we say that G is a **cyclic group**, and g is a **generator** of G.*

Proposition 16 (Cyclic Groups are Abelian)

All cyclic groups are abelian.

Proof

Note that a cyclic group G is of the form $G = \langle\, g \,\rangle$. So

$$\forall a, b \in G \;\; \exists m, n \in \mathbb{Z} \;\; a = g^m \wedge b = g^n$$
$$a \cdot b = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = b \cdot a$$

□

8 Lecture 8 May 18th 2018

8.1 Subgroups (Continued 4)

8.1.1 Cyclic Groups (Continued)

Note

Consider the converse of Proposition 16: Are abelian groups cyclic? No! For example, $K_4 \cong C_2 \times C_2$ is abelian but not cyclic, since no one element can generate the entire group.

Proposition 17 (Subgroups of Cyclic Groups are Cyclic)

Every subgroup of a cyclic group is cyclic.

Proof

Let $G = \langle\, g \,\rangle$ and H be a subgroup of G.

$$\begin{aligned} H = \{1\} &\implies H = \langle\, 1 \,\rangle \\ H \neq \{1\} &\implies \exists k \neq 0 \in \mathbb{Z} \;\; g^k \in H \\ &\implies g^{-k} \in H \quad (\because H \text{ is a group }) \end{aligned}$$

We may assume that $k \in \mathbb{N}$. By the **Well Ordering Principle**, let $m \in \mathbb{N}$ be the smallest positive integer such that $g^m \in H$. We will now show that $H = \langle\, g^m \,\rangle$.

$$
\begin{aligned}
g^m \in H &\implies \langle\, g^m \,\rangle \subseteq H \\
\because H \subseteq G = \langle\, g \,\rangle &\quad \forall h \in H\ \exists k \in \mathbb{Z}\ h = g^k \\
\textit{Division Algorithm} &: \exists q, r \in \mathbb{Z}\ 0 \leq r < m \quad k = mq + r \\
h = g^k &\implies g^r = g^{k-mq} = g^k (g^m)^{-q} \in H \\
r \neq 0 &\implies \exists 0 < r < m \quad g^r \in H \quad \lightning \quad m \text{ is the smallest +ve integer} \\
&\implies g^k \in \langle\, g^m \,\rangle \implies H \subseteq \langle\, g^m \,\rangle
\end{aligned}
$$

Finally,

$$\langle\, g^m \,\rangle \subseteq H \wedge H \subseteq \langle\, g^m \,\rangle \implies H = \langle\, g^m \,\rangle$$

□

Proposition 18 (Other generators in the same group)

Let $G = \langle\, g \,\rangle$ *with* $o(g) = n \in \mathbb{N}$. *We have*

$$G = \langle\, g^k \,\rangle \iff \gcd(k, n) = 1$$

If we have k such that $g^k \in G$, and k and n are coprimes, then g^k is also a generator of G.

Proof

For $(\implies)$,

$$
\begin{aligned}
G = \langle\, g^k \,\rangle &\implies g \in \langle\, g^k \,\rangle \implies \exists x \in \mathbb{Z} \quad g = g^{kx} \\
&\implies 1 = g^{kx-1} \implies n \mid (kx - 1) \quad (\because 0 \;\; Proposition\ 13) \\
&\implies \exists y \in \mathbb{Z} \quad kx - 1 = ny \quad (\because \textit{Division Algorithm}) \\
&\implies 1 = kx + ny
\end{aligned}
$$

Then

$$
\begin{aligned}
&\because 1 \mid kx \ \wedge \ 1 \mid ny \ \wedge \ 1 = kx + ny \\
&\gcd(k, n) = 1 \qquad (\because \textit{gcd Characterization})
\end{aligned}
$$

For $(\impliedby)$, *note that* $g \in G \implies \langle\, g^k \,\rangle \subseteq G$. *It suffices to show that*

$G \subseteq \langle g^k \rangle$, *i.e.* $g \in \langle g^k \rangle$.

$$\begin{aligned} \gcd(k,n) = 1 &\implies \exists x, y \in \mathbb{Z} \;\; 1 = kx + ny \quad (\because \text{Bezout's Lemma}) \\ &\implies g = g^1 = g^{kx+ny} = (g^k)^x (g^n)^y = (g^k)^x \in \langle g^k \rangle \end{aligned}$$

□

Theorem 19 (Fundamental Theorem of Finite Cyclic Groups)

Let $G = \langle g \rangle$ with $o(g) = n \in \mathbb{N}$.

1. *H is a subgroup of $G \implies \exists d \in \mathbb{N} \;\; d \mid n \quad H = \langle g^d \rangle \implies |H| \mid n$.*
2. *$k \mid n \implies \langle g^{\frac{k}{n}} \rangle$ is the unique subgroup of G of order k.*

This is a significant result that classifies the structure of a cyclic group (hence its name). The theorem tells us that for a group with finite order, it has only finitely many subgroups, and the order of each of these subgroups are multiples of n. Inversely, there are no subgroups of G where its order is some integer that does not divide n.
Note: It is clear that $d \in \mathbb{N}$ and $d \leq n$.
In a sense, this theorem is more powerful than Proposition 17.

Proof

1. *Note*

$$0 \;\; \textit{Proposition } 17 \implies \exists m \in \mathbb{N} \;\; H = \langle g^m \rangle$$

Let $d = \gcd(m,n)$. Want to show that $H = \langle g^d \rangle$.

$$\begin{aligned} d = \gcd(m,n) &\implies d \mid m \implies \exists k \in \mathbb{Z} \;\; m = dk \\ &\implies g^m = g^{dk} = (g^d)^k \in \langle g^d \rangle \implies H \subseteq \langle g^d \rangle \\ d = \gcd(m,n) &\implies \exists x, y \in \mathbb{Z} \quad d = mx + ny \quad (\because \text{Bezout's Lemma}) \\ &\implies g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x (1) \in H \\ &\implies \langle g^d \rangle \subseteq H \\ &\therefore H = \langle g^d \rangle \end{aligned}$$

Note: $d = \gcd(m,n) \implies d \mid n \implies |H| = o(g^d) = \frac{n}{d}$
$\because 0$ Proposition 15. Thus $|H| \mid n$.

2. *Let K be a subgroup of G with order k such that $k \mid n$. By 1, we have $K = \langle g^d \rangle$ with $d \mid n$. Note that*

$$k = |K| \overset{(1)}{=} o(g^d) \overset{(2)}{=} \frac{n}{d}$$

where (1) is by Proposition 13 and (2) is by Proposition 15. Thus $d = \frac{n}{k}$ and $K = \langle g^{\frac{n}{k}} \rangle$

□

9 Lecture 9 May 22nd 2018

9.1 Subgroups (Continued 5)

9.1.1 Examples of Non-Cyclic Groups

Example 9.1.1

The Klein 4-group is

$$K_4 = \{1, a, b, c\} \text{ where } a^2 = b^2 = c^2 = 1 \text{ and } ab = c.$$

We may also write

$$K_4 = \langle\, a, b : a^2 = 1 = b^2,\ ab = ba \,\rangle.$$

Note that we can replace $(a,\ b)$ *by* $(a,\ c)$ *or* $(b,\ c)$.

Example 9.1.2

The symmetric group of degree 3 *is*

$$S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

where $\sigma^3 = \varepsilon = \tau^2$ *and* $\sigma\tau = \tau\sigma^2$. *We may also express* S_3 *as*

$$S_3 = \langle\, \sigma, \tau : \sigma^3 = \varepsilon = \tau^2,\ \sigma\tau = \tau\sigma^2 \,\rangle$$

Definition 18 (Dihedral Group)

For $n \geq 2$, *the* ***dihedral group*** *of order* $2n$ *is*

$$D_{2n} = \{1, a, ..., a^{n-1}, b, ba, ..., b^{n-1}\}$$

Recall from Assignment 1 that the dihedral group is a set of rigid motions for transforming a regular polygon back to its original position while changing the index of its vertices.

where $a^n = 1 = b^2$ and $aba = b$. Note that a represents a rotation of $\frac{2\pi}{n}$ radians, and b represents a reflection through the x-axis

Example 9.1.3

We may write the dihedral group as

$$D_{2n} = \langle\, a, b : a^n = 1 = b^2,\, aba = b \,\rangle$$

Exercise 9.1.1

Prove the following:

1. $D_4 \cong K_4$
2. $D_6 \cong S_3$

9.2 Normal Subgroup

9.2.1 Homomorphism and Isomorphism

Definition 19 (Group Homomorphism)

Let G, H be groups. A mapping

$$\alpha : G \to H$$

is called a group ***homomorphism*** *if $\forall a, b \in G$,*[1]

$$\alpha(ab) = \alpha(a)\alpha(b).$$

[1] Note that ab uses the operation of G while $\alpha(a)\alpha(b)$ uses the operation of H.

Example 9.2.1 (A classical example)

Consider the determinant map:

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^* \quad \textit{given by } A \to \det A$$

Note that $\mathbb{R}^*$ is the set of real numbers that has a multiplicative inverse.

Since

$$\det AB = \det A \det B$$

we have that the determinant map is a homomorphism.

This is a classical example to show a homomorphism, especially since the group $GL_n(\mathbb{R})$ uses **matrix multiplication** while $\mathbb{R}^*$ uses regular **arithmetic multiplication**.

Proposition 20 (Properties of Homomorphism)

Let $\alpha : G \to H$ be a group homomorphism. Then

1. $\alpha(1_G) = 1_H$
2. $\forall g \in G \;\; \alpha(g^{-1}) = \alpha(g)^{-1}$
3. $\forall g \in G \; \forall k \in \mathbb{Z} \;\; \alpha(g^k) = \alpha(g)^k$

Proof

1. *Note that*

$$\alpha(1_G)\alpha(g) = \alpha(1_G \cdot g) = \alpha(g) = \alpha(g \cdot 1_G) = \alpha(g)\alpha(1_G)$$

Thus it must be that $\alpha(1_G) = 1_H$ for only the identity of H satisfies this equation.

2. *Since H is a group, we know that*

$$1_H = \alpha(g)\alpha(g)^{-1}.$$

Now with part 1, we have that

$$\alpha(g)\alpha(g^{-1}) = \alpha(gg^{-1}) = \alpha(1_G) = 1_H = \alpha(g)\alpha(g)^{-1}.$$

By Proposition 6, we have that $\alpha(g^{-1}) = \alpha(g)^{-1}$.

3. *This is simply a result of applying the definition repeatedly, which we can then perform an induction procedure to complete the proof.* □

Definition 20 (Isomorphism)

Let G, H be groups. Consider a mapping

$$\alpha : G \to H$$

*We say that α is an **isomorphism** if it is a homomorphism and bijective.*

*If α is an isomorphism, we say that G is **isomorphic to** H, or that G and H are **isomorphic**, and denote that by $G \cong H$.*

Proposition 21 (Isomorphism as an Equivalence Relation)

1. *(Reflexive) The identity map $G \to G$ is an isomorphism.*
2. *(Symmetric) If $\sigma : G \to H$ is an isomorphism, then the inverse map $\sigma^{-1} : H \to G$ is also an isomorphism.*
3. *(Transitive) If $\sigma : G \to H$ and $\tau : H \to K$, then the composition map $\tau\sigma : G \to K$ is also an isomorphism.*

Proof

1. The identity map is clearly bijective. For all $g_1, g_2 \in G$, we have that

$$\alpha(g_1 g_2) = g_1 g_2 = \alpha(g_1)\alpha(g_2).$$

Thus the identity map is a homomorphism, and hence an isomorphism.

2. Since σ is a bijective map, its inverse σ^{-1} exists and is also a bijective map. Since σ is bijective, we have that

$$\forall h_1, h_2 \in H \;\; \exists! g_1, g_2 \in G \quad \sigma(g_1) = h_1,\, \sigma(g_2) = h_2.$$

Note that since σ has a bijective inverse, we also have

$$g_1 = \sigma^{-1}(h_1) \text{ and } g_2 = \sigma^{-1}(h_2).$$

Then since σ is a homomorphism,

$$\begin{aligned} \sigma^{-1}(h_1 h_2) &= \sigma^{-1}(\sigma(g_1)\sigma(g_2)) = \sigma^{-1}(\sigma(g_1 g_2)) \\ &= g_1 g_2 = \sigma^{-1}(h_1)\sigma^{-1}(h_2). \end{aligned}$$

3. We know that the composition map of two bijective map is bijective. Let $g_1, g_2 \in G$, then since both τ and σ are homomorphisms

$$\tau\sigma(g_1 g_2) = \tau(\sigma(g_1)\sigma(g_2)) = \tau\sigma(g_1)\tau\sigma(g_2),$$

where we note that $\sigma(g_1), \sigma(g_2) \in H$.

$\square$

Example 9.2.2

Let $\mathbb{R}^+ = \{r \in \mathbb{R} : r \geq 0\}$*. Show that* $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$*.*

Solution

Consider the map

$$\alpha : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot) \quad r \mapsto e^r,$$

where e *is the natural exponent. Note that the exponential map from* $\mathbb{R}$ *to* $\mathbb{R}^+$ *is bijective*[2]*. Also,* $\forall r, s \in \mathbb{R}$ *we have that*

$$\alpha(r+s) = e^{r+s} = e^r e^s = \alpha(r)\alpha(s).$$

Therefore, α *is an isomorphism and* $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$*.* □

[2] The image of the map covers all positive real numbers while taking all real numbers, which is the perfect candidate as a map here.

Example 9.2.3

Show that $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$*.*

Solution

Suppose, for contradiction, that $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ *is an isomorphism. In particular, we have that* τ *is onto. Then* $\exists q \in \mathbb{Q}$ *such that* $\tau(q) = 2$*. Let* $\tau(\frac{q}{2}) = \alpha$*. Since* τ *is an isomorphism, we have*

$$\alpha^2 = \tau(\frac{q}{2})\tau(\frac{q}{2}) = \tau(\frac{q}{2} + \frac{q}{2}) = \tau(q) = 2.$$

But that implies that $\alpha = \sqrt{2}$*, which is clearly not rational. Thus, we know that there is no such* τ *and*

$$(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$$

as required. □

9.2.2 Cosets and Lagrange's Theorem

Definition 21 (Coset)

Let H *be a subgroup of a group* G*.*

$$\forall a \in G \quad Ha = \{ha : h \in H\} \quad \text{is the right coset of } H \text{ generated by } a$$

and

$$\forall a \in G \quad aH = \{ah : h \in H\} \quad \text{is the left coset of } H \text{ generated by } a$$

Note

Note that $1H = H = H1$. Also, since $a1 = a$ and $1 \in H$, we have that $a \in aH$, and similarly so for $a \in Ha$.

In general, aH and Ha are not subgroups of G. For example, we know that A_n is a subgroup of S_n. But if σ is an odd permutation, then σA_n and $A_n \sigma$ are sets of odd permutations since A_n is the set of even permutations. As proven before, O_n, the set of odd permutations is not a subgroup of S_n.

Also, in general, $aH \neq Ha$, since not all groups are abelian.

Proposition 22 (Properties of Cosets)

Let H be a subgroup of G, and let $a, b \in G$. Then

1. $Ha = Hb \iff ab^{-1} \in H$. *In particular,* $Ha = H \iff a \in H$.
2. $a \in Hb \implies Ha = Hb$.
3. $Ha = Hb \veebar Ha \cap Hb = \emptyset$.[3] *Then the distinct right cosets of H forms a partition of G.*[4]

We can create an analogued version of this proposition for the left cosets.

[3] $\veebar \equiv$ XOR

[4] Note that this is true because by definition, we iterate over all elements of G to construct the cosets of the subgroup H. The earlier part of this statement implies that cosets must be distinct (otherwise, they are the same set), and so if we take the union of these cosets, by iterating through all elements of G, we get that

$$\bigcup_{a \in G} Ha = G.$$

Summarizing the above argument, we observe that the distinct cosets partitions G.

Proof

1. For ($\implies$),

$$\begin{aligned} Ha = Hb &\implies a = 1a \in Ha = Hb \\ &\implies \exists h \in H \;\; a = hb \\ &\implies ab^{-1} = h \in H. \end{aligned}$$

For ($\impliedby$),

$$\begin{aligned} ab^{-1} \in H &\implies \forall h \in H \;\; ha = h(ab^{-1})b \in Hb \\ &\implies Ha \subseteq Hb \\ ab^{-1} \in H &\implies (ab^{-1})^{-1} = ba^{-1} \in H \\ &\implies \forall h \in H \;\; hb = h(ba^{-1})a \in Ha \\ &\implies Hb \subseteq Ha \end{aligned}$$

Let $b = 1$*. Then*

$$Ha = H \iff a \in H \qquad \because 1^{-1} = 1$$

2. *Note*

$$a \in Hb \implies \exists h \in H \;\; a = hb \implies ab^{-1} \in H \overset{\text{by 1}}{\implies} Ha = Hb$$

3. *Trivially, if* $Ha \cap Hb = \emptyset$*, we are done.*

$$\begin{aligned} &Ha \cap Hb \neq \emptyset \\ &\implies \exists x \in Ha \cap Hb \\ &\implies (x \in Ha \overset{\text{by 1}}{\implies} Hx = Hb) \wedge (x \in Hb \overset{\text{by 1}}{\implies} Hx = Hb) \\ &\implies Ha = Hb \end{aligned}$$

□

By Proposition 22, we have that G can be written as a disjoint union of cosets of a subgroup H. We now define the following terminology that we shall use for the upcoming content.

Definition 22 (Index)

Let H *be a subgroup of a group* G*. We call the number of disjoint cosets of* H *in* G *as the* ***index*** *of* H *in* G*, and denote this number by* $[G : H]$*.*

10 Lecture 10 May 23rd 2018

10.1 Normal Subgroup (Continued)

10.1.1 Cosets and Lagrange's Theorem (Continued)

Theorem 23 (Lagrange's Theorem)

*Let H be a subgroup of a **finite** group G. Then*

$$|H| \,\Big|\, |G| \text{ and } [G : H] = \frac{|G|}{|H|}$$

Proof

Since G is finite, there can only be finitely many cosets of H. Let $k = [G : H]$ and $Ha_1, Ha_2, ..., Ha_k$ be the distinct right cosets of H in G. By Proposition 22, we have that these cosets partition G, i.e.

$$G = \bigcup_{i=1}^{k} Ha_i.$$

Note that by the definition of a right coset, the map

$$H \to Hb \text{ defined by } h \mapsto hb$$

is a surjection from H to Hb. By Cancellation Laws, the map is injective, since if $hb_1 = hb_2$, then $b_1 = b_2$. Therefore, for $i = 1, ..., k$,

$$|H| = |Ha_i|.$$

Then we have

$$|G| = k\,|H| \implies |H| \;\Big|\; |G| \wedge [G:H] = k = \frac{|G|}{|H|}$$

□

Corollary 24

1. *If G is a finite group and $g \in G$, then $o(g) \,\Big|\, G$.*
2. *If G is a finite group and $|G| = n$, then $g^n = 1$.*

Proof

1. *Let $H = \langle\, g \,\rangle$. Then by Lagrange's Theorem 23, $o(g) = |H| \;\Big|\; |G|$.*
2. *For some $g \in G$, let $o(g) = m \in \mathbb{Z} \setminus \{0\}$. Then by 1, $m \mid n$ and so $g^n = (g^m)^{\frac{n}{m}} = 1$.*

□

Note

*Let $n \in \mathbb{N} \setminus \{1\}$. **Euler's Totient Function**, or more generally written as **Euler's ϕ-function** is defined as*

$$\phi(n) \equiv \Big|\{k \in \{1, ..., n-1\} \,:\, \gcd(k, n) = 1\}\Big|. \tag{10.1}$$

Note that the set $\mathbb{Z}_n^*$ under multiplication has a similar definition to the set on the RHS, since the only numbers from 1 to n that has an inverse are those that are coprime with n. Thus $\phi(n) = |\mathbb{Z}_n^*|$.

*With Corollary 24, we have **Euler's Theorem** that states that*

$$\forall a \in \mathbb{Z} \;\; \gcd(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \mod n. \tag{10.2}$$

*If $n = p$ where p is some prime number, then Euler's Theorem implies **Fermat's Little Theorem**, i.e. $a^{p-1} \equiv 1 \mod p$.*

Corollary 25

If p is prime, then every group G of order p is cyclic. In fact, $g = \langle g \rangle$ for $g \neq 1 \in G$. Hence, the only subgroup of G are $\{1\}$ and G itself.

Proof

Let $g \in G$ such that $g \neq 1$. By Corollary 24, $o(g) \mid p$. Since $g \neq 1$ and p is prime, by uniqueness of prime factorization, it must be that $o(g) = p$. Thus we can write $G = \langle g \rangle$. If H is a subgroup of G, then by Lagrange's Theorem, we have $|H| \bigm| p$. Since p is prime, we either have $|H| = 1$ or p. In other words, we either have that $H = \{1\}$ or $H = G$, respectively. $\square$

Corollary 26

Let H and K be finite subgroups of G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof

Since $H \cap K$ is a subgroup of H and of K, by Lagrange's Theorem 23, $|H \cap K| \Bigm| |H| \wedge |H \cap K| \Bigm| |K|$. By assumption that $\gcd(|H|, |K|) = 1$, we have[1] that $|H \cap K| = 1$, and hence $|H \cap K| = \{1\}$. $\square$

[1] $|H \cap K|$ is a common divisor for $|H|$ and $|K|$. But $\gcd(|H|, |K|) = 1$

10.1.2 Normal Subgroup

We have seen that given H is a subgroup of a group G and $g \in G$, gH and Hg are generally not the same.

Definition 23 (Normal Subgroup)

Let H be a subgroup of a group G. If $\forall g \in G$, we have $Hg = gH$, then we say that H is a normal subgroup of G, and write

$$H \triangleleft G$$

Example 10.1.1

$\{1\} \lhd G$ and $G \lhd G$.

Example 10.1.2

The center, $Z(G)$, of a group G is an abelian group. By Definition 23,

$$Z(G) \lhd G.$$

Example 10.1.3

If G is abelian, then every subgroup of G is normal in G.

Proposition (Normality Test)

Let H be a subgroup of G. The following are equivalent:

1. $H \lhd G$;
2. $\forall g \in G \quad gHg^{-1} \subseteq H$;
3. $\forall g \in G \quad gHg^{-1} = H$ [2]

[2] This means that

$H \lhd G \iff H$ is the only conjugate of H

11 Lecture 11 May 25th 2018

The following theorem is useful for A2. The proof is not provided in this lecture, but expect the corollary to be restated and proven in a later lecture.

Corollary

Let G be a finite group and $H, K \triangleleft G$, $H \cap K = \{1\}$ and $|H|\,|K| = |G|$. Then $G \cong H \times K$.

11.1 Normal Subgroup (Continued 2)

11.1.1 Normal Subgroup (Continued)

Note (Recall)

Recall the definition of a normal subgroup as in Definition 23. Let H be a subgroup of G. If $gH = Hg$ for all $g \in G$, then $H \triangleleft G$.

Proposition 27 (Normality Test)

Let H be a subgroup of a group G. The following are equivalent:

1. $H \triangleleft G$
2. $\forall g \in G \;\; gHg^{-1} \subseteq H$
3. $\forall g \in G \;\; gHg^{-1} = H$

Note

Note that item 3 is indeed a stronger statement that item 2. But since the statements are equivalent, while using the Normality Test, if we can show that item 2 is true, item 3 is automatically true.

Proof

(1) $\implies$ (2):

$$\begin{aligned} x \in gHg^{-1} &\implies \exists h \in H \;\; x = ghg^{-1} \\ &\implies \exists h_1 \in H \;\; gh = h_1 g \qquad \because gh \in gH = Hg \\ &\implies x = ghg^{-1} = h_1 gg^{-1} = h_1 \in H \\ &\implies gHg^{-1} \subseteq H \end{aligned}$$

(2) $\implies$ (3):

$$\begin{aligned} (2) &\implies \forall g \in G \quad gHg^{-1} \subseteq H \\ &\implies \exists g^{-1} \in G \quad g^{-1}Hg \subseteq H \\ &\implies H \subseteq gHg^{-1} \\ &\overset{(2)}{\implies} gHg^{-1} = H \end{aligned}$$

(3) $\implies$ (1):

$$\begin{aligned} (3) &\implies \forall g \in G \quad gHg^{-1} = H \\ &\implies \forall x \in gH \quad xg^{-1} \in gHg^{-1} = H \\ &\implies x \in Hg \qquad \because gg^{-1} = 1 \\ &\implies gH \subseteq Hg \end{aligned}$$

Using a similar argument, we would have $Hg \subseteq Hg$. And so $gH = Hg$ as required. □

Example 11.1.1

Let $G = GL_n(\mathbb{R})$ and $H = SL_n(\mathbb{R})$.[1] *For $A \in G$ and $B \in H$ we have*

$$\det ABA^{-1} = \det A \det B \det A^{-1} = \det A(1)\frac{1}{\det A} = 1.$$

Thus $\forall A \in G$, $ABA^{-1} \in H$. By Proposition 27, $H \lhd G$, i.e. $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.[2]

[1] Recall Definition 8 and Definition 11.

[2] **Note**
The normality is true for any field, not just $\mathbb{R}$.

Proposition 28 (Subgroup of Index 2 is Normal)

$$\forall H \text{ subgroup of } G \wedge [G : H] = 2 \implies H \triangleleft G$$

Proof

Let $a \in G$.

$$\begin{aligned}
a \in H &\implies aH = H = Ha \\
a \notin H &\implies G = H \cup Ha \implies Ha = G \setminus H \quad \because 0 \;\; \textit{Proposition } 22 \\
a \notin H &\implies G = H \cup aH \implies aH = G \setminus H \quad \because 0 \;\; \textit{Proposition } 22
\end{aligned}$$

That implies that $aH = Ha$ for any $a \in G$. Hence, by Proposition 27, $H \triangleleft G$. □

Example 11.1.2

*Let A_n be the **Alternating Group** contained by S_n.*[3] *By Proposition 28, since $[S_n : A_n] = 2$ because $S_n = A_n \cup O_n$ and O_n is a coset of A_n, we have that*

$$A_n \triangleleft S_n.$$

[3] Recall the definition of alternating group from Theorem 11 and S_n from Definition 4

Example 11.1.3

Let

$$D_{2n} = \{1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1}\}$$

*be the **Dihedral Group** of order $2n$. Since $[D_{2n} : \langle\, a\, \rangle] = 2$,*[4] *we have that*

$$\langle\, a\, \rangle \triangleleft D_{2n} \quad \because 0 \;\; \textit{Proposition } 27.$$

[4] The coset of $\langle\, a\, \rangle$ is $b\langle\, a\, \rangle$.

Let H and K be subgroups of a group G. Recall an earlier discussion: $H \cap K$ is the largest subgroup contained in both H and K.

What is the "smallest" subgroup that contains both H and K? Since $H \cap K$ is the largest, it makes sense to think about $H \cup K$. However,

$$H \cup K \text{ is a subgroup of } G \iff H \subseteq K \veebar K \subseteq H$$

While we know that $H \cup K$ can indeed be such a subgroup, the price of the restriction is too high, since it is overly restrictive.

A more "useful" construction turns out to be the **product** of the subgroups.

Definition 24 (Product of Groups)

$$HK := \{hk \,:\, h \in H,\, k \in K\}$$

However, HK is not necessarily a subgroup. For example, for $h_1k_1, h_2k_2 \in HK$, it is not necessary that $h_1k_1h_2k_2 \in HK$, since k_1h_2 is not necessarily equal to h_2k_1.

Lemma 29 (Product of Groups as a Subgroup)

Let H and K be subgroups of G. The following are equivalent:

1. *HK is a subgroup of G*
2. *$HK = KH$* [5]
3. *KH is a subgroup of G*

[5] If one of H or K is normal, then the lemma immediately kicks in.

Proof

It suffices to prove $(1) \iff (2)$, *since* $(1) \iff (3)$ *simply through exchanging H and K.*

$(1) \implies (2)$: *Let $kh \in KH$ such that $k \in K$ and $h \in H$. Their inverses are $k^{-1} \in K$ and $h^{-1} \in H$, since K and H are groups. Note that*

$$kh = (h^{-1}k^{-1})^{-1} \in HK \quad \because HK \text{ is a subgroup of } G.$$

Therefore $kh \in HK$, which implies $KH \subseteq HK$. By a similar argument, we can arrive at $HK \subseteq KH$ and so $HK = KH$.

$(2) \implies (1)$: *Note that $1 = 1 \cdot 1 \in HK$. $\forall hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. For $h_1k_1, h_2k_2 \in HK$, note that $k_1h_2 \in KH = HK$, so there exists $hk \in HK$ such that $k_1h_2 = hk$. Therefore,*

$$h_1k_1h_2k_2 = h_1hkk_2 \in HK.$$

By the Subgroup Test, HK is a subgroup of G. $\square$

Proposition 30 (Product of Normal Subgroups is Normal)

Let H and K be subgroups of G.

1. $H \triangleleft G \vee K \triangleleft G \implies HK = KH$ *is a subgroup of* G
2. $H, K \triangleleft G \implies HK = KH \triangleleft G$

Proof

1. *Without loss of generality, suppose* $H \triangleleft G$. *Then*

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH \tag{11.1}$$

   By Lemma 29, $HK = KH$ *is a subgroup of* G.

2. *Suppose* $H, K \triangleleft G$. *Then*

$$\forall g \in G \;\; \forall hk \in HK \quad g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$$

   Thus $gHKg^{-1} \subseteq HK$. *Thus by Proposition 27, we have that* $HK \triangleleft G$.

□

Note

Note that Equation (11.1) is a weaker statement than the regular normality that we have defined, since it only requires all elements of K to work instead of the entire G.

With that, we define the following notion:

Definition 25 (Normalizer)

Let H be a subgroup of G. The **normalizer of H**, *denoted by* $N_G(H)$, *is defined to be*

$$N_G(H) := \{g \in G : gH = Hg\}$$

Note

By the above definition, we immediately see that $H \triangleleft G \iff N_G(H) = G$ by Equation (11.1). Observe that since we only needed $kH = Hk$ in Equation (11.1) for all $k \in K$, we have that $k \in N_G(H)$.

Corollary 31

Let H and K be subgroups of a group G.

$$K \subseteq N_G(H) \lor H \subseteq N_G(K) \implies HK = KH \text{ is a subgroup of } G$$

The proof of Corollary 31 is embedded in the proof of Proposition 30 while using the definition of a **normalizer**.

12 Lecture 12 May 28th 2018

12.1 Normal Subgroup (Continued 3)

12.1.1 Normal Subgroup (Continued 2)

Theorem 32

If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then

$$HK \cong H \times K$$

Proof

Claim 1:

$$H \lhd G \,\land\, K \lhd G \,\land\, H \cap K = \{1\} \implies \forall h \in H \;\; \forall k \in K \quad hk = kh$$

Consider $x = hkh^{-1}k^{-1}$. Note that since $H \lhd G$, by Proposition 27, we have that $\forall g \in G$, $gHg^{-1} = H$. Then $khk^{-1} \in kHk^{-1} = H$. Thus $x = h(kh^{-1}k^{-1}) \in H$. Using a similar argument, we can get that $x \in K$. Since $x \in H \cap K = \{1\}$, we have that $hkh^{-1}k^{-1} = 1$, we have that $hk = kh$ as claimed.

Note that since $H \lhd G$, by Proposition 30, we have that HK is a subgroup of G.[1] *Define $\sigma : H \times K \to HK$ by*

$$\forall h \in H \;\; \forall k \in K \qquad \sigma\big((h,k)\big) = hk$$

[1] We do not need the more powerful statement that says that HK is a normal subgroup.

Claim 2: *σ is an isomorphism.*

Let $(h,k),(h_1,k_1) \in H \times K$. By Claim 1, note that $h_1 k = k h_1$. Therefore,

$$\begin{aligned} \sigma\big((h,k)\cdot(h_1,k_1)\big) &= \sigma\big((hh_1,kk_1)\big) = hh_1kk_1 \\ &= hkh_1k_1 = \sigma\big((h,k)\big)\sigma\big((h_1,k_1)\big) \end{aligned}$$

Thus we see that σ is a group homomorphism. Note that by the definition of HK, σ is a surjection. Also, if $\sigma\big((h,k)\big) = \sigma\big((h_1,k_1)\big)$, we have that

$$\begin{aligned} hk = h_1k_1 &\implies h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\} \\ &\implies h_1^{-1}h = 1 = k_1k^{-1} \implies h_1 = h \wedge k_1 = k. \end{aligned}$$

Thus σ is an injection, and hence σ is bijective. Therefore, σ is an isomorphism. This proves that $HK \cong H \times K$. □

An immediate result is the corollary that we were given in the last class but not proven.

Corollary 33

Let G be a finite group, $H,K \lhd G$ such that $H \cap K = \{1\}$ and $|H|\,|K| = |G|$. Then $G \cong H \times K$.

Example 12.1.1

Let $m,n \in \mathbb{N}$ with $\gcd(m,n) = 1$. Let G be a cyclic group of order mn. Write $G = \langle\, a \,\rangle$ with $o(a) = mn$. Let $H = \langle\, a^n \,\rangle$ and $K = \langle\, a^m \,\rangle$. Then we have

$$|H| = o(a^n) = m \wedge |K| = o(a^m) = n.$$

It follows that $|H|\,|K| = mn = |G|$. Note that $H \cong C_m$ and $K \cong C_n$. Since $\gcd(m,n) = 1$, by Corollary 26, we have that $H \cap K = \{1\}$.

Also, since G is cyclic and thus abelian, we have that $H,K \lhd G$. Then by Corollary 33, we have that $G \cong C_{mn} \cong C_m \times C_n$.

12.2 Isomorphism Theorems

12.2.1 Quotient Groups

Let G be a group and K a subgroup of G. Given a set

$$\{Ka : a \in G\},$$

how can we create a group out of it?

A "natural" way to define an operation on the set of right cosets above is

$$\forall a, b \in G \qquad Ka * Kb = Kab. \tag{†}$$

Note that it is entirely possible that for $a_1 \neq a$ and $b_1 \neq b$, we have $Ka = Ka_1$ and $Kb = Kb_1$. In order for Equation (†) to make sense as an operation, it is necessary that

$$Ka = Ka_1 \wedge Kb = Kb_1 \implies Kab = Ka_1 b_1.$$

If the condition is satisfied, we say that the "multiplication" $KaKb$ is well-defined.

Lemma 34 (Multiplication of Cosets of Normal Subgroups)

Let K be a subset of G. The following are equivalent:

1. $K \lhd G$;
2. $\forall a, b \in G \;\; KaKb = Kab$ *is well-defined.*

Proof

$(1) \implies (2)$ *Suppose $K \lhd G$. Suppose $Ka = Ka_1$ and $Kb = Kb_1$. Then $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To show that $Kab = Ka_1b_1$, it suffices to show that $(ab)(a_1b_1)^{-1} \in K$. Note that since $K \lhd G$, we have that $aKa^{-1} = K$. Therefore,*

$$\begin{aligned} ab(a_1b_1)^{-1} &= ab(b_1^{-1}a_1^{-1}) = a(bb_1^{-1})a_1^{-1} \\ &= \left(a(bb_1^{-1})a^{-1}\right)(aa_1^{-1}) \in K. \end{aligned}$$

Therefore $Kab = Ka_1b_1$ as required.

$(2) \implies (1)$ *If $a \in G$, we need to show that $\forall k \in K$, $aka^{-1} \in K$. Since $Ka = Ka$ and $Kk = K(1)$ [2], by (2), we have that $Kak = Ka(1)$, i.e.*

[2] This is cause 1 is in the same coset.

$Kak = Ka$. Thus $aka^{-1} = 1 \in K$, implying that $aKa^{-1} \subseteq K$ and hence $K \lhd G$. $\square$

13 Lecture 13 May 30th 2018

13.1 Isomorphism Theorems (Continued)

13.1.1 Quotient Groups (Continued)

Proposition 35

Let $K \triangleleft G$ and write $G/K = \{Ka : a \in G\}$ for the set of cosets of K.

1. *G/K is a group under the operation $KaKb = Kab$.*
2. *The mapping $\phi : G \to G/K$ given by $\phi(a) = Ka$ is a surjective homomorphism.*[1]
3. *If $[G : K]$ is finite, then $\left| G/K \right| = [G : K]$. In particular, if $|G|$ is finite, then $\left| G/K \right| = \frac{|G|}{|K|}$.*

[1]

Exercise 13.1.1
Is ϕ injective?

Solution
We know that we cannot uniquely express a coset, since for $a, b \in Ka$ such that $a \neq b$, we have that $Ka = Kb$.

Proof

1. *By Lemma 34, the operation is well-defined, and G/K is closed under the operation. The identity of G/K is $K = K(1)$ since $\forall Ka \in G/K$,*

$$KaK(1) = Ka = K(1)Ka.$$

Also, since

$$KaKa^{-1} = K(1) = Ka^{-1}Ka,$$

the inverse of Ka is Ka^{-1}. Finally, by associativity of G, we have that

$$Ka(KbKc) = Kabc = (KaKb)Kc.$$

It follows that G/K is a group.

2. *Clearly, ϕ is surjective. For $a, b \in G$,*

$$\phi(ab) = Kab = KaKb = \phi(a)\phi(b).$$

Thus ϕ is a surjective homomorphism.

3. *If $[G : K]$ is finite, then by definition of the index $[G : K]$, we have that $[G : K] = \left| {}^{G}\!/_{K} \right|$. Also, if $|G|$ is finite, then by Theorem 23,*

$$\left| {}^{G}\!/_{K} \right| = [G : K] = \frac{|G|}{|K|}.$$

□

Definition 26 (Quotient Group)

Let $K \triangleleft G$. The group ${}^{G}\!/_{K}$ of all cosets of K in G is called the ***quotient group*** *of G by K. Also, the mapping*

$$\phi : G \to {}^{G}\!/_{K} \text{ defined by } a \mapsto Ka$$

is called the ***coset*** *(or* ***quotient****)* ***map****.*

13.1.2 Isomorphism Theorems

Definition 27 (Kernel and Image)

Let $\alpha : G \to H$ be a group homomorphism. The ***kernel*** *of α is defined by*

$$\ker \alpha := \{ g \in G : \alpha(g) = 1_H \} \subseteq G$$

and the image of α is defined by

$$\operatorname{im} \alpha := \alpha(G) = \{ \alpha(g) : g \in G \} \subseteq H.$$

Proposition 36

Let $\alpha : G \to H$ be a group homomorphism.

1. $\operatorname{im}\alpha$ *is a subgroup of* H

2. $\ker\alpha \lhd G$

Proof

1. *Note that* $1_H = \alpha(1_G) \in \alpha(G)$ *(i.e. the identity is in* $\operatorname{im}\alpha$*). Also, for* $h_1 = \alpha(g_1)$ *and* $h_2 = \alpha(g_2)$ *in* $\alpha(G)$ *and* $h_1, h_2 \in H$*, we have*

$$h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G).$$

(i.e. $\operatorname{im}\alpha$ *i closed under its operation). By Proposition 20,* $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$ *(i.e. the inverse of an element is also in* $\operatorname{im}\alpha$*). Thus by the* **Subgroup Test***, we have that* $\operatorname{im}\alpha$ *is a subgroup of* H*.*

2. *For* $\ker\alpha$*,* $\alpha(1_G) = 1_H$*. For* $k_1, k_2 \in \ker\alpha$*, we have*

$$\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1 \cdot 1 = 1.$$

Also,

$$\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1.$$

By the **Subgroup Test***,* $\ker\alpha$ *is a subgroup of* G*.*

If $g \in G$ *and* $k \in \ker\alpha$*, then*

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g)\alpha(g^{-1}) = 1.$$

Thus by Proposition 27, $\ker\alpha \lhd G$*.*

□

Example 13.1.1

Consider the determinant map

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^* \text{ defined by } A \mapsto \det A.$$

Then $\ker\det = SL_n(\mathbb{R})$*. Then* $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$*, as proven before.*

Example 13.1.2

Define the ***sign of a permutation*** $\sigma \in S_n$ *by*

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even;} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Then the sign mapping, $\operatorname{sgn} : S_n \to \{\pm 1\}$ *defined by* $\sigma \mapsto \operatorname{sgn}(\sigma)$ *is a homomorphism.*[2] *Also,* $\ker \operatorname{sgn} = A_n$*. Thus, we have* $A_n \triangleleft S_n$*, as proven before.*

[2] Think about why. It's quite straightforward using the defintion.

Proposition 37 (Normal Subgroup as the Kernel)

If $K \triangleleft G$*, then* $K = \ker \phi$ *where* $\phi : G \to G/K$ *is the coset map.*

Proof

Recall that $\phi : G \to G/K$ *is defined by* $g \mapsto Kg$*,* $\forall g \in G$*, and is a group homomorphism. By Proposition 22, we have*

$$Kg = K = K1 \iff g \in K.$$

Thus $K = \ker \phi$. $\square$

Theorem 38 (First Isomorphism Theorem)

Let $\alpha : G \to H$ *be a group homomorphism. We have*

$$G/\ker \alpha \cong \operatorname{im} \alpha$$

Proof

Let $K = \ker \alpha$*. Since* $K \triangleleft G$ *(by Proposition 36),* G/K *is a group. Let*[3]

$$\bar{\alpha} : G/K \to \operatorname{im} \alpha \text{ be defined by } Kg \mapsto \alpha(g)$$

[3] We must check that the function is well-defined, since cosets are not uniquely represented and so it is likely that a constructed mapping is not well-defined.

Note that

$$Kg = Kg_1 \iff gg_1^{-1} \in K \iff \alpha(gg_1^{-1}) = 1 \iff \alpha(g) = \alpha(g_1).$$

Thus $\bar{\alpha}$ *is well-defined and injective. Clearly,* $\bar{\alpha}$ *is surjective. It remains to* *show that $\bar{\alpha}$ is a group homomorphism. $\forall g, h \in G$, we have*

$$\bar{\alpha}(KgKh) = \bar{\alpha}(Kgh) = \alpha(gh) = \alpha(g)\alpha(h) = \bar{\alpha}(Kg)\bar{\alpha}(Kh).$$

Therefore, we have that $\bar{\alpha}$ is an isomorphism and hence $G/_{\ker\alpha} \cong \operatorname{im}\alpha$ as desired. $\square$

14 Lecture 14 Jun 01st 2018

14.1 Isomorphism Theorems (Continued 2)

14.1.1 Isomorphism Theorems (Continued)

Note (Recall)

In First Isomorphism Theorem 38, we had that for a group homomorphism $\alpha : G \to H$ where G and H are groups,

$$G/\ker\alpha \cong \operatorname{im}\alpha$$

Now let $\alpha : G \to H$ be a group homomorphism, $K = \ker\alpha$, $\phi : G \to G/K$ be the coset map, and $\bar{\alpha}$ be as defined in the proof of First Isomorphism Theorem 38. We then have the following commutative diagram to illustrate the relationship between the three groups.

$$\begin{tikzcd}
G \arrow[r, "\alpha"] \arrow[d, "\phi"'] & H \\
G/K \arrow[ur, "\bar{\alpha}"'] &
\end{tikzcd}$$

A natural question to ask after seeing the relationship is: Is $\bar{\alpha}\phi = \alpha$? If it is, is the definition of $\bar{\alpha}$ unique? The answer is: **YES!** on both accounts.

Proof

Let $g \in G$. Then

$$\bar{\alpha}\phi(g) = \bar{\alpha}\big(\phi(g)\big) = \bar{\alpha}(Kg) = \alpha(g)$$

Suppose $\alpha = \beta\phi$ where $\beta : {}^{G}\!/_{K} \to H$. Then

$$\beta(Kg) \overset{(1)}{=} \beta(\phi(g)) = \beta\phi(g) = \alpha(g) = \bar{\alpha}(Kg)$$

where (1) is because ϕ is surjective by Proposition 35. Therefore, we observe that $\beta = \bar{\alpha}$ for any $Kg \in {}^{G}\!/_{K}$. This proves that $\bar{\alpha}$ is the unique homomorphism such that ${}^{G}\!/_{K} \to H$ satisfying $\alpha = \bar{\alpha}\phi$. □

With that, we have the following proposition.

Proposition 39

Let $\alpha : G \to H$ be a group homomorphism, where G and H are groups. Let $K = \ker \alpha$. Then α factors uniquely as $\alpha = \bar{\alpha}\phi$< where $\phi : G \to {}^{G}\!/_{K}$ is the coset map and $\bar{\alpha} : {}^{G}\!/_{K} \to H$ is defined by

$$\bar{\alpha}(Kg) = \alpha(g).$$

Note that ϕ is surjective and $\bar{\alpha}$ is injective.

*In such a scenario, we also say that α **factors through** ϕ.*[1]

[1] Reference for the terminology: `https://math.stackexchange.com/questions/68941/terminology-a-homomorphism-factors`.

Example 14.1.1

Let $G = \langle\, g \,\rangle$ be a cyclic group. Consider $\alpha : \mathbb{Z} \to G$, defined as

$$\forall k \in \mathbb{Z} \quad \alpha(k) = g^k,$$

which is a group homomorphism. By definition, α is surjective. Note that

$$\ker \alpha = \{k \in \mathbb{Z} : g^k = 1\}.$$

We have, therefore, two cases to consider.

- *G is an infinite group*
  This would imply that $\ker \alpha = \{0\}$ since only $g^0 = 1$. Then by First Isomorphism Theorem 38, we have that

$$ {}^{\mathbb{Z}}\!/_{\ker \alpha} \cong G$$

Note that[2]

[2] We are assuming that the group $\mathbb{Z}$ here works under the operation of addition, otherwise, if we employ multiplication, then $\mathbb{Z}$ would not be a group and α would not be a group homomorphism.

$$\mathbb{Z}/_{\ker\alpha} = \{(\ker\alpha)k : k \in \mathbb{Z}\} = \{0 + k : k \in \mathbb{Z}\} = \mathbb{Z}.$$

Therefore

$$\mathbb{Z} \cong G$$

- *G is a finite group*
  Suppose that $|G| = o(g) = n \in \mathbb{N}$, *which is valid by Corollary 24. Then*
  $$\ker\alpha = n\mathbb{Z}$$
  Then by the First Isomorphism Theorem 38, we have
  $$\mathbb{Z}/_{n\mathbb{Z}} \cong G.$$
  Observe that
  $$\mathbb{Z}/_{n\mathbb{Z}} = \{n\mathbb{Z} + k : k \in \mathbb{Z}\} = \mathbb{Z}_n$$
  since the set in the middle is the definition of the set of integers modulo n.[3] *Therefore,*
  $$\mathbb{Z}_n \cong G$$
  Therefore, we have that
  $$\mathbb{Z} \cong G \text{ or } \mathbb{Z}_{o(g)} \cong G$$

[3] This is why we often see texts from various authors using $\mathbb{Z}/_{n\mathbb{Z}}$ to represent the set of integers modulo n.

Theorem 40 (Second Isomorphism Theorem)

Let H and K be the subgroups of a group G with $K \lhd G$. *Then*

- HK *is a subgroup of* G;
- $K \lhd HK$;
- $H \cap K \lhd H$; *and*
- $HK/_K \cong H/_{H \cap K}$.

Proof

Since $K \lhd G$, *by Lemma 29 and Proposition 30, we have that* $HK = KH$ *is a subgroup of* G. *Consequently, we have* $K \lhd HK$, *since* K *is clearly a subgroup of* HK *and* $K \lhd G$, *and so* $\forall x \in HK \subseteq G$ *we have that* $gK = Kg$.

Consider $\alpha : H \to {}^{HK}\!/_{K}$, *defined by*[4]

$$\alpha(h) = Kh$$

Now if $x = kh \in KH = HK$, *then*

$$Kx = K(kh) = Kh = \alpha(h).$$

Therefore, we have that α *is surjective. Now by* Proposition 22, *observe that*

$$\ker \alpha = \{h \in H : Kh = K\} = \{h \in Hh \in K\} = H \cap K.$$

Then by the First Isomorphism Theorem, we have that

$${}^{HK}\!/_{K} \cong {}^{H}\!/_{H \cap K}.$$

Since we have that $\ker \alpha = H \cap K$ *and* $\ker \alpha \triangleleft H$, *we have that* $H \cap K \triangleleft H$. □

[4] Note that $Kh \in {}^{HK}\!/_{K}$ since $h \in H \subseteq HK$.

Theorem 41 (Third Isomorphism Theorem)

Let $K \subseteq H \subseteq G$ *be groups, with* $K \triangleleft G$ *and* $H \triangleleft G$. *Then*

$${}^{H}\!/_{K} \triangleleft {}^{G}\!/_{K} \text{ and } \left({}^{G}\!/_{K}\right) \Big/ \left({}^{H}\!/_{K}\right) \cong {}^{G}\!/_{H}$$

Proof

Define $\alpha : {}^{G}\!/_{K} \to {}^{G}\!/_{H}$ *by* $\alpha(Kg) = Hg$ *for all* $g \in G$. *Clearly,* α *is surjective. Now if* $Kg = Kg_1$, *for any* $g, g_1 \in G$, *then* $gg_1 \in K \subseteq H$. *Therefore,* $Hg = Hg_1$. *Thus* α *is well-defined. Now*

$$\ker \alpha = \{Kg : Hg = H\} = \{Kg : g \in H\} = {}^{H}\!/_{K}.$$

Then

$${}^{H}\!/_{K} = \ker \alpha \triangleleft {}^{G}\!/_{K}.$$

By the First Isomorphism Theorem, we have

$$\left({}^{G}\!/_{K}\right) \Big/ \left({}^{H}\!/_{K}\right)$$

as required. □

One reason that we are interested in the symmetric group is that they contain all finite groups.

Theorem (Cayley's Theorem)

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

15 Lecture 15 Jun 04th 2018

15.1 Group Action

15.1.1 Cayley's Theorem

Theorem 42 (Cayley's Theorem)

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof

Since G is finite, let $G = \{g_1, g_2, ..., g_n\}$ and let S_G be the permutation group of G. By identifying g_i with i, where $1 \leq i \leq n$, we see that $S_G \cong S_n$ [1]*. Therefore, it suffices to find an injective homomorphism*[2] *$\sigma : G \to S_G$.*

Consider the function $\mu_a : G \to G$, where $a \in G$, such that $\mu_a(g) = ag$ for all $g \in G$. Clearly, μ_a is surjective. Suppose $\mu_a = \mu_b$, where $b \in G$. Then $a = \mu_a(1) = \mu_b(1) = b$. Thus μ_a is also injective. It follows that $\mu_a \in S_G$ by definition.

Now define the function $\sigma : G \to S_G$ such that $\sigma(a) = \mu_a$. Clearly, σ is injective, since $\sigma(a) = \sigma(b) \implies \mu_a = \mu_b$. Observe that $\sigma(ab) = \mu_{ab} = ab = \mu_a \mu_b$. Thus σ is a group homomorphism. Note that $\ker \sigma = \{1\}$, the trivial group. It follows from the First Isomorphism Theorem that $G \cong \operatorname{Im} \sigma \leq S_G \cong S_n$.[3] [4] $\square$

[1] S_G is the permutation group of G. We can think of S_G as a group of permutations that permutes the index of the elements of G. Since there are n indices, there are $n!$ ways to permute the indices, and so $|S_G| = n! = |S_n|$. Then we can certainly find some isomorphism from S_G to S_n, and so $S_G \cong S_n$.

[2] **Why do we need injectivity?** We need homomorphicity in order to invoke the First Isomorphism Theorem so that we can get $G \cong \operatorname{im} \sigma \leq S_G \cong S_n$.

[3] We shall use $H \leq G$ to denote that H is a subgroup of G from here on.

[4] This is a result from Proposition 36

Cayley's Theorem is, however, too strong at times. We can certainly find a smaller integer m such that G is contained in S_m. Consider the following example.

Example 15.1.1

Let $H \leq G$ with $[G : H] = m < \infty$. Let $X = \{g_1 H, g_2 H, ..., g_m H\}$ be the set of all distinct left cosets of H in G [5]*. For $a \in G$, define $\lambda_a : X \to X$ by $\lambda_a(gH) = agH$, $gH \in X$.*

Note that λ_a is a bijection[6]*, and so $\lambda_a \in S_X$, the permutation group of X. Consider the mapping $\tau : G \to S_X$ defined by $\tau(a) = \lambda_a$ for $a \in G$. Note that $\forall a, b \in G$, $\lambda_{ab} = \lambda_a \lambda_b$. Thus τ is a homomorphism. Note that if $a \in \ker \tau$, then $aH = H$ which implies $a \in H$ by Proposition 22. Thus $\ker \tau \subseteq H$.*

[5] This is simply a consequence of $[G : H] = m$.

[6] This is true as shown in the proof above, but it can also serve as a tiny exercise.

From the example above, if we apply the First Isomorphism Theorem, then

$$G/\ker \tau \cong \operatorname{im} \tau \leq S_X \cong S_m \leq S_n.$$

This is the result that we desired.

Theorem 43 (Extended Cayley's Theorem)

Let $H \leq G$ with $[G : H] = m < \infty$. If G has no normal subgroup contained in H except for the trivial subgroup $\{1\}$, then G is isomorphic to a subgroup of S_m.

Proof

By our assumption, let X be the set of all distinct left cosets of H in G. Then we have that $|X| = m$ and so $S_X \cong S_m$ [7]*. From Example 15.1.1, we have that there exists a group homomorphism $\tau : G \to S_X$ with $K := \ker \tau \subseteq H$. So by the First Isomorphism Theorem, we have that*

$$G/K \cong \operatorname{im} \tau.$$

Since $K \subseteq H$ and $K \lhd G$, we have, by assumption, that $K = \{1\}$. It follows that

$$G \cong \operatorname{im} \tau \leq S_X \cong S_m.$$

$\square$

[7] This is as argued in the proof of Cayley's Theorem.

Corollary 44

Let $|G| = m \in \mathbb{N}$ and p the smallest prime such that $p \big| m$. If $H \leq G$ with $[G : H] = p$, then $H \triangleleft G$.

Proof

Let X be the set of all distinct left cosets of H in G. We have $|X| = p$ and so $S_X \cong S_p$. Let $\tau : G \to S_X \cong S_p$ be as defined in Example 15.1.1, with $K := \ker \tau \subseteq H$. By the First Isomorphism Theorem, we have that

$$G/K \cong \operatorname{im} \tau \leq S_X \cong S_p,$$

i.e. G/K is isomorphic to a subgroup of S_p. Therefore, by Lagrange's Theorem, we have that $\left| G/K \right| \Bigg| \, p!$.

Also, since $K \subseteq H$, if $[H : K] = k \in \mathbb{N}$, then

$$\left| G/K \right| \overset{(1)}{=} \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = pk,$$

where (1) is by Proposition 35. Therefore we have that $pk \mid p!$ and so $k \mid (p-1)!$.

Note that $k \mid |H|$ [8], which divides $|G|$, and p is the smallest prime dividing $|G|$. Thus evrey prime divisor of k must be $\geq p$.[9] Thus $k = 1$, which implies that $K = H$. Therefore, $H \triangleleft G$ as desired. □

[8] This is clear since $|H| = k|K|$.

[9] By the **Fundamental Theorem of Arithmetic**, and since k is finite, let $k = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, where p_i's are distinct primes and $a_i \in \mathbb{N}$ are the multiplicities of the i^{th}, and by the **Well-Ordering Principle**, let $p_i < p_{i+1}$. Then we have, for some $b = b_1^{c_1} b_2^{c_2} \ldots b_j^{c_j} \in \mathbb{N}$ where the b_i's are distint primes, $b_i < b_{i+1}$, and $c_i \in \mathbb{N} \cup \{0\}$,

$$m = kb = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} b_1^{c_1} b_2^{c_2} \ldots b_j^{c_j}.$$

Since p is the smallest prime that divides m, we have

$$\begin{aligned} p &= \min\{p_1, p_2, \ldots, p_m, b_1, b_2, \ldots, b_j\} \\ &= \min\{p_1, b_1\} \end{aligned}$$

15.1.2 Group Action

Definition 28 (Group Action)

*Let G be a group, X a non-empty set. A **group action** of G on X is a mapping $G \times X \to X$ denoted as $(a, x) \to ax$ such that*

1. $1 \cdot x = x$, $x \in X$
2. $a \cdot (b \cdot x) = (ab) \cdot x$, $a, b \in G$, $x \in X$

*In this case, we say G **acts on** X.*

16 Lecture 16 Jun 06th 2018

16.1 Group Action (Continued)

16.1.1 Group Action (Continued)

Remark

Let G be a group acting on a set X. For $a, b \in G$, and $x, y \in X$, we have that

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y.$$

In particular, we have

$$a \cdot x = a \cdot y \iff x = y.$$

For $a \in G$, define $\sigma_a : X \to X$ by $\sigma_a(x) = a \cdot x$ for all $x \in X$. In A3, we will be showing that[1]:

1. $\sigma_a \in S_X$, the permutation group of X; and
2. The function $\Theta : G \to S_X$ given by $\Theta(a) = \sigma_a$ is a group homomorphism with
$$\ker \Theta = \{a \in G : a \cdot x = x, \, x \in X\}.$$

Note that the group homomorphism $\Theta : G \to S_X$ gives an **equivalent definition** of a **Group Action** of G on X. If $X = G$, $|G| = n$ and $\ker \Theta = \{1\}$ [2], then the map $\Theta : G \to S_G \cong S_n$ shows that G is isomorphic to a subgroup of S_n [3], which the equivalent statement of Cayley's Theorem.

[1] This will be added after the assignment.

[2] This is also called a **faithful group action**.

[3]

Exercise 16.1.1
Verify that G is indeed isomorphic to a subgroup of S_n using the given information and the equivalent definition of a group action.

Example 16.1.1

If G is a group, let G act on itself by $a \cdot x = a \cdot x \cdot a^{-1}$, for all $a, x \in G$. Note that the axioms of a group action is satisfied:

1. $1 \cdot x = 1 \cdot x \cdot 1^{-1} = x$; *and*
2. $a \cdot (b \cdot x) = a \cdot (b \cdot x \cdot b^{-1}) \cdot a = ab \cdot x \cdot (ab)^{-1} = (ab) \cdot x$.

In this case, we say that G ***acts on itself by conjugation****.*

Definition 29 (Orbit & Stabilizer)

Let G be a group acting on a set X, and $x \in X$. We denote by

$$G \cdot x = \{g \cdot x : \forall g \in G\}$$

the ***orbit*** *of X and*

$$S(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

the ***stabilizer*** *of X.*

There is no standardized way of expressing the orbit and the stabilizer, i.e. the notation for orbit and stabilizers will be different across many references.

Proposition 45

Let G be a group acting on a set X an $x \in X$. Let $G \cdot x$ and $S(x)$ be the orbit and stabilizer of X respectively. Then

1. $S(x) \leq G$
2. *there is a bijection from $G \cdot x$ to $\{gS(x) : g \in G\}$ and thus $|G \cdot x| = [G : S(x)]$.*

Proof

1. *Since $1 \cdot x = x$, we have $1 \in S(x)$. If $g, h \in S(x)$, then*

$$gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

i.e. $S(x)$ is closed under "composition of group action". Also note that

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x.$$

Thus the inverse of each element is also in $S(x)$. Therefore, by the ***Subgroup Test****, $S(x) \leq G$.*

2. *For the sake of simplicity, let us write $S = S(x)$. Consider the map*

$$\phi : G \cdot x \to \{gS(x) : g \in G\}$$

defined by $\phi(g \cdot x) = gS$ [4]*. To verify that the map is well-defined, note that*

$$\begin{aligned} g \cdot x = h \cdot x &\iff (h^{-1}g) \cdot x = x = 1 \cdot x \\ &\iff \phi(h^{-1}g \cdot x) = \phi(1 \cdot x) \\ &\iff h^{-1}gS = 1 \cdot S = S \\ &\iff gS = hS \end{aligned}$$

We also observe that ϕ is injective. It is also clear that ϕ is onto, and therefore we have that ϕ is a bijection. It follows that

$$|G \cdot x| = |\{gS : g \in G\}| = [G : S]$$

□

[4] We go with the most simplistic and rather naive kind of function here.

Theorem 46 (Orbit Decomposition Theorem)

Let G be a group acting on a non-empty finite set X. Let

$$X_f = \{x \in X : a \cdot x = x, \forall a \in G\}$$

(Note that $x \in X_f \iff |G \cdot x| = 1$)[5]

Let $G \cdot x_1$, $G \cdot x_2$, ..., $G \cdot x_n$ denote the distinct nonsingleton orbits (i.e. $|G \cdot x_i| > 1$ for all $1 \leq i \leq n$). Then

$$|X| = \left| X_f \right| + \sum_{i=1}^{n} [G : S(x_i)].$$

[5] Notice that

$$\begin{aligned} x \in X_f &\iff \forall a \in G \quad a \cdot x = x \\ &\iff \forall g \cdot x \in G \cdot x \quad g \cdot x = x \\ &\iff |G \cdot x| = 1 \end{aligned}$$

Proof

Note that for $a, b \in G$ and $x, y \in X$,

$$\begin{aligned} a \cdot x = b \cdot y &\overset{WLOG}{\iff} (b^{-1}a) \cdot x = y \\ &\iff y \in G \cdot x \\ &\overset{(1)}{\iff} G \cdot x = G \cdot y \end{aligned}$$

where (1) *is the conclusion after consider the other case where* $(a^{-1}b) \cdot y = x$.

Thus, we see that the two orbits are either disjoint or the same, but not both. It follows that the orbits form a disjoint union of X. *Since* $x \in X_f \iff |G \cdot x| = 1$, *the set* $X \setminus X_f$ *contains all nonsingleton orbits, which are disjoint. It follows that*

$$|X| = \left|X_f\right| + \sum_{i=1}^{n} |G \cdot x_i| \overset{(2)}{=} \left|X_f\right| + \sum_{i=1}^{n} [G : S(x_i)]$$

where (2) *is by* 💧 *Proposition 45.* $\square$

17 Lecture 17 Jun 08th 2018

17.1 Group Action (Continued 2)

17.1.1 Group Action (Continued 2)

Note (Recall Theorem 46)

Let G act on a finite set $X \neq \emptyset$. Let[1]

$$X_f = \{x \in X : a \cdot x = x,\ a \in G\}$$

Let $G \cdot x_1, G \cdot x_2, \ldots, G \cdot x_n$ be distinct nonsingleton orbits (ie. $|G \cdot x_i| > 1$). Then

$$|X| = \left|X_f\right| + \sum_{i=1}^{n} [G : S(x_i)].$$

[1] X_f is also called the set of elements of X that are fixed by the action of G.

Example 17.1.1 (Conjugacy Class & Centralizer)

Let G be a finite group acting on itself by ***conjugation****. In the context of Theorem 46, we have that*

$$\begin{aligned} X &= G \\ G_f &= \{x \in G : gxg^{-1} = x,\ g \in G\} \\ &= \{x \in G : gx = xg,\ g \in G\} = Z(G), \end{aligned}$$

where we recall that $Z(G)$ is the center of G. Now for any $x \in G$, we have

$$G \cdot x = \{gxg^{-1} : g \in G\},$$

which is known as the ***conjugacy class*** *of x. We also have*

$$S(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C_G(x),$$

which is called the ***centralizer*** *of x.*

Putting the above example with Theorem 46, we have the following corollary.

Corollary 47 (Class Equation)

Let G be a finite group and $\{gx_1g^{-1} : g \in G\}$, ..., $\{gx_ng^{-1} : g \in G\}$ denote the distinct nonsingleton conjugacy classes. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)].$$

Lemma 48

Let G be a group of order p^m, where p prime and $m \in \mathbb{N}$, which acts on a finite set X. Let

$$X_f = \{x \in X : a \cdot x = x, \, a \in G\}.$$

Then we have

$$|X| \equiv \left| X_f \right| \mod p$$

Proof

By the Orbit Decomposition Theorem, we have that

$$|X| = \left| X_f \right| + \sum_{i=1}^{n} [G : S(x_i)],$$

where $[G : S(x_i)] > 1$ for $1 \leq i \leq n$. For any x_i, by Lagrange's Theorem, $[G : S(x_i)] \mid |G| = p^m$. Since $[G : S(x_i)] > 1$, we have, by the ***Fundamental Theorem of Arithmetic****, that $[G : S(x_i)]$ must be a multiple of p, i.e. p divides $[G : S(x_i)]$, for all i. Therefore, $p \mid \left(|X| - \left| X_f \right| \right)$, i.e.*

$$|X| \equiv \left| X_f \right| \mod p,$$

as required. $\square$

Recall Lagrange's Theorem: If G is finite and $g \in G$, then

$$o(g) \mid |G| .$$

An interesting question to ask here is: Is the converse true? I.e., given a group G with an integer m such that $m \mid |G|$, does G contain an element of order m?

Consider K_4, the Klein 4-group. Note that all elements of K_4 have order at most 2, but $4 \mid |K_4| = 4$.

Now if m is some prime, is the converse still true?

Theorem 49 (Cauchy's Theorem)

Let p be a prime, G be a finite group. If $p \mid |G|$, then G contains an element of order p.

Proof (McKay)

Let $|G| = n$. Suppose $p \mid n$. Let

$$X = \{(a_1, ..., a_p) : a_i \in G,\ a_1 \ldots a_p = 1\}.$$

Note that $X \neq \emptyset$, since $(1, ..., 1) \in X$ (so the proof is not vacuous). Take any $a_1, ..., a_{p-1} \in G$, then a_p is uniquely determined, i.e.

$$a_p = (a_1 \ldots a_{p-1})^{-1}.$$

Now for each a_i, we have n choices, thus $|X| = n^{p-1}$.[2]

Let $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ act on X by "cycling", i.e. $\forall k \in \mathbb{Z}_p$,

$$k \cdot (a_1, a_2, ..., a_p) = (a_{k+1}, a_{k+2}, ..., a_p, a_1, ..., a_k).$$

[3] *Note that*

$$\begin{aligned}(a_1, ..., a_p) \in X_f &\iff \text{every cycled shift of } (a_1, ..., a_p) \text{ is itself} \\ &\iff a_1 = a_2 = \ldots = a_p \text{ and } a_1 a_2 ... a_p = 1\end{aligned}$$

i.e. all of the components of the p-tuple are the same. Now if $(a_1, ..., a_p)$ has at least 2 distinct components, then its orbits must have p elements.

[2] Convince yourself why this is true.

[3] We want to use Theorem 46 from here.

In other words, for some $r \in \mathbb{N}$, for each $1 \leq i \leq r$, we have that $[G : S(x_i)] = p$. Then, by the Orbit Decomposition Theorem,

$$n^{p-1} = |X| = \left|X_f\right| + \sum_{i=1}^{r} [G : S(x_i)]$$
$$\left|X_f\right| = n^{p-1} - rp.$$

We observe that $\left|X_f\right|$ is indeed divisible by p and is non-zero, since $(1, ..., 1) \in X_f$. Therefore, there exists some $a \neq 1 \in G$, such that $(a, ..., a) \in X_f$, i.e. $a^p = 1$. We know that p is the smallest power by construction, and therefore $o(a) = p$ as required. □

18 Lecture 18 Jun 13th 2018

18.1 Finite Abelian Groups

18.1.1 Primary Decomposition

Note (Notation)

Let G be an abelian group and $m \in \mathbb{Z}$. We define

$$G^{(m)} := \{g \in G : g^m = 1\}$$

Proposition 50 (Group of Elements of the Same Order is a Subgroup)

Let G be an abelian group. Then $G^{(m)} \leq G$.

Proof

Note that $1^m = 1 \in G^{(m)}$. $\forall g, h \in G^{(m)}$, since G is abelian, we have that[1]

$$(gh)^m = g^m h^m = 1 \cdot 1 = 1.$$

Therefore $gh \in G^{(m)}$. Also, for $g \in G^{(m)}$, we have

$$\left(g^{-1}\right)^m = (g^m)^{-1} = 1.$$

Thus $g^{-1} \in G^{(m)}$. By the **Subgroup Test***, we have that $G^{(m)} \leq G$.* $\square$

[1] Pay attention that this is only true if G is abelian.

Proposition 51 (Decomposition of a Finite Abelian Group)

Let G be a finite abelian group with $|G| = mk$ such that $\gcd(m,k) = 1$. Then

1. $G \cong G^{(m)} \times G^{(k)}$*; and*
2. $\left|G^{(m)}\right| = m$ *and* $\left|G^{(k)}\right| = k$.

Proof

1. *Since G is abelian, $G^{(m)} \lhd G$ and $G^{(k)} \lhd G$.*

   Claim 1: $G^{(m)} \cap G^{(k)} = \{1\}$
   Proof of Claim 1: $\forall g \in G^{(m)} \cap G^{(k)}$, $g^m = 1 = g^k$
   $\because \gcd(m,k) = 1$, *by Bezout's Lemma*, $\exists x, y \in \mathbb{Z} \quad 1 = mx + ky$
   $\implies g = g^1 = g^{mx+ky} = (g^m)^x (g^k)^y = 1 \cdot 1 = 1$
   $\implies G^{(m)} \cap G^{(k)} = \{1\}$ *as claimed.*

   Claim 2: $G = G^{(m)} G^{(k)}$ [2]
   $\forall g \in G \quad \because o(g) = mk \quad 1 = g^{mk} = (g^k)^m = (g^m)^k$
   *It follows that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. From **Claim 1** and by abelianness, we have that*

   $$g = g^{mx+ky} = (g^k)^y (g^m)^x \in G^{(m)} G^{(k)}$$

   Thus $G \subseteq G^{(m)} G^{(k)}$. On the other hand, since $G^{(m)} \lhd G$ and $G^{(k)} \lhd G$, by Lemma 29, we have that $G^{(m)} G^{(k)} \leq G$ and hence $G^{(m)} G^{(k)} \subseteq G$. Thus $G = G^{(m)} G^{(k)}$ as claimed.

   *From **Claims 1 and 2**, we can conclude by Corollary 33* [3]*, that $G \cong G^{(m)} \times G^{(k)}$ as required.*

2. *Write $\left|G^(m)\right| = m'$ and $\left|G^{(k)}\right| = k'$. By part (1), we have that $mk = |G| = m'k'$.*

   Claim 3: $\gcd(m, k') = 1$
   Suppose not
   $\implies \exists p$ *prime* $\quad p \mid m$ *and* $p \mid k'$
   $\implies \exists g \in G^{(k)} \quad o(g) = p \qquad \because$ *Cauchy's Theorem*
   Now $p \mid m \implies \exists q \in \mathbb{Z} \quad m = pq$
   $\implies g^m = g^{pq} = 1 \quad \because o(g) = p$
   $\implies g \in G^{(m)}$.
   By part (1), we have that $g \in G^{(m)} \cap G^{(k)} = \{1\} \implies g = 1$, which

[2] Recall that this is the Product

[3] Should this not be Theorem 32?

contradicts the fact that $o(g) = p$. *Thus* $\gcd(m, k') = 1$ *as claimed. Similarly, we can get that* $\gcd(m', k) = 1$.

Notice that $mk = m'k' \implies m \mid m'k'$
$\implies m \mid m' \quad \because \gcd(m, k') = 1$ *and similarly* $k \mid k'$. *But then* $mk = m'k'$ *would imply that* $m' = m$ *and* $k' = k$.

$\square$

As a direct consequence of Proposition 51, we have the following:

Theorem 52 (Primary Decomposition)

Let G *be a finite abelian group with* $|G| = p_1^{n_1} \dots p_k^{n_k}$, *where* $p_1, ..., p_k$ *are distinct primes, and* $n_1, ..., n_k \in \mathbb{N}$. *Then*

1. $G \cong G^{\left(p_1^{n_1}\right)} \times \dots \times G^{\left(p_k^{n_k}\right)}$; *and*
2. $\forall i \; 1 \leq i \leq k \quad \left| G^{\left(p_i^{n_i}\right)} \right| = p_i^{n_i}$.

18.1.2 p-Groups

On a related note of the groups $G^{\left(p_i^{n_i}\right)}$, we define the following:

Definition 30 (p-Group)

Let p *be a prime. A* ***p-group*** *is a group in which every element has an order that is a non-negative power of* p.

Proposition 53 (p-Groups are Finite)

A finite group G *is a p-group* $\iff$ $|G|$ *is a power of* p *(including* p^0*).*

Proof

($\Longleftarrow$) *If* $|G| = p^\alpha$ *for some* $\alpha \in \mathbb{N} \cup \{0\}$ *and* $g \in G$, *by* Corollary 24, $o(g) \mid p^\alpha$

$\implies$ *G is a p-group.*

($\implies$) *Consider the contrapositive and let* $|G| = p^n p_2^{n_2} \dots p_k^{n_k}$ *where* $p, p_2, ..., p_k$ *are distinct primes,* $n \in \mathbb{N} \cup \{0\}$, *and* $n_2, ..., n_k \in \mathbb{N}$. *For* $k \geq 2$, *by Cauchy's Theorem,* $p_2 \mid |G|$

$\implies \exists g_1 \in G \quad o(g_1) = p_2$

$\implies$ *G is not a p-group.*

Therefore, our desired result follows. □

Our end goal here is to prove to ourselves that all finite abelian groups can be written as cross products of cyclic groups, i.e. if G is an abelian group, then

$$G \cong C_1 \times C_2 \times \dots \times C_n.$$

With Theorem 52, we have that

$$G \cong G_1 \times G_2 \times \dots \times G_n.$$

The following proposition will enable us to get to our goal from our current position:

Proposition (Finite Abelian p-Groups of order p are Cyclic)

If G is a finite abelian p-group that contains only one subgroup of order p, where p is prime, then G is cyclic. In other words, if a finite abelian p-group is not cyclic, then it must have at least 2 *subgroups of order* p.

19 Lecture 19 Jun 15th 2018

19.1 Finite Abelian Groups (Continued)

19.1.1 *p*-Groups (Continued)

Note (Recall)

Recall the definition of a p-group:

G is a p-group if the order of all of its elements is a non-negative power of $p \iff |G| = p^k$ for some $k \in \mathbb{N} \cup \{0\}$.

We shall now proceed to prove the proposition mentioned by the end of last class.

Proposition 54 (Finite Abelian p-Groups of Order p are Cyclic)

If G is a finite abelian p-group that contains only 1 subgroup of order p, then G is cyclic. In other words, if a finite abelian p-group is not cyclic, then G has at least 2 subgroups of order p.

Proof

Since G is finite, let $y \in G$ have maximal order.

Claim: $G = \langle\, y \,\rangle$

***Proof of Claim**: Suppose not. Since $\langle\, y \,\rangle \triangleleft G$ [1], consider the quotient group ${}^{G}\!/\!_{\langle\, y \,\rangle}$, which is, therefore, a nontrivial p-group, since $|\langle\, y \,\rangle| = p$. By Cauchy's Theorem, we know that $\exists z \in {}^{G}\!/\!_{\langle\, y \,\rangle}$ such that $o(z) = p$ [2]. In particular, we have that $z \neq 1$ [3]. Consider the coset map*

[1] We have $\langle\, y \,\rangle \leq G$ and G is abelian.

[2] Note that we have ${}^{G}\!/\!_{\langle\, y \,\rangle}$ is a p-group $\iff \left|{}^{G}\!/\!_{\langle\, y \,\rangle}\right| = p^k$ for some $k \in \mathbb{N} \cup \{0\}$. The existence of our chosen z follows from there by Cauchy's Theorem.

[3] If $z = 1$, then its order would not be p.

$$\pi : G \to {}^{G}\!/\!_{\langle\, y \,\rangle}.$$

Let $x \in G$ such that $\pi(x) = z$ [4]*. Since*

$$\pi(x^p) = \pi(x)^p = z^p = 1,$$

we have that x^p gets mapped to 1 by π, i.e. $x^p \in \langle\, y \,\rangle$.

$\implies \exists m \in \mathbb{Z}$ *such that $x^p = y^m$. We shall consider two cases:*

***Case 1**: $p \nmid m$.*

$\because p \nmid m$, *we have that $\gcd(m, |\langle\, y \,\rangle|) = 1$, and hence by Proposition 18* [5]*, we have that $o\,(y^m) = o(y)$. Because y has maximal order, we have*

$$o(x^p) \overset{(1)}{<} o(x) \leq o(y) = o(y^m) = o(x^p)$$

where note that (1) is true because x would need to take more powers of p than x^p to get back to 1. We observe that we have arrived at a contradiction.

***Case 2**: $p \mid m$.*

$p \mid m \implies \exists k \in \mathbb{Z} \;\; m = pk \implies x^p = y^m = y^{pk}$

$\because G$ *is abelian, we have that $(xy^-k)^p = 1$.*

By assumption, there is only one subgroup of G of order p, call it H. Thus $xy^k \in H$. On the other hand, by the Fundamental Theorem of Finite Cyclic Groups [6]*, $\langle\, y \,\rangle$ has only one subgroup of of order p, which must be H. Therefore, in particular, we have $xy^{-k} \in \langle\, y \,\rangle$ which implies $x \in \langle\, y \,\rangle$. It follows that $z = \pi(x) = 1$ since $\langle\, y \,\rangle$ is the identity in the quotient group ${}^{G}\!/\!_{\langle\, y \,\rangle}$, which contradicts our choice of $z \neq 1$.*

Therefore, by combining the two cases, we have that $G = \langle\, y \,\rangle$. $\square$

[4] Recall that π is surjective by Proposition 35.

[5] **Proposition (Proposition 18)**
Let $G = \langle\, g \,\rangle$ with $o(g) = n \in \mathbb{N}$. We have

$$G = \langle\, g^k \,\rangle \iff \gcd(k, n) = 1$$

[6] **Theorem (Theorem 19)**
Let $G = \langle\, g \,\rangle$ with $o(g) = n \in \mathbb{N}$.

1. *H is a subgroup of $G \implies \exists d \in \mathbb{N} \;\; d \mid n \quad H = \langle\, g^d \,\rangle \implies |H| \mid n$.*
2. *$k \mid n \implies \langle\, g^{\frac{k}{n}} \,\rangle$ is the unique subgroup of G of order k.*

Proposition 55

Let $G \neq \{1\}$ be a finite abelian p-group that contains one subgroup of order p. Let C be the cyclic subgroup of G of maximal order. Then $\exists B \leq G$ such that $G = CB$ and $C \cap B = \{1\}$. By Corollary 33, we have $G \cong C \times B$.

Proof

We shall prove this result by induction. If $|G| = p$, then $C = G$ by definition and we can choose $B = \{1\}$. The result follows from there.

Suppose that the result holds for all groups of order p^{n-1} with $n \in \mathbb{N}$ and $n \geq 2$. Consider the case for $|G| = p^n$. There are two cases to consider from here.

***Case 1**: If $C = G$, then we can pick $B = \{1\}$ so that the result follows.*

***Case 2**: If $C \neq G$, then G is not cyclic. By Proposition 54, there exists at least 2 subgroups of G that are of order p. Since C is cyclic, by the Fundamental Theorem for Finite Cyclic Groups, we have that C contains exactly one subgroup of order p. Then $\exists D \leq G$ such that $|D| = p$ and $D \nsubseteq C$, and consequently $C \cap D = \{1\}$. Now since G is abelian, $D \triangleleft G$ and hence we may consider its coset map:*

$$\pi : G \to G/D.$$

*If we consider $\pi \restriction_C$, called the **restriction** of π on C [7], then $\ker \pi \restriction_C = C \cap D = \{1\}$. Then by the First Isomorphism Theorem, we have*

$$C = C/\ker \pi \restriction_C \cong \operatorname{im} \pi \restriction_C = \pi(C).$$

Now let y be the generator of the cyclic group C. Then since $\pi(C) \cong C$, we have $\pi(C) = \langle\ \pi(y)\ \rangle$. By assumption on C, $\pi(C)$ is the cyclic subgroup of G/D of maximal order [8]. Since $\left| G/D \right| = p^{n-1}$ by Lagrange's Theorem, and by the induction hypothesis, G/D has a subgroup E such that $\pi(C)E = G/D$ and $\pi(C) \cap E = \{1\}$.

Therefore, choose $B = \pi^{-1}(E)$, i.e. $\pi(B) = E$.

Claim 1: $G = CB$

Note that $D \subseteq B$ [9]. If $x \in G$, $\because \pi(C)\pi(B) = \pi(C)E = G/D$, we have that $\exists u \in C$, $\exists v \in B$ such that

$$\pi(x) = \pi(u)\pi(v).$$

By homomorphicity, we have $\pi(xu^{-1}v^{-1}) = 1$ which implies $xu^{-1}v^{-1} \in D \subseteq B$. Then because $v \in B$, we have that $xu^{-1} \in B$ since B is a group. Then since G is abelian, we have

$$x = uxu^{-1} \in CB.$$

Claim 2: $C \cap B = \{1\}$.

Let $x \in C \cap B$. Then $\pi(x) \in \pi(C) \cap \pi(B) = \pi(C) \cap E = \{1\}$. Then, $\because \pi(x) = 1 \in C/D$, we have that $x \in D$. Therefore, $x \in C \cap D = \{1\}$ which then $x = 1$.

[7] The restriction of π on C simply means that we restrict the domain of π to work solely for the subset C. In plain words, we are only considering the case where π is applied onto elements of C.

[8] Since $C \cong \pi(C)$, this is a clear result. Otherwise, if there is some other $\pi(K)$ that has a larger order than $\pi(C)$, then by $\pi^{-1}(K)$, we will get some cyclic subgroup that has an order that is larger than C, which is a clear contradiction to our assumption.

[9] Note that E is a subgroup of G/D, so the identity of G/D, D must be in E. Therefore, we clearly have $D \subseteq B$.

*Since **Claims 1 & 2** hold, the result follows by induction.* □

20 Lecture 20 Jun 18th 2018

20.1 Finite Abelian Groups (Continued 2)

20.1.1 p-Groups (Continued 2)

Recall that we had the following subgroup of a group G.

$$G^{(m)} = \{g \in G : g^m = 1\}.$$

We discussed about the Primary Decomposition, Theorem 52, and then arrived at Proposition 55. With these, we can have the following theorem:

Theorem 56 (Finite Abelian Groups are Isomorphic to a Direct Product of Cyclic Groups)

Let $G \neq \{1\}$ be a finite abelian p-group. Then G is isomorpic to a direct product of cylic groups.

Proof

By Proposition 55, there is a cyclic group C_1 and a subgroup B_1 of G, such that $G \cong C_1 \times B_1$. Since $B_1 \leq G$, we have that $|B_1| \bigm| |G|$, and so by Theorem 23, B_1 is also a p-group. If $B_1 \neq \{1\}$, then by Proposition 55, there exists a cyclic group C_2 and a $B_2 \leq B_1$ such that $B_1 \cong C_2 \times B_2$.

By continuing this line of argument, we can get $C_1, C_2, ...$ until we get to some C_k with $B_k = \{1\}$, for some $k \in \mathbb{N}$. Then

$$G \cong C_1 \times C_2 \times \ldots \times C_k$$

as required. □

Remark

We can verify that the decomposition of a finite abelian p-group into a direct product of cyclic groups is in fact unique up to their orders.[1]

[1] This is the bonus question on A4. It will be included once the assignment is over.

Combining the above remark, ☕ Theorem 52 and ☕ Theorem 56, we have the following theorem.

☕ Theorem 57 (Finite Abelian Group Structure)

If G is a finite abelian group, then

$$G \cong C_{p_1^{n_i}} \times \ldots \times C_{p_k^{n_k}}$$

where $C_{p_i^{n_i}}$ is a cyclic group of order $p_i^{n_i}$, where $1 \leq i \leq k$. The numbers $p_i^{n_i}$ are uniquely determined up to their order.[2]

[2] Note that the p_i's do not have to be unique.

Remark

Note that if p_1 and p_2 are distinct primes, then

$$C_{p_1^{n_1}} \times C_{p_2^{n_2}} \cong C_{p_1^{n_1} p_2^{n_2}},$$

the cyclic group of order $p_1^{n_1} p_2^{n_2}$. Thus, by combining suitable prime factors together, for a finite abelian group G, we can also write

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_r},$$

where $m_i \in \mathbb{N}$, $i \leq 1 \leq r$, $m_1 > 1$ and

$$m_1 \mid m_2 \mid \ldots \mid m_r$$

Example 20.1.1

Conder an abelian group G with order 48. Since $48 = 2^4 \cdot 3$, an abelian group of order 48 is isomorphic to $H \times \mathbb{Z}_3$, where H is an abelian group of order 2^4. The options for H are:

$$\mathbb{Z}_{2^4} \qquad \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}$$
$$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Therefore, we have the following possible decompositions of G:

$$G \cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48}$$
$$G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_{24}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$$

20.2 Rings

20.2.1 Rings

Definition 31 (Ring)

A set R is a ring if $\forall a, b, c \in R$,

1. $a + b \in R$
2. $a + b = b + a$
3. $a + (b + c) = (a + b) + c$
4. $\exists 0 \in R \;\; a + 0 = a = 0 + a$
5. $\exists (-a) \in R \;\; a + (-a) = 0 = (-a) + a$
6. $ab \in R$
7. $a(bc) = (ab)c$
8. $\exists 1 \in R \;\; 1 \cdot a = a = a \cdot 1$
9. $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$

We call 1 as the ***Unity*** *of R, 0 as the Zero of R, and $-a$ as the* ***negative*** *of a.*

The ring R is called a ***Commutative Ring*** *if it also satisfies the following:*

10. $ab = ba$.

As daunting as this definition seems, it is much easier to remember if we think of R being an **abelian group under addition**, **"almost" a group under multiplication**, save the fact that the **multiplicative inverse of an element does not necessarily exist**, and with the **distributive law**.

Example 20.2.1

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *and* $\mathbb{C}$ *are commutative rings with the zero being* 0*, and unity being* 1*.*

Example 20.2.2

For $n \in \mathbb{N}$*,* $n \geq 2$*,* $\mathbb{Z}_n$ *is a commutative ring with the zero being* $[0]$*, and unity being* $[1]$*.*

Example 20.2.3

The set $M_n(\mathbb{R})$ *is a ring using matrix addition and matrix multiplication, with zero being the zero matrix* 0*, and unity being the identity matrix* I*. We also know that* $M_n(\mathbb{R})$ *is not commutative.*

Warning

Note that since $(R, \cdot)$ *is not a group, we no longer have the liberty of using Proposition 6, i.e. we do not have left or right cancellation. For example, in* $\mathbb{Z}$*,* $0 \cdot x = 0 \cdot y \not\Longrightarrow x = y$*.*

21 Lecture 21 Jun 20th 2018

21.1 Rings (Continued)

21.1.1 Rings (Continued)

Note (Notation)

Given a ring R, to distinguish the difference between multiples in addition and in multiplication, for $n \in \mathbb{N} \wedge a \in R$, we write

$$na = \underbrace{a + a + \ldots + a}_{n \text{ times}}$$

and

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ times}}$$

respectively. Also, we will define

$$(-n)a = \underbrace{(-a) + (-a) + \ldots + (-a)}_{n \text{ times}}$$

and

$$a^{-n} = \left(a^{-1}\right)^n$$

if a^{-1} exists.

Note

Recall that for a group G and $g \in G$, we have $g^0 = 1$, $g^1 = g$, and $\left(g^{-1}\right)^{-1} = g$. Thus for addition, we have[1]

[1] Note that the first 0 is an integer while the second 0 is a zero in R.

$$0 \cdot a = 0 \qquad 1 \cdot a = a$$
$$-(-a) = a$$

Also, by 💧 *Proposition 5, if $n, m \in \mathbb{Z}$, we have*

$$m \cdot a + n \cdot a = (m + n) \cdot a$$
$$n(ma) = (nm)a$$
$$n(a + b) = na + nb$$

💧 Proposition 58 (More Properties of Rings)

Let R be a ring and $r, s \in \mathbb{R}$.

This is a problem in A4.

1. *If 0 is the zero of R, then $0 \cdot r = 0 = r \cdot 0$;* [2]
2. $-r(s) = -(rs) = r(-s)$;
3. $(-r)(-s) = rs$;
4. $\forall m, n \in \mathbb{Z}$, $(mr)(ns) = (mn)(rs)$.

[2] i.e. all the 0's are zeros of R.

Definition 32 (Trivial Ring)

*A **trivial ring** is a ring of only one element. In this case, we have $1 = 0$, i.e. the unity is the zero and vice versa.*

Remark

If R is a ring with $R \neq \{0\}$, since $r = r \cdot 1$ for all $r \in R$, we have $1 \neq 0$. Otherwise, if $1 = 0$, then $r = r \cdot 1 = r \cdot 0 = 0$, i.e. $R = \{0\}$.

Example 21.1.1

Let $R_1, R_2, ..., R_n$ be rings. We define component-wise operation on the product

$$R_1 \times R_2 \times \ldots \times R_n$$

as follows:

$$(r_1, r_2, ..., r_n) + (s_1, s_2, ..., s_n) = (r_1 + s_1, r_2 + s_2, ..., r_n + s_n)$$
$$(r_1, r_2, ..., r_n)(s_1, s_2, ..., s_n) = (r_1 s_1, r_2 s_2, ..., r_n s_n)$$

We can check that $R_1 \times R_2 \times \ldots \times R_n$ is a ring with the zro being $(0, 0, ..., 0)$ and the unity being $(1, 1, ..., 1)$. This set

$$R_1 \times R_2 \times \ldots \times R_n$$

is called the ***direct product*** *of $R_1, R_2, ..., R_n$.*

Definition 33 (Characteristic of a Ring)

If R is a ring, we define the ***characteristic*** *of R, denoted by $\mathrm{ch}(R)$, in terms of the order of 1_R in the additive group $(R, +)$, by*

$$\mathrm{ch}(R) = \begin{cases} n & \text{if } o(1_R) = n \in \mathbb{N} \text{ in } (R, +) \\ 0 & \text{if } o(1_R) = \infty \text{ in } (R, +) \end{cases}$$

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean that $\forall r \in R$, $kr = 0$.

By Proposition 58, we have

$$kr = k(1_R \cdot r) = (k1_R) \cdot r$$

and so $kR = 0$ if and only if $k1_R = 0$. Then, since $(R, +)$ is a group, by Proposition 13 and Proposition 14, it follows that:

Proposition 59 (Implications of the Characteristic)

Let R be a ring and $k \in \mathbb{Z}$.[3]

1. $\mathrm{ch}(R) = n \in \mathbb{N} \implies (kR = 0 \iff n \mid k)$
2. $\mathrm{ch}(R) = 0 \implies (kR = 0 \iff k = 0)$

[3] This is why we defined $\mathrm{ch}(R) = 0$ if $o(1_R) = \infty$

Example 21.1.2

Each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ has characteristic 0. For $n \in \mathbb{N}$ with $n \geq 2$, the ring $\mathbb{Z}_n$ has characteristic n.

21.1.2 Subring

Definition 34 (Subring)

A subset S of a ring R is a subring if S is a ring itself (under the same operations: addition and multiplication).

Unlike subgroups, since there is no proper suggestion of a symbolic representation, I shall use $S \leq_r R$ to denote that S is a subring of R, in comparison to $\leq$ for subgroups, which has no subscript. Note that this is purely for keeping my writing succinct, and so the subscript r is used simply to indicate that the $\leq$ symbol is for denoting a subring and should not be confused with other r's that may be used in a proof. This notation is also not used in class, and should be avoided during materials outside of this set of notes.

Note that properties (2), (3), (7) and (9) from Definition 31 are automatically satisfied. Thus, to show that S is a subring, it suffices to show the following:

Subring Test

1. $0, 1 \in S$ [4]
2. $s, t \in S \implies (s - t), st \in S$

[4] The $0 \in S$ is certainly not necessary to be shown, since from part (2) we would have $s \in S \implies 0 \in (s - s) \in S$.

Example 21.1.3

We have the following chain of commutative rings:

$$\mathbb{Z} \leq_r \mathbb{Q} \leq_r \mathbb{R} \leq_r \mathbb{C}$$

Example 21.1.4

If R is a ring, the center $Z(R)$ of R is defined as

$$Z(R) = \{z \in R : zr = rz, r \in R\}.$$

Note taht $0, 1 \in Z(R)$. Also, if $s, t \in Z(R)$, then $\forall r \in R$,

$$(s - t)r = sr - tr = rs - rt = r(s - t)$$

and so $(s - t) \in Z(R)$. Also,

$$(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$$

and so $st \in Z(R)$. By the Subring Test, $Z(R) \leq_r R$.

Example 21.1.5

Let

$$\mathbb{Z}[c] = \{a + bi : a, b \in \mathbb{Z},\ i^2 = -1\} \subseteq \mathbb{C}.$$

It can be shown that $\mathbb{Z}[i] \leq_r \mathbb{C}$, and is called the ring of ***Gaussian integers***.[5]

[5] Proof that the Gaussian integers is a subring is in A4, which shall be included after the assignment is over.

22 Lecture 22 Jun 22nd 2018

22.1 Ring (Continued 2)

22.1.1 Ideals

Let R be a ring and A an additive subgroup of R. Since $(R, +)$ is abelian, we have that $A \triangleleft R$. Thus, we can talk about the additive quotient group

$$\begin{gathered} R/A = \{r + a : r \in \mathbb{R}\} \text{ with} \\ r + A = \{r + a : a \in A\} \end{gathered}$$

Using the properties that we know about cosets and quotient groups, we have the following proposition.

Proposition 60 (Properties of the Additive Quotient Group)

Let R be a ring and A an additive subgroup of R. For $r, s \in R$, we have

1. $r + A = s + A \iff (r - s) \in A$
2. $(r + A) + (s + A) = (r + s) + A$
3. $0 + A = A$ *is the additive identity of* R/A
4. $-(r + A) = (-r) + A$ *is the additive inverse of* $r + A$
5. $\forall k \in \mathbb{Z} \quad k(r + A) = kr + A$

This is just a translation of the properties of cosets and quotient groups, that we are familiar with, into the language of addition. You can (read: should) prove this as an exercise for yourself (read: myself).

Since R is a ring, it is natural to ask if we could make R/A into a ring[1]. A natural way to define "multiplication" in R/A is

[1] *Ideally* (see what I did there?), we would want R/A as a ring, just as we had R/A as a group.

$$(r+A)(s+A) = rs + A \quad \forall r, s \in \mathbb{R} \tag{$\dagger$}$$

Note, however, that we would have

$$r + A = r_1 + A \qquad s + A = s_1 + A$$

with $r \neq r_1$ and $s \neq s_1$. In order for Equation ($\dagger$) to make sense, it is necessary that

$$r + A = r_1 + A \wedge s + A = s_1 + A \implies rs + A = r_1 s_1 + A$$

so that this "multiplication" is **well-defined**.

Proposition 61

Let A be an additive subgroup of a ring R. Then $\forall a \in A$, define

$$Ra = \{ra : r \in R\} \quad aR = \{ar : r \in R\}.$$

The following are equivalent (TFAE):

1. *$Ra \subseteq A$ and $aR \subseteq A$, $\forall a \in A$;*
2. *$\forall r, s \in R$, $(r+A)(s+A) = rs + A$ is well-defined in R/A.*

Proof

$(1) \implies (2)$: *If $r + A = r_1 + A$ and $s + A = s_1 + A$, for $r, r_1, s, s_1 \in R$, we need to show that*

$$rs + A = r_1 s_1 + A.$$

By Proposition 60, we have that $(r - r_1), (s - s_1) \in A$, and so by (1), we have

$$\begin{aligned} rs - r_1 s_1 &= rs - r_1 s + r_1 s - r_1 s_1 \\ &= (r - r_1)s + r_1(s - s_1) \\ &\in (r - r_1)R + R(s - s_1) \subseteq A \end{aligned}$$

Therefore, by Proposition 60 again, we have $rs + A = r_1 s_1 + A$.

$(2) \implies (1)$: *Let $r \in R$ and $a \in A$. We have that*

$$\begin{aligned} ra + A &= (r+A)(a+A) \quad \because (2) \\ &= (r+A)(0+A) \quad \because a, 0 \in A \\ &= (r \cdot 0) + A \quad \because (2) \\ &= 0 + A \quad \because 0 \;\; Proposition\ 58 \\ &= A \quad \because 0 \;\; Proposition\ 60 \end{aligned}$$

Thus $ra \in A$ and so $Ra \subseteq A$. Similarly, we can show that $aR \subseteq A$. $\square$

Definition 35 (Ideal)

*An additive subgroup A of a ring R is called an **ideal** of R if $Ra, aR \subseteq A$, $\forall a \in A$.*

Example 22.1.1

If R is a ring, $\{0\}$ and R are both ideals of R.

Proposition 62 (The Only Ideal with the Multiplicative Identity is the Ring Itself)

Let A be an ideal of a ring R. If $1 \in A$, then $A = R$.

This also shows that if we want a non-trivial ideal, then the ideal should not have 1.

Proof

$\forall r \in R$, $\because A$ is an ideal and $1 \in A$, we have $r = r \cdot 1 \in A$. It follows that $R \subseteq A \subseteq R$ and so $R = A$. $\square$

Proposition 63 (Construction of the Quotient Ring)

Let A be an ideal of a ring R. Then the additive quotient group R/A is a ring with the multiplication $(r+A)(s+A) = rs + A$, $\forall r, s \in R$. The unity of R/A is $1 + A$.

Proof

$\because$ A is an additive subgroup of a ring R, R/A is an additive abelian group. By Proposition 61, the multiplication on R/A is well-defined. The multiplication is associative, since $\forall r, s, q \in R$,

$$\begin{aligned}(r+A)\big((s+A)(q+A)\big) &= (r+A)(sq+A) = (rsq+A) \\ &= (rs+A)(q+A) \\ &= \big((r+A)(s+A)\big)(q+A).\end{aligned}$$

We also have

$$(r+A)(1+A) = r+A = (1+A)(r+A)$$

and so the unity of R/A is $1+A$. The distributive property is inherited from R. $\square$

Definition 36 (Quotient Ring)

Let A be an ideal of a ring R. Then the ring R/A is called the *quotient ring* of R by A.

Definition 37 (Principal Ideal)

Let R be a commutative ring and A an ideal of R. If $A = aR = \{ar : r \in R\} = Ra$ for some $a \in A$, we say that A is a *principal ideal* generated by a, and denote $A = \langle a \rangle$.

Example 22.1.2

If $n \in \mathbb{Z}$, then $\langle n \rangle = n\mathbb{Z}$ is a(n) (principal) ideal of $\mathbb{Z}$, since $\mathbb{Z}$ is commutative.

Proposition (Ideals of $\mathbb{Z}$ are Principal Ideals)

All ideals of $\mathbb{Z}$ are of the form $\langle a \rangle$ for some $n \in \mathbb{Z}$.

We shall prove this in the next lecture.

23 Lecture 23 Jun 25th 2018

23.1 Ring (Continued 3)

23.1.1 Ideals (Continued)

Proposition 64 (Ideals of $\mathbb{Z}$ are Principal Ideals)

All ideals of $\mathbb{Z}$ are of the form $\langle\, n \,\rangle$ for some $n \in \mathbb{Z}$.

Proof

Let A be an ideal of $\mathbb{Z}$. If $A = \{0\}$, then $A = \langle\, 0 \,\rangle$. Otherwise, let $a \in A$ with $a \neq 0$, and $|a|$ be the minimum. Clearly, $\langle\, a \,\rangle = a\mathbb{Z} \subseteq A$. To prove the other inclusion, let $b \in A$. By the **Division Algorithm**, *$\exists q, t \in \mathbb{Z}$ with $0 \leq r < |a|$ such that $b = qa + r$. Because A is an ideal, we have $r = b - qa \in A$. Since $|r| < |a|$ which is the minimal case, it must be that $r = 0$. Therefore $b = qa \in \langle\, a \,\rangle$ and so $A \subseteq \langle\, a \,\rangle$.* $\square$

23.1.2 Isomorphism Theorems for Rings

Definition 38 (Ring Homomorphism)

Let R and S be rings. A mapping

$$\Theta : R \to S$$

is a ring **homomorphism** *if $\forall a, b \in R$, we have*

1. $\Theta(a+b) = \Theta(a) + \Theta(b)$
2. $\Theta(ab) = \Theta(a)\Theta(b)$
3. $\Theta(1_R) = 1_S$

Note (Remark)

$(2) \not\Longrightarrow (3)$ *because* $\Theta(1_R) \in S$ *does not necessarily have a multiplicative inverse, since* S *is a ring.*

Example 23.1.1

The mapping $k \mapsto [k]$ *from* $\mathbb{Z} \to \mathbb{Z}_n$ *is a surjective ring homomorphism.*

Example 23.1.2 (Direct Product of Rings)

If R_1, R_2 *are rings, the projection*

$$\pi_1 : R_1 \times R_2 \to R_1 \text{ defined by } \pi_1(r_1, r_2) = r_1$$

is a surjective ring homomorphism, since

1. $\pi_1(r_1 + r_2, q_1 + q_2) = r_1 + r_2 = \pi_1(r_1, q_1) + \pi_1(r_2, q_2)$;
2. $\pi_1(r_1 r_2, q_1 q_2) = r_1 r_2 = \pi_1(r_1, q_1)\pi_1(r_2, q_2)$; *and*
3. $\pi(1, 1) = 1$.

We can a similar $\pi_2 : R_1 \times R_2 \to R_2$ *such that* $(r_1, r_2) \mapsto r_2$*, and we will get that* π_2 *is also a surjective ring homomorphism.*

Proposition 65 (Properties of Ring Homomorphisms)

Let $\Theta : R \to S$ *be a ring homomorphism and let* $r \in R$*. Then*

1. $\Theta(0_R) = 0_S$
2. $\Theta(-r) = -\Theta(r)$
3. $\Theta(kr) = k\Theta(r)$
4. $\forall n \in \mathbb{N} \cup \{0\} \quad \Theta(r^n) = \Theta(r)^n$
5. $u \in R^* \implies \forall k \in \mathbb{Z} \quad \Theta(u^k) = \Theta(u)^k$

Proof

1. *Note that*
$$\Theta(r) = \Theta(0_R + r) = \Theta(0_R) + \Theta(r).$$
Therefore,
$$\Theta(0_R) = 0_S$$
as required.

2. *Note that*
$$0_S = \Theta(0_R) = \Theta(r - r) = \Theta(r) + \Theta(-r),$$
so
$$\Theta(-r) = -\Theta(r).$$

3. *Observe that*
$$\Theta(kr) = \Theta(\underbrace{r + r + \ldots + r}_{k \text{ times}}) = \underbrace{\Theta(r) + \Theta(r) + \ldots + \Theta(r)}_{k \text{ times}} = k\Theta(r)$$

Item 4 follows by induction on the definition of a ring homomorphism, and Item 5 follows as a result from Item 4 because if $u \in R^*$, then $u^{-1} \in R^*$ such that $uu^{-1} = 1_R$. □

Definition 39 (Ring Isomorphism)

A mapping of rings $\Theta : R \to S$ is a ring **isomorphism** *if Θ is a bijective ring homomorphism. In this case, we say that R and S are* **isomorphic** *and denote that by $R \cong S$.*

Definition 40 (Kernel and Image)

Let $\Theta : R \to S$ be a ring homomorphism. The **kernel** *of Θ is defined by*
$$\ker\Theta = \{r \in R : \Theta(r) = 0_S\}$$

and the image of Θ is defined by

$$\operatorname{im}\Theta := \Theta(R) = \{\Theta(r) : r \in R\}.$$

Proposition 66

Let $\Theta : R \to S$ be a ring homomorphism. Then

1. $\operatorname{im}\Theta \leq_r S$
2. $\ker\Theta$ *is an ideal of* R

Proof

1. $\Theta(1_R) = 1_S$ *by definition of a homomorphism so* $\Theta(1_R) \in \operatorname{im}\Theta$. *Suppose* $s_1 = \Theta(r_1)$ *and* $s_2 = \Theta(r_2)$, *then*

$$\begin{aligned} s_1 - s_2 &= \Theta(r_1) - \Theta(r_2) = \Theta(r_1 - r_2) \\ s_1 s_2 &= \Theta(r_1)\Theta(r_2) = \Theta(r_1 r_2) \end{aligned}$$

   are both in $\operatorname{im}\Theta$. *By the Subring Test,* $\operatorname{im}\Theta \leq_r S$.

2. *Since* $\ker\Theta$ *is an additive subgroup of* R, *it suffices to show that* $ra, ar \in \ker\Theta$ *for all* $r \in R$ *and* $a \in \ker\Theta$. *Let* $r \in R$ *and* $a \in \ker\Theta$. *Then*

$$\Theta(ra) = \Theta(r)\Theta(a) = \Theta(r) \cdot 0 = 0$$

   So $ra \in \ker\Theta$. *Similarly so,*

$$\Theta(ar) = \Theta(a)\Theta(r) = 0 \cdot \Theta(r) = 0$$

   and so $ar \in \ker\Theta$. *Therefore,* $\ker\Theta$ *is an ideal of* R.

$\square$

Theorem 67 (First Isomorphism Theorem for Rings)

Let $\Theta : R \to S$ be a ring homomorphism. Then

$$R/\ker\Theta \cong \operatorname{im}\Theta.$$

Proof

Let $A = \ker \Theta$. *Since* A *is an ideal of* R, *we have that* R/A *is a ring. Define*

$$\overline{\Theta} : R/A \to \operatorname{im}\Theta \text{ by } (r+A) \mapsto \theta(a).$$

Note that

$$r + A = s + A \iff (r-s) \in A \iff \Theta(r-s) = 0 \iff \Theta(r) = \Theta(s).$$

Therefore $\overline{\Theta}$ *is well-defined and injective. Also, it is clear that* $\overline{\Theta}$ *is surjective. To show that* $\overline{\Theta}$ *is a homomorphism, note that* $\forall r, s \in R$, *we have*

$$\begin{aligned}\overline{\Theta}(r+A+s+A) &= \overline{\Theta}(r+s+A) = \Theta(r+s) \\ &= \Theta(r) + \Theta(s) = \overline{\Theta}(r+A) + \overline{\Theta}(s+A).\end{aligned}$$

It follows that $\overline{\Theta}$ *is a ring isomorphism and so*

$$R/\ker\Theta \cong \operatorname{im}\Theta$$

as required. $\square$

Exercise 23.1.1

Let $A, B \leq_r R$, *where* R *is a ring. Prove that*

1. $A \cap B$ *is the largest subring of* R *contained in both* A *and* B.
2. *If either* A *or* B *is an ideal of* R, *the sum*

$$A + B = \{a + b : a \in A,\, b \in B\}$$

is a subring of R, *and is the smallest subring of* R *that contains both* A *and* B.

Theorem 68 (Second Isomorphism Theorem for Rings)

Let A *be a subring and* B *an ideal of a ring* R. *Then*

1. $A + B \leq_r R$;
2. B *is an ideal of* $A + B$;

3. *$A \cap B$ is an ideal of A; and*

4. $$ {}^{(A+B)}\!\big/_{B} \cong {}^{A}\!\big/_{(A \cap B)} $$

Theorem 69 (Third Isomorphism Theorem for Rings)

Let A and B be ideals of R with $A \subseteq B$, then ${}^{B}\!/_{A}$ is an ideal of ${}^{R}\!/_{A}$ and

$$ \left({}^{R}\!/_{A} \right) \Big/ \left({}^{B}\!/_{A} \right) \cong {}^{R}\!/_{B}. $$

24 Lecture 24 Jun 27th 2018

24.1 Rings (Continued 4)

24.1.1 Isomorphism Theorems for Rings (Continued)

Theorem 70 (Chinese Remainder Theorem)

Let A and B be ideals of R.

1. $A + B = R \implies R/(A \cap B) \cong R/A \times R/B$
2. $A + B = R \land A \cap B = \{0\} \implies R \cong R/A \times R/B$

Proof

It suffices to prove (1) *since if* (1) *is true and* $A \cap B = \{0\}$*, then* (2) *immediately follows.*

Define

$$\Theta : R \to R/A \times R/B \qquad r \mapsto (r + A, r + B)$$

Then Θ is a ring homomorphism [1].

[1]

Exercise 24.1.1
Prove that Θ is a ring homomorphism.

Proof (Θ is a ring homomorphism)

$\forall r, s \in R$, *we have*

$$\begin{aligned} \Theta(rs) &= (rs + A, rs + B) \\ &\overset{(*)}{=} (r + A, r + B)(s + A, s + B) \\ &= \Theta(r)\Theta(s) \end{aligned}$$

where $(*)$ *is by Proposition 63. Also by the same proposition, we have*

$$\Theta(1) = (1 + A, 1 + B).$$

Then,

$$\begin{aligned}\Theta(r+s) &= (r+s+A, r+s+B) \\ &\overset{(\dagger)}{=} (r+A, r+B) + (s+A, s+B) \\ &= \Theta(r) + \Theta(s)\end{aligned}$$

where $(\dagger)$ *is by Proposition 60.*

Note that $\ker\Theta = A \cap B$*, since*

$$\ker\Theta = \{r \in R : \Theta(r) = (A, B)\} = \{r \in A \wedge r \in B\} = A \cap B.$$

To show that Θ *is surjective, let* $(s + A, t + B) \in R/A \times R/B$ *with* $s, t \in R$*. Since* $A + B = R$*,* $\exists a \in A$*,* $\exists b \in B$ *such that* $a + b = 1$*. Let* $r = sb + ta$*. Then*

$$\begin{aligned}s - r &= s - sb - ta = s(1-b) - ta = sa - ta = (s-t)a \in A \\ t - r &= t - sb - ta = t(1-a) - sb = tb - sb = (t-s)b \in B\end{aligned}$$

and so by Proposition 60,

$$s + A = r + A \text{ and } t + B = r + B.$$

Therefore

$$\Theta(r) = (r + A, r + B) = (s + A, t + B),$$

and so Θ *is surjecive. Then by the Theorem 67,*

$$R/(A \cap B) \cong R/A \times R/B.$$

□

Why is Theorem 70 called the Chinese Remainder Theorem?

Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Then we know that

$$m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}.$$

Also, $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ since $1 = ma + nb$ for some $a, b \in \mathbb{Z}$ by **Bezout's Lemma**. And so:

Corollary 71

1. *If $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, then*

$$\mathbb{Z}/_{mn\mathbb{Z}} \cong \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$

i.e.

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

2. *If $m, n \in \mathbb{N}$ with $m, n \geq 2$ and $\gcd(m, n) = 1$, then*

$$\phi(mn) = \phi(m)\phi(n)$$

*where $\phi(m) = |\mathbb{Z}_m^*|$ is **Euler's ϕ-function**.*

Let p be a prime. Recall that one consequence of Lagrange's Theorem is that every group G of order p is cyclic, i.e. $G \cong C_p$.

An analogous notion in rings is the following:

Proposition 72 (Ring With Prime Order Is Isomorphic to Integer Modulo Prime)

If R is a non-trivial ring with $|R| = p$ where p is prime, then $R \cong \mathbb{Z}_p$.

Proof

Define

$$\Theta : \mathbb{Z}_p \to R \qquad [k] \mapsto k \cdot 1_R.$$

Note that since R is an additive group with $|R| = p$, by Lagrange's Theorem, $o(1_R) = 1$ or p. Since R is non-trivial, we have that $1_R \neq 0$ by the remark on the definition of a trivial ring, and so $o(1_R) \neq 1$. Thus $o(1_R) = p$. Then, by Proposition 59, we have

$$[k] = [m] \iff p \mid (k - m) \iff (k - m)1_R = 0 \iff k \cdot 1_R = m \cdot 1_R$$

in R. Thus, Θ is well-defined and injective. Θ is also a ring homomorphism [2].

[2]

Exercise 24.1.2
Prove that Θ is a ring homomorphism.

Proof (Θ is a ring homomorphism)
$\forall [a], [b] \in \mathbb{Z}$, *we have*

$$\begin{aligned} \Theta([a][b]) &= \Theta([ab]) = ab \cdot 1_R \\ &= (a \cdot 1_R)(b \cdot 1_R) = \Theta([a])\Theta([b]). \end{aligned}$$

$$\Theta([1]) = 1 \cdot 1_R = 1_R$$

and

$$\begin{aligned} \Theta([a] + [b]) &= \Theta([a + b]) = (a + b) \cdot 1_R \\ &= a \cdot 1_R + b \cdot 1_R = \Theta([a]) + \Theta([b]). \end{aligned}$$

So Θ is a ring homomorphism.

Now because $|\mathbb{Z}_p| = p = |R|$ and Θ is injective, Θ must be surjective. Therefore Θ is a ring isomorphism and hence $R \cong \mathbb{Z}_p$ as required. $\square$

24.2 Commutative Rings

24.2.1 Integral Domain and Fields

Definition 41 (Units)

*Let R be a ring. We say that $u \in R$ is a **unit** if u has a multiplicative inverse in R, and denote it by u^{-1}. We have*

$$uu^{-1} = 1 = u^{-1}u$$

Note

If u is a unit in R, and $r, s \in R$, we have

$$\begin{aligned} ur = us &\implies r = s \quad (\text{ Right Cancellation }) \\ ru = su &\implies r = s \quad (\text{ Left Cancellation }) \end{aligned}$$

Let R^* denote the set of all units in R. We know that the definition of a ring is that R is "almost" a group under multiplication except that its elements do not necessarily have multiplicative inverses. Since $R^* \subseteq R$ is the set that contains all units, i.e. all elements with multiplicative inverses in R, we have that $(R^*, \cdot)$ is a group. This is called the ***Group of Units*** *of R.*

Example 24.2.1

Note that 2 is a unit in $\mathbb{Q}$, but it is not a unit in $\mathbb{Z}$. We have that

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \text{ and } \mathbb{Z}^* = \{\pm 1\}$$

Example 24.2.2

Consider the ring of ***Gaussian Integers****,*

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z},\ i^2 = -1\} \subseteq \mathbb{C}.$$

Then[3]

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}.$$

[3] **Proof to be added once A4 is over.**

Definition 42 (Division Ring and Field)

A non-trivial ring R is a ***division ring*** *if*

$$R^* = R \setminus \{0\}.$$

A commutative division ring is a ***field****.*

Example 24.2.3

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields but $\mathbb{Z}$ is not.

Example 24.2.4

$\mathbb{Z}_n$ is a field $\iff$ n is prime.

This remark is not as useful or spectacular within this course, but it will be once we go into PMATH348 contents.

Remark

If R is a division ring or a field, then its only ideals are $\{0\}$ or R, since if $A \neq \{0\}$ is an ideal of R, then $\exists a \in A$, $a \neq 0$, such that $1 = aa^{-1} \in A$, which implies that $A = R$ by Proposition 62.

Remark

It can be shown that every finite division ring is a field, and this is known as Wedderburn's Theorem.

Note that if $n = ab$ for some integer n with $0 < a, b < n$, then in $\mathbb{Z}$ we have

$$[a][b] = [n] = [0]$$

but $[a] \neq [0] \neq [b]$ by our definition of a, b.

Definition 43 (Zero Divisor)

Let R be a non-trivial ring. If $0 \neq a \in R$, then a is called a ***zero divisor*** *if $\exists 0 \neq b \in R$ such that $ab = 0$.*

25 Lecture 25 Jun 29th 2018

25.1 Commutative Rings (Continued)

25.1.1 Integral Domain and Fields (Continued)

Recall the definition of a **zero divisor**.

Definition (Zero Divisor)

Let R be a non-trivial ring. If $0 \neq a \in R$, then a is called a ***zero divisor*** *if $\exists 0 \neq b \in R$ such that $ab = 0$.*

Example 25.1.1

$[2], [3], [6]$ in $\mathbb{Z}_6$ are all zero divisors since

$$[0] = [2][3] = [4][3] = [6][2].$$

Example 25.1.2

The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor in $M_n(\mathbb{R})$ since

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Proposition 73 (Ring Cancellations and Zeros)

Let R be a ring. TFAE:

1. $\forall ab = 0 \in R \quad a = 0 \vee b = 0$;

2. $\forall ab = ac \in R \wedge a \neq 0 \implies b = c$;
3. $\forall ba = ca \in R \wedge a \neq 0 \implies b = c$.

Proof

It suffices to prove $(1) \iff (2)$, *since* $(1) \iff (3)$ *would have a similar argument.*

$(1) \implies (2)$: *Let* $ab = ac$ *with* $a \neq 0$. *Then* $a(b-c) = 0$. *Then by* (1), *since* $a \neq 0$, $(b-c) = 0 \iff b = c$.

$(2) \implies (1)$: *Let* $ab = 0 \in R$. *We now have 2 cases:*

Case 1 *If* $a = 0$, *we are done.*

Case 2 *If* $a \neq 0$, *then* $ab = 0 = a \cdot 0$, *and so by* (2), $b = 0$.

$\square$

With that, we can make the following definition.

Definition 44 (Integral Domain)

A commutative ring $R \neq \{0\}$ *(i.e. non-trivial ring) is called an* ***integral domain*** *if it has* ***no zero divisor****, i.e. if* $ab = 0 \in R$ *then* $a = 0$ *or* $b = 0$.

Example 25.1.3

$\mathbb{Z}$ *is an integral domain since* $ab = 0 \implies a = 0$ *or* $b = 0$.

Example 25.1.4

Note that if p *is prime, then* $p \mid ab \implies p \mid a \vee p \mid b$, *i.e.* $[a][b] = [0]$ *in* $\mathbb{Z}_p \implies [a] = 0$ *or* $[b] = 0$. *So* $\mathbb{Z}_p$ *is an integral domain.*

However, for n *not prime, with* $n = ab$, *if we have* $n = ab$ *such that* $1 < a, b < n$, *then*

$$[a][b] = [0] \text{ in } \mathbb{Z}_n$$

but neither $[a]$ *nor* $[b]$ *is* $[0]$.

With that, we have that $\mathbb{Z}_n$ *is an integral domain if and onoly if* n *is prime.*

Proposition 74 (Fields are Integral Domains)

Every field is an integral domain.

Proof

$\forall a, b \in R$, where R is a field, such that $ab = 0$, we want to show that $a = 0$ or $b = 0$. We have 2 cases:

Case 1: $a = 0$. There is nothing to do since the proof is complete.

Case 2: $a \neq 0$. Since $a \neq 0 \in R$, we know that $\exists a^{-1} \in R$ since R is a field. And so

$$b = a^{-1}ab = a^{-1} \cdot 1 = 0$$

Therefore, by definition, the field R is an integral domain. □

Note

Using the proof from above, we can show that every subring of a field is an integral domain[1].

[1] This will become useful in PMATH348

Note

The converse of Proposition 74 is not true. As shown in Example 25.1.3, $\mathbb{Z}$ is an integral domain but not a field.

However, we have the following partial converse:

Proposition 75 (Finite Integral Domains are Fields)

*Every **finite** integral domain is a field.*

Proof
Let R be a finite integral domain, say $|R| = n \in \mathbb{N}$. Let

$$R = \{r_1, r_2, ..., r_n\}.$$

Then for some $a \in R$ such that $a \neq 0$, by Proposition 73, the set

$$\{ar_1, ar_2, ..., ar_n\}$$

have distinct elements. Since R is finite and so $|aR| = n$, and $aR \subseteq R$, we have that $aR = R$. In particular, $\exists 1 \in aR$ such that $1 = ab$ for some $b \in R$ [2]. It follows that $ab = 1 = ba$ since R is commutative, which then implies that a is a unit. Therefore, R is a field. □

[2] We can prove for a more general case by not assuming that R is a commutative ring: We can find $c \in R$ such that $1 = ca$. Then

$$b = (ca)b = c(ab) = c.$$

Recall that the characteristic of a ring R, denoted by $\mathrm{ch}(R)$, is the order of the unity, 1_R, in $(R, +)$, and write

$$\mathrm{ch}(R) = \begin{cases} 0 & o(1_R) = \infty \\ n & o(1_R) = n \in \mathbb{N} \end{cases}$$

Proposition 76 (Integral Domains have Zero or Prime Characteristics)

The characteristic of any integral domain is 0 or a prime p.

Proof
Let R be an integral domain. We have 2 cases:

Case 1: $\mathrm{ch}(R) = 0$. *Our job is done.*

Case 2: $\mathrm{ch}(R) = n \in \mathbb{N}$. *Suppose $n \neq p$ a prime, and say $n = ab$ for some $a, b \in R$ such that $1 < a, b < n$. If 1 is the unity of R, then by Proposition 58, we have*

$$ab = (a \cdot 1)(b \cdot 1) = (ab)(1) = n(1) = 0.$$

Since R is an integral domain, we have that either

$$a \cdot 1 = 0 \text{ or } b \cdot 1 = 0.$$

This contradicts that fact that n is the characteristic. Therefore, n must be prime. $\square$

Note

Let R be an integral domain with $\mathrm{ch}(R) = p$ a prime. For $a, b \in R$, by the ***Binomial Theorem****, we have*

$$(a+b)^p = \sum_{i=1}^{p} \binom{p}{i} a^{p-i} b^i.$$

Since p is prime, we have $p \mid \binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$ for $1 \leq i \leq p-1$. Therefore, since $\mathrm{ch}(R) = p$, we have that

$$(a+b)^p = a^p + b^p$$

This is known as the Freshman's Dream.

26 Lecture 26 Jul 04th 2018

26.1 Commutative Rings (Continued 2)

26.1.1 Prime Ideals and Maximal Ideals

Definition 45 (Prime Ideals)

Let R be a commutative ring. An ideal $P \neq R$ is a prime ideal of R if $r, s \in R$ satisfy: $rs \in R \implies r \in P$ or $s \in P$.

Example 26.1.1

For $n \in \mathbb{N} \setminus \{1\}$, $n\mathbb{Z} = \langle\, n \,\rangle$ is a prime ideal if and only if n is prime.

Proposition 77 (Ideal is Prime $\iff$ Quotient of Ring by Ideal is an Integral Domain)

If R is a commutative ring, then an ideal $P \neq R$ of R is a prime ideal if and only if R/P is an integral domain.

Proof

Since R is commutative, so is R/P. Since $P \neq R$, we know that $1 \notin P$ [1], *i.e. $0 + P = P \neq 1 + P$, and so R/P is a non-trivial ring.*

[1] See Proposition 62.

To prove ($\implies$), let $(r+P)(s+P) = 0 + P = P$. Since P is an ideal[2], *we have that $rs + P = P$ and so $rs \in P$. WLOG, since P is a prime ideal, if $r \in P$, then $r + P = P$. And so R/P is an integral domain.*

[2] See Proposition 61.

To prove ($\impliedby$), let $rs \in P$. Then since P is an ideal,

$$(r+P)(s+P) = rs + P = P.$$

Since R/P is an integral domain, either

$$r + P = P \text{ or } s + P = P$$

so $r \in P$ or $s \in P$, which implies that P is a prime ideal. $\square$

Definition 46 (Maximal Ideals)

Let R be a (commutative) ring. An ideal $M \neq R$ or R is a maximal ideal if $\forall A$ that is an ideal of R, we have that

$$M \subseteq A \subseteq R \implies A = M \text{ or } A + R.$$

Proposition 78 (Ideal is Maximal $\iff$ Quotient of Ring by Ideal is a Field)

If R is a commutative ring, then an ideal $M \neq R$ is a maximal ideal if and only if R/M is a field.

Proof

Similar to the proof of Proposition 77, R/M is a nontrivial commutative ring. Let $r \in R$.

($\implies$) Suppose M is a maximal ideal. Since R/M is non-trivial, let $r + M \neq 0 + M \in R/M$. Let $\langle r \rangle = rR$ Note that $r \notin M$ and $r \in \langle r \rangle + M$. Thus, $M \subsetneq \langle r \rangle + M$. Since M is maximal and M is a proper subset of $\langle r \rangle + M$, we have that $\langle r \rangle + M = R$. In particular, we have $1 \in \langle r \rangle + M$ and so $\exists s \in R$ and $m \in M$ such that $1 = rs + m$. Thus

$$1 + M = rs + M = (r+M)(s+M).$$

Therefore $s + M$ is the multiplicative inverse of $r + M$, and so R/M is a field.

($\impliedby$) Since R/M is a non-trivial field, we know $0 + M \neq 1 + M$.

Therefore $M \neq R$. Suppose A is an ideal such that $M \subsetneq A \subseteq R$. Choose $r \in A \setminus M$. Since $r \notin M$ and so $r + M \neq 0 + M$ and R/M is a field, we have that $\exists s + M \in R/M$ such that $(r + M)(s + M) = 1 + M$. Since M is an ideal, we have

$$rs + M = 1 + M \implies \exists m \in M \quad 1 = rs + m.$$

Since $r, m \in A$ and A is an ideal, we have that $1 \in A$ and so $A = R$, implying that M is maximal. $\square$

Combining Proposition 74, Proposition 77, and Proposition 78, we get the following corollary.

Corollary 79 (Maximal Ideals of a Commutative Rings are Prime)

Every maximal ideal of a commutative ring is a prime ideal.

Note

The converse of Corollary 79 is not true.

Example 26.1.2

In $\mathbb{Z}$, $\{0\}$ is a prime ideal, but is clearly not maximal.

26.1.2 Fields of Fractions

Recall that every subring of a field is an integral domain. The converse is actually true[3], i.e. every integral domain R is isomorphic to a subring of a field F.

[3] This is in comparison with Proposition 74.

Let R be an integral domain and $D = R \setminus \{0\}$. Consider

$$X = R \times D = \{(r, s) : r \in R, s \in D\}$$

We say that

$$(r, s) \equiv (r_1, s_1) \in X \iff rs_1 = r_1 s \tag{26.1}$$

Example 26.1.3

Show that Equation (26.1) *is an equivalence relation.*

1. $(r, s) \equiv (r, s)$
2. $(r, s) \equiv (r_1, s_1) \iff (r_1, s_1) \equiv (r, s)$
3. $(r, s) \equiv (r_1, s_1) \land (r_1, s_1) \equiv (r_2, s_2) \implies (r, s) = (r_2, s_2)$

Note that using the above idea, we can construct the smallest field that contains $\mathbb{Z}$, and that field is $\mathbb{Q}$. Motivated by this idea, we make the following definition.

Definition 47 (Fraction)

*Let R be an integral domain, $D = R \setminus \{0\}$, and $X = R \times D$. The **fraction**, $\frac{r}{s}$ to be the equivalent class $[(r, s)]$ of the pair $(r, s) \in X$.*

Let F denote the set of all these fractions, i.e.

$$F = \{[(r, s)] : r \in R, s \in D\} = \{\frac{r}{s} : r \in R, s \in R \setminus \{0\}\}.$$

The addition and multiplication of F are defined by

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + sr_1}{ss_1}$$
$$\frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

where we note that $ss_1 \neq 0$ since $s, s_1 \in R \setminus \{0\}$ and R is an integral domain.

It can be shown that F is a field[4]. Also, we have $R \cong R' = \frac{r}{1} : r \in R\} \subseteq F$.

[4] Prove this as an easy exercise to ease yourself with the concept.

Exercise 26.1.1
Prove that F is a field.

Theorem 80 (Field of Fractions)

*Let R be an integral domain. Then there is a field F containing fractions $\frac{r}{s}$ with $r, s \in R$ and $s \neq 0$. By identifying that $r = \frac{r}{1}$, for any $r \in R$, we have that R is a subring of F. The field F is called the **field of fractions** of R.*

Note

We can generalize $D = R \setminus \{0\}$ to any subset $D \subseteq R$ satisfying

1. $1 \in D$
2. $0 \notin D$
3. $a, b \in D \implies ab \in D$

27 Lecture 27 Jul 06th 2018

27.1 Polynomial Ring

27.1.1 Polynomials

Definition 48 (Polynomials)

Let R be a ring and x a variable. Let

$$R[x] = \left\{ f(x) = \sum_{i=0}^{m} a_i x^i : m \in \mathbb{N} \cup \{0\},\, a_i \in R, 0 \leq i \leq m \right\}.$$

Each element in $R[x]$ is called a ***polynomial*** *in x over R. If $a_m \neq 0$, we say that $f(x)$ has* ***degree*** *m, denoted by $\deg f = m$, and we say that a_m is the* ***leading coefficient*** *of $f(x)$.*

If $\deg f = 0$, then $f(x) = a_0 \in R$. In this case, we call $f(x)$ a ***constant polynomial****. Note if*

$$f(x) = 0 \iff a_0 = a_1 = ... = a_m = 0,$$

we define $\deg 0 = -\infty$, and $f(x)$ is called a ***zero polynomial****.*

For

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m$$
$$g(x) = b_0 + b_1 x + \ldots + b_n x^n$$

in $R[x]$. If $m \leq n$, we can define $a_i = 0$ for $m + 1 \leq i \leq n$. Then the addition and multiplication on $R[x]$ can be defined as

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n \\ f(x)g(x) &= (a_0 + a_1 x + \ldots + a_m x^m)(b_0 + b_1 x + \ldots + b_n x^n) \\ &= a_0 b_0 + (a_1 b_0 + a_1 b_0)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \ldots \\ &\quad + (a_m b_m)x^{m+n} \\ &= c_0 + c_1 x + \ldots + c_{m+n} x^{m+n} \end{aligned}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_{i-1} b_1 + a_i b_0$.

Proposition 81 (Ring is a Subring of Its Polynomial Ring)

Let R be a ring and x a variable.

1. *$R[x]$ is a ring*
2. *R is a subring of $R[x]$*
3. *If $Z = Z(R)$ denote the center of R, then the center of $R[x]$ is $Z[x]$. In particular, x is in the center of $R[x]$.*

Proof

1. ***Checking all 9 properties**: Let*

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_m x^m \\ g(x) &= b_0 + b_1 x + \ldots + b_n x^n \\ h(x) &= d_0 + d_1 x + \ldots + d_k x^k \end{aligned}$$

be in $R[x]$.

- *(**Closed under addition and multiplication**) Suppose, WLOG, that $m \leq n$. Let $a_i = 0$ for $m + 1 \leq i \leq n$. Then*

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n$$

and we observe that $a_i + b_i \in R$ for $0 \leq i \leq n$ since R is a ring. And so $f(x) + g(x) \in R[x]$. Also, we have

$$f(x)g(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_{i-1} b_1 + a_i b_0 \in R$ for $1 \leq i \leq$

$m+n$. And so $f(x)g(x) \in R[x]$.

- ***(Commutativity of Addition)*** *Suppose, WLOG, that $m \leq n$. Let $a_i = 0$ for $m+1 \leq i \leq n$. Then*

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n \\ &= (b_0 + a_0) + (b_1 + a_1)x + \ldots + (b_n + a_n)x^n \\ &= g(x) + f(x) \end{aligned}$$

- ***(Zero and Unity)*** *It is clear that the zero and unity of R are the zero and unity of $R[x]$ respectively, since only*

$$f(x) + 0 = f(x) = 0 + f(x)$$

and

$$1f(x) = f(x) = f(x) \cdot 1.$$

- ***(Associativity)*** *Suppose, WLOG, that $m \leq n \leq k$. Let $a_i = b_j = 0$ for $m+1 \leq i \leq k$ and $n+1 \leq j \leq k$. Then*

$$\begin{aligned} & f(x) + [g(x) + h(x)] \\ &= f(x) + [(b_0 + d_0) + (b_1 + d_1)x + \ldots + (b_k d_k)x^k] \\ &= (a_0 + b_0 + d_0) + (a_1 + b_1 + d_1)x + \ldots + (a_k + b_k + d_k)x^k \\ &= [(a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_k + b_k)x^k] + d(x) \\ &= [f(x) + g(x)] + h(x) \end{aligned}$$

and if we use the summation notation for $f(x), g(x)$ and $h(x)$, we *have*

$$\begin{aligned} f(x)[g(x)d(x)] &= f(x)\left[\left(\sum_{j=0}^{n} b_j x^j\right)\left(\sum_{l=0}^{k} d_l x^l\right)\right] \\ &= \left[\sum_{i=0}^{m} a_i x^i\right]\left[\sum_{j=0}^{n}\sum_{l=0}^{k} b_j d_l x^{j+l}\right] \\ &= \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{l=0}^{k} a_i b_j d_l x^{i+j+k} \\ &= \left[\sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j}\right]\left[\sum_{l=0}^{k} d_l x^l\right] \\ &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right)\right] h(x) \\ &= [f(x)g(x)]h(x) \end{aligned}$$

- *(**Inverse**) Since R is a ring, and in particular an additive ring, for each $a_i \in R$, $0 \leq i \leq m$, we have that $\exists(-a_i) \in R$ such that $a_i + (-a_i) = 0$. Particularly, we have that*

$$-f(x) = (-a_0) + (-a_1)x + (-a_2)x^2 + \ldots + (-a_m)x^m$$

  is the inverse of $f(x) \in R[x]$.

- *(**Distributivity**) Again, using the summation notation, since R is a ring, we have*

$$\begin{aligned} & f(x)[g(x)+h(x)] \\ &= \left[\sum_{i=0}^{m} a_i x^i\right]\left[\sum_{j=0}^{n} b_j x^j + \sum_{l=0}^{k} d_l x^l\right] \\ &= \left[\sum_{i=0}^{m} a_i x^i\right]\left[\sum_{j=0}^{k} (b_j + d_j) x^j\right] \\ &= \sum_{i=0}^{m}\sum_{j=0}^{k} a_i(b_j + d_j)x^{i+j} = \sum_{i=0}^{m}\sum_{j=0}^{k} (a_i b_j + a_i d_j)x^{i+j} \\ &= \sum_{i=0}^{m}\sum_{j=0}^{k} a_i b_j x^{i+j} + \sum_{i=0}^{m}\sum_{j=0}^{k} a_i d_j x^{i+j} \\ &= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j} + \sum_{i=0}^{m}\sum_{j=0}^{k} a_i d_j x^{i+j} \\ &= f(x)g(x) + f(x)d(x). \end{aligned}$$

  Proof for the other side is similar.

With that, we have that $R[x]$ is a ring.

2. *We already have that R is a ring, and so it suffices to prove that $R \subseteq R[x]$. This is, however, rather simple, since $\forall r \in R$, we have that r is a constant polynomial, and so $r \in R[x]$, and therefore $R \subseteq R[x]$.*

3. *Let*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m \in Z[x]$$
$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n \in R[x].$$

We have that
$$f(x)g(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j}.$$

Since $a_i \in Z$ for $0 \leq i \leq n$, we have

$$f(x)g(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} b_j a_i x^{i+j} = \sum_{j=0}^{n} \sum_{i=0}^{m} b_j a_i x^{j+i} = g(x)f(x)$$

for any $g(x) \in R[x]$. And so $Z[x] = Z(R[x])$.

For $\supseteq$, $f(x) \in Z(R[x]) \implies \forall b \in R \subseteq R[x]$ we have $f(x)b = bf(x)$. It follows that

$$\forall 0 \leq i \leq n \quad a_i b = b a_i$$

and so $a_i \in Z(R)$, which implies that $Z(R[x]) \subseteq Z[x]$. Therefore, $Z(R[x]) = Z[x]$.

□

Warning

Althought $f(x) \in R[x]$ can be used to define a function from $R \to R$, the polynomial is not the same as the function it defines. For example, if $R = \mathbb{Z}_2$, then $\mathbb{Z}_2[x]$ is an infinite set, but there are only 4 different functions from $\mathbb{Z}_2 \to \mathbb{Z}_2$

Proposition 82 (Polynomial Ring is an Integral Domain)

Let R be an integral domain. Then

1. *$R[x]$ is an integral domain.*

2. *If* $f(x) \neq 0$ *and* $g(x) \neq 0$ *in* $R[x]$, *then*[1]

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

3. *The units in* $R[x]$ *are* R^*, *the units in* R.

[1] In order to preserve this for when we have the case of $\deg 0$, we have to define $\deg 0 = -\infty$. Otherwise, say if we define $\deg 0 = -1$, then if $\deg f = -1$, then $\deg(fg) = \deg f + \deg g$ would imply that $\deg g = -2$, which is undefined.

Proof

We shall prove (1) *and* (2) *together.*

1 & 2. *Suppose* $f(x) \neq 0 \neq g(x) \in R[x]$, *say*

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m \quad a_m \neq 0$$
$$g(x) = b_0 + b_1 x + \ldots + b_n x^n \quad b_n \neq 0.$$

Then

$$f(x)g(x) = a_m b_n x^{m+n} + \ldots a_0 b_0.$$

Now since R *is an integral domain, we have that* $a_m b_n \neq 0$ *and so* $f(x)g(x) \neq 0$. *Thus* $R[x]$ *is an integral domain. Moreover, we see that*

$$\deg(fg) = m + n = \deg f + \deg g.$$

3. *Suppose that* $u(x) \in R[x]$ *is a unit of* $R[x]$ *with inverse* $u^{-1}(x)$ *which we shall write as* $v(x)$. *Since* $u(x)v(x) = 1$, *by* (2), *we have that*

$$\deg u + \deg v = \deg 1 = 0. \tag{27.1}$$

Now by (1), $R[x]$ *is an integral domain, and so since* $u(x)v(x) = 1$, *we have that* $u(x) \neq 0 \neq v(x)$. *Therefore,* $\deg u, \deg v \geq 0$, *which implies that we must have* $\deg u = 0 = \deg v$ *from Equation* (27.1). *Therefore, units in* $R[x]$ *are from* R^*.

□

Note

Recall that $\mathbb{Z}_n$ *is an integral domain if and only if* $n = p$ *a prime. If* $n \neq p$, *then, e.g., for* $\mathbb{Z}_4[x]$, *we have*

$$2x \cdot 2x = 4x^2 = 0$$

and so

$$\deg(2x) + \deg(2x) \neq \deg(4x^2) = \deg(2x \cdot 2x).$$

27.1.2 Factorization of Polynomials

Definition 49 (Division of Polynomials)

Let R be a commutative ring and $f(x), g(x) \in R[x]$. We say that $f(x)$ divides $g(x)$, denoted as $f(x) \mid g(x)$ if $\exists q(x) \in R[x]$ such that

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

Definition 50 (Monic Polynomial)

Let R be a commutative ring and $f(x) \in R[x]$. $f(x)$ is monic if its leading coefficient is 1.

We shall prove the following proposition next class.

Proposition

Let R be an integral domain, and $f(x)$, $g(x) \in R[x]$ be monic polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

28 Lecture 28 Jul 09th 2018

28.1 Polynomial Ring (Continued 1)

28.1.1 Factorization of Polynomials (Continued)

Since the actual focus of our study right now is really fields instead of just integral domains, we shall use fields in place of integral domains or commutative rings from here on unless explicitly stated otherwise. So we redefine Definition 49 as follows:

Definition (Division of Polynomials)
Let F be a field and consider $F[x]$. For $f(x), g(x) \in F[x]$, we say that $f(x) \mid g(x)$ if $\exists q(x) \in F[x]$ such that

$$g(x) = q(x) f(x).$$

and restate the last stated proposition as follows:

Proposition 83 ($f(x) \mid g(x) \land g(x) \mid f(x) \implies f(x) = g(x)$)

Let F be a field and $f(x), g(x) \in F[x]$ be monic polynomials[1]. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

[1] Note that polynomials being monic is analogous to integers being positive. For example, you (read: I) should try to reiterate the proof below by replacing the monic property with positive integers.

Proof
Since $f(x) \mid g(x)$ and $g(x) \mid f(x)$, $\exists r(x), s(x) \in F[x]$ such that

$$g(x) = r(x) f(x) \text{ and } f(x) = s(x) g(x).$$

Then

$$f(x) = s(x)r(x)f(x).$$

By Proposition 82, *we have that*

$$\deg f = \deg s + \deg r + \deg f$$

and so

$$\deg s + \deg r = 0 \implies \deg s = \deg r = 0 \quad \because \deg s, \deg r \geq 0.$$

And so $\exists t \in F$ *such that* $f(x) = tg(x)$. *Since* $f(x)$ *and* $g(x)$ *are monic, we must have* $t = 1$ *and so* $f(x) = g(x)$. □

Proposition 84 (Division Algorithm for Polynomials)

Let F *be a field, and* $f(x), g(x) \in F[x]$ *with* $f(x) \neq 0$. *Then* $\exists! q(x), r(x) \in F[x]$ *such that*

$$g(x) = q(x)f(x) + r(x)$$

with $\deg r < \deg f$.[2]

[2] Note that this includes the case for $r = 0$, and this is yet another reason why we defined $\deg 0 = -\infty$.

Proof

We shall first prove the existence of such a $q(x)$ *and* $r(x)$. *For simplicity, write*

$$\deg f = m \text{ and } \deg g = n.$$

If $n < m$, *then*

$$g(x) = 0f(x) + g(x)$$

and we are done. Suppose that $n \geq m$ *and proceed by induction of* n. *Write*

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m$$
$$g(x) = b_0 + b_1 x + \ldots + b_n x^n.$$

Consider[3]

[3] We are implicitly using the fact that $x \in Z[x]$.

$$\begin{aligned} g_1(x) &= g(x) - b_n a_m^{-1} x^{n-m} f(x) \\ &= (b_n x^n + \ldots + b_0) - b_n a_m^{-1} x^{n-m} (a_m x^m + \ldots a_0) \\ &= 0x^n + (b_{n-1} - b_n a_m^{-1} a_{m-1}) x^{n-1} + \ldots, \end{aligned}$$

thus either $g_1(x) = 0$ *or* $g_1(x) \neq 0$*, but in any case,* $\deg g_1 < n$.

Case 1*:* $g_1(x) = 0$*. In this case, we have*

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

and so we can pick

$$\begin{aligned} q(x) &= b_n a_m^{-1} x^{n-m} \\ r(x) &= 0, \end{aligned}$$

and the result follows.

Case 2*:* $g_1(x) \neq 0$*. By induction, we can find some* $q_1(x), r_1(x) \in F[x]$ *such that*

$$g_1(x) = q_1(x) f(x) + r_1(x)$$

with $\deg r_1 < \deg f$*. It follows that*

$$\begin{aligned} g(x) &= g_1(x) + b_n a_m^{-1} x^{n-m} f(x) \\ &= q_1(x) f(x) + r_1(x) + b_n a_m^{-1} x^{n-m} f(x). \end{aligned}$$

So pick

$$\begin{aligned} q(x) &= q_1(x) + b_n a_m^{-1} x^{n-m} \\ r(x) &= r_1(x) < \deg f, \end{aligned}$$

and so the result follows.

To prove uniqueness, suppose we have

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

with $\deg r_1, \deg r_2 < \deg f$*. Then*

$$r_2(x) - r_1(x) = [q_1(x) - q_2(x)] f(x).$$

If $q_1(x) - q_2(x) \neq 0$*, then*

$$\deg(r_2 - r_1) = \deg(q_1 - q_2) + \deg f \geq \deg f$$

which is a contradiction since $\deg(r_2 - r_1) < \deg f$*. Thus we must have* $q_1(x) = q_2(x)$ *and so* $r_1(x) = r_2(x)$. □

Proposition 85 (Properties of the Greatest Common Divisor)

Let F *be a field and* $f(x), g(x) \in F[x]$ *with* $f(x) \neq 0 \neq g(x)$*. Then* $\exists! d(x) \in F[x]$ *such that*

1. $d(x)$ *is monic;*
2. $d(x) \mid f(x)$ *and* $d(x) \mid g(x)$*;*
3. $e(x) \mid f(x) \wedge e(x) \mid g(x) \implies e(x) \mid d(x)$*;*
4. $\exists u(x), v(x) \in F[x] \quad d(x) = u(x)f(x) + v(x)g(x)$

In this case, we say that $d(x)$ *is the* ***greatest common divisor*** *of* $f(x)$ *and* $g(x)$*, and denote this by* $d(x) = \gcd[f(x), g(x)]$.

Proof

Consider the set

$$X = \{u(x)f(x) + v(x)g(x) : u(x), v(x) \in F[x]\}.$$

Since $f(x) = 1 \cdot f(x) + 0 \cdot g(x) \in X$*, the set* X *contains non-zero polynomial and thus contains monic polynomials (since* F *is a field*[4]*). Among all of the monic polynomials, choose*

$$d(x) = u(x)f(x) + v(x)g(x)$$

to have minimal degree. Then we get (1) *and* (4) *in the bag automatically so.* (3) *also follows almost immediately, since*

$$\begin{aligned} &e(x) \mid f(x) \wedge e(x) \mid g(x) \\ &\quad \implies \exists a(x), b(x) \in F[x] \quad f(x) = a(x)e(x) \wedge g(x) = b(x)e(x) \\ &\quad \implies d(x) = u(x)f(x) + v(x) = [u(x)a(x) + v(x)b(x)]e(x) \\ &\quad \implies e(x) \mid d(x). \end{aligned}$$

It remains to prove (2)*. By Proposition 84, we have that* $\exists q(x), r(x) \in$

[4] This is cause if we have

$$f(x) = a_m x^m + \ldots + a_0$$

Then

$$a_m^{-1} f(x) = x^m + \ldots + a_m^{-1} a_0$$

is a moic polynomial in $F[x]$.

$F[x]$ with $\deg r < \deg f$ such that

$$f(x) = q(x)d(x) + r(x).$$

Then

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) = f(x) - q(x)[u(x)f(x) + v(x)g(x)] \\ &= [1 - q(x)u(x)]f(x) - q(x)v(x)g(x). \end{aligned}$$

Note that if $r(x) \neq 0$, then write $k \neq 0 \in F$ as the leading coefficient of $r(x)$. Since F is a field, we have that $\exists k^{-1} \in F$, and so $k^{-1}r(x)$ is a monic polynomial of X with $\deg(k^{-1}r) < \deg d$, which contradicts the fact that the degree of $d(x)$ is minimal. Thus $r(x) = 0$ and $d(x) \mid f(x)$. Using a similar argument, we can show that $d(x) \mid g(x)$. Therefore, (2) follows. $\square$

Exercise 28.1.1
Reiterate this proof for integers, by removing the '(x)' and replacing instances of monic polynomials with positive integers.

29 Lecture 29 Jul 11th 2018

29.1 Polynomial Ring (Continued 2)

29.1.1 Factorization of Polynomials (Continued 2)

Note

If $d(x)$ and $d_1(x)$ satisfies Proposition 85, then in particular (3) is satisfied, i.e.

$$d(x) \mid d_1(x) \text{ and } d_1(x) \mid d(x),$$

then since $d_1(x) = d(x)$ by Proposition 83. Thus $d(x)$ is unique and is therefore called the greatest common divisor of $f(x)$ and $g(x)$, denoted by $\gcd\left(f(x), g(x)\right) = d(x)$.

NOTE THAT in integers, $p \in \mathbb{Z}$ is prime if $p \geq 2$ and whenever $p = ab$, then $a = \pm 1$ or $b = \pm 1$, where $a, b \in \mathbb{Z}$. We can have an "analogous" notion with polynomials.

Definition 51 (Irreducible Polynomials)

Let F be a field. A non-zero polynomial $l(x) \in F[x]$ is ***irreducible*** *if* $\deg l \geq 1$ *and if*

$$l(x) = l_1(x) l_2(x)$$

for $l_1(x), l_2(x) \in F[x]$, then $\deg l_1 = 0$ or $\deg l_2 = 0$ [1].

Polynomials that are not irreducible are called ***reducible polynomials****.*

[1] Note that polynomials of degree 0 are the units of $F[x]$.

Proposition 86 (Euclid's Lemma for Polynomials)

Let F be a field and $a(x), b(x) \in F[x]$. If $l(x) \in F[x]$ is irreducible and $l(x) \mid a(x)b(x)$, then $l(x) \mid a(x)$ or $l(x) \mid b(x)$.

This is a good proof for an exercise.

Exercise 29.1.1
Prove Proposition 86.

Proof

Suppose $l(x) \mid f(x)g(x)$ and $l(x) \nmid f(x)$. Since $l(x) \nmid f(x)$, we have $\gcd[l(x), f(x)] = 1$. *Then by Proposition 85, $\exists s(x), t(x) \in F[x]$ such that*

$$l(x)s(x) + f(x)t(x) = 1.$$

Multiplying the equation by $g(x)$, and since $F[x]$ is a field, we have

$$l(x)s(x)g(x) + f(x)g(x)t(x) = g(x).$$

Since $l(x) \mid f(x)g(x)$ by assumption, we have that $l(x)$ divides the right hand side, and so it must also divide the left hand side, i.e. $l(x) \mid g(x)$. $\square$

Theorem 87 (Unique Factorization Theorem for Polynomials)

Let F be a field and $f(x) \in F[x]$ with $\deg f \geq 1$. *Then we can write*

$$f(x) = cl_1(x)l_2(x) \dots l_m(x)$$

where $c \in F^*$ is a unit, and for $1 \leq i \leq m$, $l_i(x)$ is a irreducible monic polynomial. This factorization is unique up to the order of l_i.

This is, yet again, a good proof for an exercise.

Exercise 29.1.2
Proof Theorem 87.

Proof

We shall only prove for when $f(x)$ is a monic polynomial, for if $f(x)$ is not monic, then it has some leading coefficient $a \neq 1 \in F$. Then since F is a field, we have that $a^{-1}f(x)$ is a monic polynomial for which we can continue our consideration.

Suppose $f(x)$ is a monic polynomial that has the least degree such that it cannot be expressed as a product of irreducible monic polynomials. Clearly, $f(x)$ cannot be irreducible itself, or it would trivially be *expressible as a product of irreducible monic polynomials. Therefore, $\exists s(x), t(x) \in F[x]$ such that*

$$f(x) = s(x)t(x)$$

where $1 \leq \deg s, \deg t \leq \deg f$. Since $f(x)$ is the polynomial of the least degree that cannot be expressed as a product of irreducible monic polnomials, $r(x)$ and $t(x)$ must be expressible as a product of irreducible monic polynomials. But this would contradict the fact that $f(x)$ is not expressible as a product of irreducible monic polynomials, and so $f(x)$ must be

$$f(x) = l_1(x)l_2(x)\ldots l_m(x)$$

where $l_i(x)$ is an irreducible monic polynomial, for $1 \leq i \leq m$. For the case where $f(x)$ is not monic, say with a as its leading coefficient, we would have

$$f(x) = al_1(x)l_2(x)\ldots l_m(x).$$

For uniqueness, suppose

$$f(x) = cl_1(x)l_2(x)\ldots l_m(x) = dk_1(x)k_2(x)\ldots k_n(x)$$

for units $c, d \in F^*$ and irreducible monic polynomials l_i, k_j for $1 \leq i \leq m$ and $1 \leq j \leq n$. Since $l_1(x) \mid f(x)$, by Proposition 86, $l_1(x) \mid k_j(x)$ for some $1 \leq j \leq n$. Relabelling the indices for the k_j's if necessary, we can have that $l_1(x) \mid k_1(x)$. Since $k_1(x)$ is irreducible and monic, we must have that $l_1(x) = k_1(x)$.

Now if we continue this line of argument for $i = 2, 3, ..., m$, and end up with $l_2(x) = k_2(x)$, $l_3(x) = k_3(x)$, $\ldots$, $l_m(x) = k_m(x)$, where, WLOG, we suppose that $m \leq n$. However, we must have that $n = m$, otherwise we would have some k_j, where $m < j \leq n$ that cannot divide any of the l_i's. □

For the sake of comparison with $\mathbb{Z}$, observe the table below:

	$\mathbb{Z}$	$F[x]$
elements	m	$f(x)$
size	$\lvert m \rvert$	$\deg f$
units	$\{\pm 1\}$	F^*
	$\left(\mathbb{Z} \setminus \{0\}\right) \big/ \{\pm 1\} \cong \mathbb{N}$	$\left(F[x] \setminus \{0\}\right) \big/ F^* \cong \{h : h \text{ is monic }\}$
unique	$m = \pm 1 p_1^{\alpha_1} \ldots p_n^{\alpha_n}$	$f(x) = c l_1(x)^{\alpha_1} \ldots l_n(x)^{\alpha_n}$
factorization	p_i prime	$\deg f \geq 1$ and l_i are irreducible
ideals	$\langle\, n \,\rangle : n \in \mathbb{N}$	$\langle\, h(x) \,\rangle : h$ monic
	$\mathbb{Z} \big/ \langle\, n \,\rangle$ is a field	$F[x] \big/ \langle\, h(x) \,\rangle$ is a field
	iff n prime	iff $h(x)$ is irreducible

In the next section, we will be investigating if the analogy given in the last row for polynomials holds.

29.1.2 Quotient Rings of Polynomials

Proposition 88 (Ideals of $F[x]$ are Principal Ideals)

If F is a field. Then all ideas of $F[x]$ are of the form

$$\langle\, h(x) \,\rangle = h(x)F[x] \quad \text{for any } h(x) \in F[x].$$

If $\langle\, h(x) \,\rangle \neq \{0\}$ and $h(x)$ is monic, then it is uniquely determined.

Proof

Let A be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle\, 0 \,\rangle$. If $A \neq \{0\}$, then it contains a non-zero polynomial. Since A is an ideal, it has a monic polynomial[2]*. Amongst all monic polynomials in A, choose $h(x) \in A$ that has the minimal degree. Clearly, $\langle\, h(x) \,\rangle \subseteq A$. To prove for $\supseteq$, note that for $f(x) \in A$, by Proposition 84,*

$$\exists q(x), r(x) \in F[x] \quad f(x) = q(x)h(x) + r(x) \quad \deg r < \deg h.$$

If $r(x) \neq 0$, then let $u \neq 0$ be the leading coefficient of $r(x)$. Then since

[2] If $f(x) \in A$ has a leading coefficient a, then we know that $a^{-1} \in F$, and so $a^{-1} f(x) \in F f(x) \subseteq A$ is monic.

A is an ideal and $f(x), h(x) \in A$, we have

$$\begin{aligned} u^{-1}r(x) &= u^{-1}\left(f(x) - q(x)h(x)\right) \\ &= u^{-1}f(x) - u^{-1}q(x)h(x) \in A. \end{aligned}$$

Then we have that $\deg u^{-1}r = \deg r < \deg h$ is a monic polynomial in A, contradicting the minimality of $\deg h$. Thus $r(x) = 0$ and so $f(x) = q(x)h(x) \in \langle\, h(x)\, \rangle$. Therefore $A \subseteq \langle\, h(x)\, \rangle$ and so $A = \langle\, h(x)\, \rangle$.

Now suppose that $A = \langle\, h(x)\, \rangle = \langle\, k(x)\, \rangle$. Then we must have $h(x) \mid k(x)$ and $k(x) \mid h(x)$. Since $h(x)$ and $k(x)$ are both monic, by Proposition 83, we have that $h(x) = k(x)$. $\square$

30 Lecture 30 Jun 13th 2018

30.1 Polynomial Ring (Continued 3)

30.1.1 Quotient Rings of Polynomials (Continued)

Let A be a non-zero ideal in $F[x]$. By Proposition 88, we know that A is a principal ideal and can be written as $A = \langle h(x) \rangle$, for a unique polynomial $h(x) \in F[x]$.

Suppose that $\deg h = m \geq 1$. Consider the quotient ring $R = F[x] / A$, and so we have

$$R = \left\{ \overline{f(x)} : f(x) + A, f(x) \in F[x] \right\}.$$

Write $t = \bar{x} = x + A$. Then by the **Division Algorithm**[1], we have

$$R = \{ \overline{a_0} + \overline{a_1} t + \ldots + \overline{a_{m-1}} t^{m-1} : a_i \in F \}.$$

The map $\theta : F \to R$, given by $a \mapsto \bar{a}$, is an injective homomorphism, since θ is not a zero map and $\ker \theta$ is an ideal of F[2]. Since we have $F \cong \theta(F)$ by the First Isomorphism Theorem for Rings, by identifying F with $\theta(F)$, we can write

$$R = \{ a_0 + a_1 t + \ldots a_{m-1} t^{m-1} : a_i \in F \}.$$

It is clear that, in R, we have

$$a_0 + a_1 t + \ldots + a_{m-1} t^{m-1} = b_0 + b_1 t + \ldots + b_{m-1} t^{m-1}$$
$$\iff$$
$$\forall i \in \mathbb{Z} \;\; 0 \leq i \leq m-1 \quad a_i = b_i$$

Finally, in the ring R, we have $h(t) = 0$.

[1] This entire part until Proposition 89 might need to be rewritten since I am a little lost as to some of the details regarding the discussion.

[2] Note that a field F has only 2 ideals: $\{0\}$ and F itself. Since $\ker \theta \neq F$, we have that $\ker \theta = \{0\}$ and so θ is injective.

The following proposition follows from the above discussion.

Proposition 89

Let F be a field and let $h(x), f(x) \in F[x]$ be monic with $(\deg h, \deg f \geq 1)$. Then the quotient ring $R = F[x]/A$ is given by

$$R = \{a_0 + a_1 t + \ldots + a_{m-1} t^{m-1} : a_i \in F,\ h(t) = 0\}$$

in which each element of R can be uniquely represented in the above form.

Note

In $\mathbb{Z}$, we have that $\mathbb{Z}/\langle\ n\ \rangle = \mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$ which is analogous to our statement in Proposition 89 for the case of integers.

Example 30.1.1

Consider $\mathbb{R}[x]$ and let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. Then

$$\mathbb{R}[x] = \{a + bt : a, b \in \mathbb{R},\ t^2 + 1 = 0\} \cong \{a + bi : a, b \in \mathbb{R},\ i^2 = -1\} = \mathbb{C}$$

Note

Recall that $\mathbb{Z}_n$ is a field (or an integral domain) if and only if n is prime.

Proposition 90

Let F be a field nad $h(x) \in F[x]$ be a monic polynomial with $\deg h \geq 1$. TFAE:

1. *$F[x]/\langle\ h(x)\ \rangle$ is a field;*
2. *$F[x]/\langle\ h(x)\ \rangle$ is an integral domain;*
3. *$h(x)$ is irreducible in $F[x]$.*

Proof

(1) $\implies$ (2) *since a field is an integral domain (see Proposition 74).*

(2) $\implies$ (3): *Write* $A = \langle\ h(x)\ \rangle$, *If* $h(x) = f(x)g(x)$ *for* $f(x), g(x) \in F[x]$, *then*

$$\begin{aligned}[f(x) + A][g(x) + A] &= f(x)g(x) + A \quad \because A \text{ is an ideal} \\ &= h(x) + A = 0 \in F[x]/A.\end{aligned}$$

Then by (2), *either* $f(x) + A = 0$ *or* $g(x) + A = 0$, *i.e. either* $f(x) \in A$ *or* $g(x) \in A$. *But if* $f(x) \in A = \langle\ h(x)\ \rangle$, *then* $f(x) = q(x)h(x)$ *for some* $q(x) \in F[x]$. *Then* $h(x) = f(x)g(x) = q(x)h(x)g(x)$, *which then implies that* $0 = h(x)[1 - q(x)g(x)] \implies q(x)g(x) = 1$ *since* $F[x]$ *is an integral domain. Then we have that* $\deg g = 0$. *Similarly, if* $g(x) \in A$, *then we have* $\deg f = 0$. *Therefore,* $h(x)$ *is irreducible in* $F[x]$ *by definition.*

(3) $\implies$ (1): *Note that* $F[x]/\langle\ h(x)\ \rangle$ *is a commutative ring. To show that it is a field, it suffices to show that every non-zero element of* $F[x]/\langle\ h(x)\ \rangle$ *has an inverse. Let* $f(x) + A \neq 0 \in F[x]/\langle\ h(x)\ \rangle$ *with* $f(x) \in F[x]$. *Then* $f(x) \notin A$, *and so* $h(x) \nmid f(x)$. *Since* $h(x)$ *is irreducible by* (3), *we have that*

$$d(x) = \gcd[f(x), h(x)] = 1.$$

Then by Proposition 85, $\exists u(x), v(x) \in F[x]$ *such that*

$$1 = u(x)h(x) + v(x)f(x).$$

Since $h(x)u(x) \in A$, *we have that*

$$[v(x) + A][f(x) + A] = 1 + A.$$

It follows that $f(x) + A$ *has an inverse in* $F[x]/\langle\ h(x)\ \rangle$ *and thus* $F[x]/\langle\ h(x)\ \rangle$ *is a field.* $\square$

30.2 Factorizations in Integral Domains

30.2.1 Irreducibles and Primes

We have discussed much about the similarities between $\mathbb{Z}$ and $F[x]$, and in this chapter, we wish to abstract these similarties and study them in a more general manner to see if other sets that share the same kind of properties. For example, if a set has a **unique factorization** for elements and the **principal ideal** being the only ideal of the set, then do we still see the same analogy playing out?

Definition 52 (Division)

Let R be an integral domain and $a, b \in R$. We say that $a \mid b$ if $b = ca$ for some $c \in R$.

Note

Recall that in $\mathbb{Z}$, if $n \mid m$ and $m \mid n$, then $n = \pm m$, and the ideal generated by them are the same, i.e. $\langle\, n \,\rangle = \langle\, m \,\rangle$.

Similarly so in $F[x]$< if $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = cg(x)$ for some $x \in F[x]^* = F^*$, and $\langle\, f(x) \,\rangle = \langle\, g(x) \,\rangle$.

Proposition 91 (Division in an Integral Domain)

Let R be an integral domain. Then $\forall a, b \in R$, TFAE:

1. *$a \mid b$ and $b \mid a$;*
2. *$a = ub$ for some unit $u \in R$;*
3. *$\langle\, a \,\rangle = \langle\, b \,\rangle$.*

This should be an easy exercise.

Exercise 30.2.1
Prove Proposition 91.

Definition 53 (Association)

*Let R be an integral domain. $\forall a, b \in R$, we say that a is **associated to** b, denoted by $a \sim b$, if $a \mid b$ and $b \mid a$.*

Note

By Proposition 91, we have that $a \sim a$ for any $a \in R$.

Also, $a \sim b \iff b \sim a$.

We also have $a \sim b \wedge b \sim c \implies a \sim c$.

In other words, $\sim$ is an equivalence relation in R. Also, it can be shown that[3]

1. $a \sim a' \wedge b \sim b' \implies ab \sim a'b'$.
2. $a \sim a' \wedge b \sim b' \implies (a \mid b \iff b \mid a)$

[3] More exercise is always good.

Exercise 30.2.2
Prove that the two statements following this is true.

Example 30.2.1

Let $R = \mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} : m, n \in \mathbb{Z}\}$. Note that this is an integral domain[4]*. Observe that*

$$(2 + \sqrt{3})(2 - \sqrt{3}) = 1 \implies 2 + \sqrt{3} \text{ is a unit in } R.$$

Then we would have

$$3 + 2\sqrt{3} = (2 + \sqrt{3})\sqrt{3}$$

and so by Proposition 91, we have

$$3 + 2\sqrt{3} \sim \sqrt{3} \in \mathbb{Z}[\sqrt{3}].$$

[4] For $(a + b\sqrt{3}), (c + d\sqrt{3}) \in R$ such that

$$(a + b\sqrt{3})(c + d\sqrt{3}) = 0$$

we would have that

$$(a + b\sqrt{3})(a - b\sqrt{3})(c + d\sqrt{3})(c - d\sqrt{3}) = 0$$
$$(a^2 - 3b^2)(c^2 - 3d^2) = 0.$$

Since $\mathbb{Z}$ is an integral domain, suppose $a^2 - 3b^2 = 0$. If $b = 0$, then $a = 0$ and we are done. If $b \neq 0$, then we have $3 = \left(\frac{a}{b}\right)^2$, and we notice that $\sqrt{3}$ is irrational. Thus it can only be that $b = 0$. Therefore, $a + b\sqrt{3} = 0$, implying that there are no zero divisors in $R = \mathbb{Z}[\sqrt{3}]$.

31 Lecture 31 Jul 16th 2018

31.1 Factorizations in Integral Domains (Continued)

31.1.1 Irreducibles and Primes (Continued)

Note

Recall that if R is an integral domain and $a, b \in R$, we say that $a \mid b$ if $\exists c \in R$ such that $b = ca$.

Also, recall the definition of **associativity**.

Definition (Associativity)

If $a \mid b$ and $b \mid a$, then we say that a is associative to b, and denote $a \sim b$ if and only if $\exists u \in R$, which is a unit, such that $a = ub$, and we have $\langle\, a \,\rangle = \langle\, b \,\rangle$.

Definition 54 (Irreducible)

Let R be an integral domain. We say $p \in R$ is ***irreducible*** *if $p \neq 0$ is not a unit, and $p = ab \in R$, then either a or b is a unit. An element that is not* ***irreducible*** *is* ***reducible***.

Example 31.1.1

Let $R = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ and $p = 1 + \sqrt{-5}$. We want to show that p is an irreducible in R. Note that for $z = m + n\sqrt{-5} \in$

R, the **norm** *of z is defined to be*

$$N(z) = \left(m + n\sqrt{-5}\right)\left(m - n\sqrt{-5}\right) = m^2 + 5n^2 \in \mathbb{N} \cup \{0\}$$

Note that[1]

$$N(xy) = N(x)N(y).$$

Now suppose that $p = ab \in R$. Then

$$6 = N(p) = N(a)N(b).$$

However, since $N(z) = m^2 + 5n^2$ for some $m, n \in \mathbb{Z}$, we must have that $N(z) \neq 2, 3$. Thus, we have either $N(a) = 1$ or $N(b) = 1$, which in turn implies that $a = \pm 1$ and $b = \pm 1$, which implies that a or b is a unit. Therefore, p is irreducible.

[1] **Proof**
Let $x = m + n\sqrt{-5}$ and $y = a + b\sqrt{-5}$. Note that

$$N(x) = m^2 + 5n^2.$$

Then

$$\begin{aligned} & N(x)N(b) \\ & = m^2a^2 + 25n^2b^2 + 5(n^2a^2 + m^2b^2). \end{aligned}$$

and since

$$xy = ma - 5nb + \sqrt{-5}(na + mb),$$

we have

$$\begin{aligned} & N(xy) \\ & = (ma - 5nb)^2 + 5(na + mb)^2 \\ & = m^2a^2 + 25n^2b^2 + 5(n^2a^2 + m^2b^2) \end{aligned}$$

Proposition 92 (Properties of Irreducibles)

Let R be an integral domain. Let $0 \neq p \in R$. TFAE:

1. *p is irreducible;*
2. $d \mid p \implies d \sim 1 \veebar d \sim p$;
3. $p \sim ab \in R \implies p \sim a \veebar p \sim b$;
4. $p = ab \in R \implies p \sim a \veebar p \sim b$.

Consequently, if $p \sim q$, we have p is irreducible if and only if q is irreducible.

Proof

$(1) \implies (2)$: $\quad d \mid p \implies \exists c \in R \quad dc = p.$

d *is a unit* $\implies d \sim 1 \ \square$;

d *is not a unit* $\implies c$ *is a unit* $\because p$ *is irreducible*

$\implies \exists c^{-1} \in R \quad cc^{-1} = 1 \implies d = pc^{-1} \implies d \sim p.$

$(2) \implies (3)$: $\quad p \sim ab \implies \exists c, c^{-1} \in R \ \ cc^{-1} = 1 \quad p = cab$

Suppose $p \not\sim a$.

$a \mid cab \implies a \mid p \overset{(2)}{\implies} a \sim 1 \implies ca$ *is a unit* $\implies p \sim b.$

$(3) \implies (4)$: $\quad 1$ *is a unit and so $p = ab \implies p \sim ab$, and the result follows from (3).*

$(4) \implies (1)$: $\because (4)$ $p = ab \implies p \sim a \veebar p \sim b$.

WLOG $p \sim a \implies \exists c, c^{-1} \in R$ $cc^{-1} = 1$ $p = ac \implies ac = ab$

Note $a \neq 0 \because p \neq 0 \land p \sim a$.

Then by Proposition 73, $c = b \implies b$ is a unit $\implies p$ is irreducible.

By (3) and (1), $p \sim q \iff p, q$ are irreducibles. $\square$

Definition 55 (Prime)

Let R be an integral domain and $p \in R$. We say p is *prime* in R if $p \neq 0$ is not a unit, and if $p \mid ab \in R \implies p \mid a \veebar p \mid b$.

Note

If $p \sim q$, then p is prime $\iff q$ is prime. This is a clear result, since $p \sim q \implies p \mid q \land q \mid p$, and if p is prime, then $q \mid p \mid ab \implies q \mid p \mid a \veebar q \mid p \mid b$.

Also, by induction, if p is prime and

$$p \mid a_1 a_2 \ldots, a_n,$$

then $p \mid a_i$ for some $1 \leq i \leq n$.

Proposition 93 (Primes are Irreducible)

Let R be an integral domain and $p \in R$. p is prime $\implies p$ is irreducible.

Proof

$\because p$ is prime $p = ab \implies p \mid a \veebar p \mid b$.

WLOG $p \mid a \implies \exists d \in R$ $dp = a$

$\implies a = dp = dab = adb$ $\because R$ is commutative

$\because a \neq 0$ and R is an integral domain, by Proposition 73, $1 = db \implies b$ is a unit (with d being its multiplicative inverse).

$\therefore p$ is irreducible. $\square$

The converse of Proposition 93 is false.

Example 31.1.2

Recall from Example 31.1.1 that $1+\sqrt{-5}$ *is irredubile in* $\mathbb{Z}[\sqrt{-5}]$*. Recall that for* $d = m + n\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$*, we defined the* ***norm*** *as*

$$N(d) = m^2 + 5n^2 \in \mathbb{N} \cup \{0\}.$$

Before proceeding further, note that

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5}) = p(1-\sqrt{-5}).$$

Suppose p *is prime, which then* $p \mid 2 \cdot 3 \implies p \mid 2 \veebar p \mid 3$*. Suppose* $p \mid 2 \implies \exists q \in \mathbb{Z}[\sqrt{-5}] \quad 2 = pq$*. It follows that*

$$4 = N(2) = N(p)N(q) = 6N(q)$$

which is impossible. Similarly, $p \mid 3 \implies \exists r \in R \quad 3 = rp \implies$

$$9 = N(3) = N(r)N(p) = 6N(r)$$

is also impossible. Therefore, p *is not prime.*

31.1.2 Ascending Chain Condition

Definition 56 (Ascengding Chain Condition on Principal Ideals (ACCP))

An integral domain R *is said to satisfy the* ***ascending chain condition on principal ideals*** *(ACCP) if for any ascending chain*

$$\langle\, a_1 \,\rangle \subseteq \langle\, a_2 \,\rangle \subseteq \langle\, a_3 \,\rangle \subseteq \ldots$$

of principal ideals in R*,* $\exists n \in \mathbb{N}$ *such that*

$$\langle\, a_n \,\rangle = \langle\, a_{n+1} \,\rangle = \ldots .$$

Example 31.1.3

$\mathbb{Z}$ *satisfies ACCP.*

If $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \ldots$ *in* $\mathbb{Z}$, *then*

$$a_2 \mid a_1,\ a_3 \mid a_2,\ \ldots .$$

Taking the absolute value of each of the a_i*'s, we have that*

$$|a_1| \geq |a_2| \geq |a_3| \geq \ldots .$$

Since each of the $|a_i| \geq 0$ *is an integer, there must be some* $n \in \mathbb{N}$ *where*

$$|a_n| = |a_{n+1}| = \ldots .$$

This implies that $a_{i+1} = \pm a_i$ *for* $i \geq n$. *Therefore, we have that*

$$\langle a_i \rangle = \langle a_{i+1} \rangle \quad \text{for } i \geq n,$$

thus showing that the ACCP is satisfied.

Theorem 94 (Factorization on an Integral Domain Satisfying ACCP)

Let R *be an integral domain that satisfies ACCP. Let* $0 \neq a \in R$ *be a non-unit. Then* a *is a product of irreducible elements of* R.

Proof

Suppose to the contrary that a *is not a product of irreducible elements of* R. *Then* a *itself must not be irreducible. By Proposition 92,* $\exists x_1 \in R$ *such that*

$$a = x_1 a_1 \quad a \not\sim x_1 \wedge a \not\sim a_1.$$

Note that at least one of x_1 *or* a_1 *is not a product of irreducible elements, for otherwise* a *would be a product of irreducible elements. WLOG, suppose* a_1 *is not a product of irreducible elements. Then Proposition 92* $\implies \exists x_2 \in R$

$$a_1 = x_2 a_2 \quad a_1 \not\sim x_2 \wedge a \not\sim a_2.$$

We can continue this argument infinitely so, in which we will then get an ascending chain of principal ideals

$$\langle a \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots .$$

However, since

$$a \not\sim a_1 \not\sim a_2 \not\sim \dots ,$$

💧 *Proposition 91 implies that*

$$\langle\, a \,\rangle \subsetneq \langle\, a_1 \,\rangle \subsetneq \langle\, a_2 \,\rangle \subsetneq \dots ,$$

which contradicts the assumption that R satisfies ACCP. Therefore, all non-unit $0 \neq a \in R$ *is a product of irreducible elements of R.* $\square$

32 Lecture 32 Jul 18th 2018

32.1 Factorizations in Integral Domains (Continued 2)

32.1.1 Ascending Chain Condition (Continued)

Theorem 95 (Integral Domain that Satisfies ACCP has a Polynomial Ring that Satisfies ACCP)

If R is an integral domain satisfying ACCP, so does $R[x]$.

Proof

Suppose not, i.e. $R[x]$ does not satisfy ACCP. Then there exists a chain of principal ideals such that

$$\langle f_1 \rangle \subsetneq \langle f_2 \rangle \subsetneq \langle f_3 \rangle \subsetneq \ldots \quad \text{in } R[x]. \tag{32.1}$$

Let a_i be the leading coefficient of f_i. Note that $a_i \in R$. From Equation (32.1), we have that $f_{i+1} \mid f_i$, and so we must have $a_{i+1} \mid a_i$. Then

$$\langle a_1 \rangle \subseteq lraa_2 \subseteq \langle a_3 \rangle \subseteq \ldots .$$

Since R satisfies ACCP, $\exists n \in \mathbb{N}$ such that

$$\langle a_n \rangle = \langle a_{n+1} \rangle = \ldots ,$$

i.e. $a_n \sim a_{n+1} \sim \ldots$. For $m \geq n$, let $f_m = g f_{m+1}$ for some $g(x) \in R[x]$. If $b \in R$ is the leading coefficient of $g(x)$, then $a_m = b a_{m+1}$. Since $a_m \sim a_{m+1}$. b is a unit in R. However, $g(x)$ is not a unit in $R[x]$ since $\langle f_m \rangle \subsetneq \langle f_{m+1} \rangle$. Thus $g(x) \neq b$, which implies $\deg g \geq 1$. Then by

Proposition 82,

$$\deg f_m > \deg f_{m+1},$$

which is true for $m \geq n$. *By the same argument, we have that*

$$\deg f_m > \deg f_{m+1} > \deg f_{m+2} > \dots ,$$

which leads to a contradiction since $\deg f_i \geq 0$ *for all* $i \in \mathbb{N}$. *Thus* $R[x]$ *must satisfy ACCP.* □

Example 32.1.1

Since $\mathbb{Z}$ *satisfies ACCP, by Theorem 95,* $\mathbb{Z}[x]$ *also satisfies ACCP.*

32.1.2 Unique Factorization Domains and Principal Ideal Domains

Definition 57 (Unique Factorization Domain (UFD))

An integral domain R *is called a* ***unique factorization domain*** *(UFD) if it satisfies the following conditions:*

1. *If* $0 \neq a \in R$ *is a non-unit, then* a *is a product of irreducible elements in* R.
2. *If* $p_1 p_2 \dots p_r \sim q_1 q_2 \dots q_s$ *where* p_i *and* q_i *are irreducibles, then* $r = s$ *and (possibly after relabelling)* $p_i \sim q_i$ *for each* $1 \leq i \leq r = s$.

Example 32.1.2

Both $\mathbb{Z}$ *and* $F[x]$, *where* F *is a field, are UFDs.*

Example 32.1.3

Any field is a UFD since all elements in a field are either 0 *or units.*

Recall Proposition 93: If p is a prime, then p is irreducible. In comparison, we have the following:

Proposition 96 (Irreducibles are Primes in a UFD)

Let R *be a UFD and* $p \in R$. *If* p *is irreducible, then* p *is a prime.*

This also means that in a UFD, primes and irreducibles are the same.

Proof

Let $p \in R$ be an irreducible. If $p \mid ab \in R$, then $\exists d \in R$ such that $ab = pd$. Since R is a UFD, we can factor a, b, and d into irreducible elements, say

$$\begin{aligned} a &= p_1 p_2 \dots p_k \\ b &= q_1 q_2 \dots q_l \\ d &= r_1 r_2 \dots r_m. \end{aligned}$$

where $k, l, m \in \mathbb{N} \cup \{0\}$. Then

$$ab = pd \iff p_1 \dots p_k q_1 \dots q_l = p r_1 \dots r_m.$$

Since p is irreducible, by Proposition 92, $p \sim p_i$ or $p \sim q_i$. Therefore $p \mid a$ or $p \mid b$, which is the definition of a prime. $\square$

Example 32.1.4

Consider $R = \mathbb{Z}[\sqrt{-5}]$ and $p = 1 + \sqrt{-5}$. We proved that p is irreducible but p is not prime. Then by Proposition 96, we have that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Definition 58 (Greatest Common Divisor)

Let R be an integral domain, and $a, b \in R$. We say $d \in R$ is the ***greatest common divisor*** *of a, b, denoted as $\gcd(a, b) = d$, if it satisfies the following conditions:*

1. $d \mid a$ *and* $d \mid b$;
2. $e \in R \; e \mid a \wedge e \mid b \implies e \mid d$.

Proposition 97

Let R be a UFD and $a, b \in R$. If $p_1, ..., p_k$ are the non-associated primes dividing a and b, say

Exercise 32.1.1
Prove Proposition 97.

$$a \sim p_1^{a_1} \dots p_k^{a_k}$$
$$b \sim p_1^{b_1} \dots b_k^{b_k}$$

with $a_i, b_i \in \mathbb{N}$, *then*

$$\gcd(a, b) \sim p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)}$$

Proof

Let $d = \gcd(a, b)$. *It suffices to show that*

$$d \mid p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)},$$

since $p_1^{\min(a_q, b_1)} \dots p_k^{\min(a_k, b_k)}$ *divides* a *and* b *and so it must also divide* d.

Suppose that $d \nmid p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)}$. *Then* $d \not\sim p_i^{\min(a_i, b_i)}$ *for* $1 \leq i \leq k$. *But that implies that* $d = 1$, *otherwise* $d \nmid a$ *and* $d \nmid b$. *However,*

$$p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)} \nmid 1$$

which contradicts the choice of d *as the greatest common divisor.* □

Note

If R *is a UFD with* $d, a_1, ..., a_m \in R$, *then*

$$\gcd(da_1, da_2, ..., da_m) \sim d \gcd(a_1, ..., a_m).$$

Theorem 98 (UFD and ACCP)

Let R *be an integral domain. TFAE:*

1. *R is a UFD;*
2. *R satisfies ACCP and $\forall a, b \in R$, $\exists d = \gcd(a, b) \in R$;*
3. *R satsifies ACCP and every irreducible element in R is a prime.*

Proof

(1) $\implies$ (2): *By Proposition 97, $\forall a, b \in R \quad \exists d = \gcd(a, b) \in R$. Suppose there exists*

$$0 \neq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \; subsetneq \ldots \text{ in } R.$$

Since $\langle a_1 \rangle \neq R$, a_1 is not a unit[1] *Since R is a UFD, let $a_1 \sim p_1^{k_1} \ldots p_r^{k_r}$, where the p_i's are non-associated primes and $k_i \in \mathbb{N}$, for $1 \leq i \leq r$. Since $a_i \mid a_1$ for $2 \leq i \leq r$, we have that*

$$a_i \sim p_1^{d_{i,1}} p_2^{d_{i,2}} \ldots p_r^{d_{i,r}}$$

where $0 \leq d_{i,j} \leq k_j$ for $1 \leq j \leq r$. This implies that there are only finitely many non-associated choices for a_i, which implies that there exists $m \neq n$ such that $a_m \sim a_n \implies \langle a_m \rangle = \langle a_n \rangle$, a contradiction. Therefore, R must satisfy ACCP.

[1] Otherwise, $1 \in \langle a_1 \rangle \implies \langle a_1 \rangle = R$.

(2) $\implies$ (3): *Let $p \in R$ be an irreducible, and suppose $p \mid ab$. By (2), let $d = \gcd(a, p)$. Then $d \mid p$, and by Proposition 92, we have either $p \sim 1$ or $d \sim p$ since p is an irreducible. If $d \sim p$, since $d \mid 1$, we have that $p \mid 1$. If $d \sim 1$, note that we have that*

$$\gcd(ab, pb) \sim b \gcd(a, p) \sim b.$$

Since $p \mid ab$ and $p \mid pb$, we have $p \mid \gcd(ab, pb)$ and so $p \mid b$.

: (3) $\implies$ (1): *R satisfies ACCP implies, by Proposition 96, every non-unit non-zero $a \in R$ is a product of irreducible elements in R. It sufficies to prove that the factorization is unique*[2]*. Suppose we have*

[2] This would ssatisfy the definition of a UFD.

$$p_1 p_2 \ldots p_r \sim q_1 q_2 \ldots q_s$$

where p_i and q_j are irreducibles, for $1 \leq i \leq r$ and $1 \leq j \leq s$. Now $p_1 \mid p_1 p_2 \ldots p_r$, and so $p_1 \mid q_1 q_2 \ldots q_s$. By Proposition 92 and since p_1 is an irreducible, $p_1 \sim q_j$ for some $1 \leq j \leq s$. We may relabel this q_j to be q_1. Now since $p_1 \sim q_1$ and $p_1 p_2 \ldots p_r \sim q_1 q_2 \sim q_s$, $\exists a, b \in R$ that are units suchthat

$$\begin{aligned} &a p_1 = q_1 \text{ and } p_1 p_2 \ldots p_r = b q_1 q_2 \ldots q_s = b a p_1 q_2 \ldots q_s \\ &\implies p_2 \ldots p_r = b a q_2 \ldots q_s \implies p_2 \ldots p_r \sim q_2 \ldots q_s. \end{aligned}$$

By repeating the same argument, we have that $r = s$ and $p_i \sim q_i$ for $1 \leq i \leq r$. Therefore the factorization is unique. $\square$

Definition 59 (Principal Ideal Domain (PID))

An integral domain R is a ***principal ideal domain*** *(PID) if every ideal is principal.*

Example 32.1.5

A field F is a PID since its only ideals are $\{0\} = \langle\, 0 \,\rangle$ and $F = \langle\, 1 \,\rangle$.

Example 32.1.6

$\mathbb{Z}$ and $F[x]$ are PIDs.

33 Lecture 33 Jul 20th 2018

33.1 Factorizations in Integral Domains (Continued 3)

33.1.1 Unique Factorization Domains and Principal Ideal Domains (Continued)

Note

Recall the definition of a gcd: $d = \gcd(a, b)$ *if*

1. $d \mid a \wedge d \mid b$
2. $\forall e \in R \; e \mid a \wedge e \mid b \implies e \mid d$

Proposition 99 (Bezout's Lemma in PIDs)

Let R be a PID and let $a_1, ..., a_n$ be non-zero elements of R. Then $d \sim \gcd(a_1, ..., a_n)$ exists and $\exists r_1, ..., r_n \in R$ such that

$$\gcd(a_1, ..., a_n) = r_1 a_1 + \ldots + r_n a_n.$$

Proof

Consider

$$A = \{r_1 a_1 + \ldots + r_n a_n : r_i \in R\}.$$

Note that A is an ideal of R, since $\forall a \in A \; \forall r \in R$, we have

$$aR \ni ar = rr_1 a_1 + \ldots + rr_n a_n \in A.$$

Since R is a PID, $\exists d \in R$ such that $A = \langle\, d \,\rangle$. Thus

$$\exists r_1, ..., r_n \in R \quad d = r_1 a_1 + \ldots r_n a_n.$$

It remains to prove that $d \sim \gcd(a_1, ..., a_n)$. Since $A = \langle\, d \,\rangle$ and $a_i \in R$, clearly so $d \mid a_i$, for all $1 \leq i \leq n$. Also, $\exists r \in R$ $1 \leq i \leq n$ $r \mid a_i \implies r \mid (r_1 a_1 + \ldots + r_n a_n) \implies r \mid d$. Then by the definition of a gcd, we have $d \sim \gcd(a_1, ..., a_n)$. $\square$

Theorem 100 (PIDs are UFDs)

Every PID is a UFD.

Proof

If R is a PID, by Theorem 98 and Proposition 99, it suffices to show that R satisfies ACCP. If $\langle\, a_1 \,\rangle \subseteq \langle\, a_2 \,\rangle \subseteq \ldots$ in R, let

$$A = \langle\, a_1 \,\rangle \cup \langle\, a_2 \,\rangle \cup \ldots .$$

Note that A is an ideal, since $\forall a \in A$, $a \in \langle\, a_i \,\rangle$ for some i, and so $\forall r \in R$, we have $ar \in \langle\, a_i \,\rangle \subseteq A$. Now since R is a PID, $\exists a \in R$ such that $A = \langle\, a \,\rangle$. Then $a \in \langle\, a_n \,\rangle$ for some $n \in \mathbb{N}$. Then

$$\langle\, a \,\rangle \subseteq \langle\, a_n \,\rangle \subseteq \langle\, a_{n+1} \,\rangle \subseteq \ldots \subseteq A = \langle\, a \,\rangle.$$

which implies that $\langle\, a_n \,\rangle = \langle\, a_{n+1} \,\rangle = \ldots$ in R, i.e. R satisfies ACCP. Therefore R is a UFD. $\square$

Note

We have the following chain of definitions:

$$\text{field} \subsetneq \text{PID} \subsetneq \text{UFD} \subsetneq \text{ACCP} \subsetneq \text{commutative ring} \subsetneq \text{ring}.$$

If F is a field, then we have shown that both F and $F[x]$ are PIDs.

And so we have the following consequence from Theorem 100:

Corollary 101 (Polynomial Rings over a Field is a UFD)

If F is a field, then F and $F[x]$ are UFDs.

Example 33.1.1

$\mathbb{Z}[x]$ is not a PID.

Consider

$$A = \{2n + xf(x) : n \in \mathbb{Z},\, f(x) \in \mathbb{Z}[x]\}.$$

Note that A is indeed an ideal, since $\forall a \in A$ and $g(x) \in \mathbb{Z}[x]$, let $g(x) = b_0 + b_1 x + \ldots b_m x^m$, and we have

$$\begin{aligned} ag(x) &= (2n + xf(x))g(x) \\ &= 2nb_0 + 2n\left(b_1 x + \ldots b_m x^m\right) + xf(x)g(x) \\ &= 2nb_0 + x(2nb_1 + \ldots + 2nb_m x^{m-1}) + xf(x)g(x) \\ &= 2nb_0 + x[h(x) + f(x)g(x)] \in A \end{aligned}$$

where $h(x) = 2nb_1 + 2nb_2 x + \ldots + 2bnb_m x^{m-1}$. Suppose for contradiction that $A = \langle\ g(x)\ \rangle$ for some $g(x) \in \mathbb{Z}[x]$. Since $2 \in A$, we must have $g(x) \mid 2$. It follows that $g(x) = \pm 1$ or ± 2 [1]. Thus $A = \mathbb{Z}[x]$ or $A = \langle\ 2\ \rangle$, respectively for $g(x) = \pm 1$ or ± 2. However, $A = \mathbb{Z}[x]$ means that A is not a principal ideal, and if $A = \langle\ 2\ \rangle$, then there must be no $xf(x)$ in A, i.e. this is an impossible case. Therefore $\mathbb{Z}[x]$ is not a PID.

[1] We must have $\deg g = 0$, otherwise there is no way that $g(x) \mid 2$. And as $\deg g = 0$, we have that $|g(x)| \leq 2$ in $\mathbb{Z}$, and hence the result.

Theorem 102 (Quotient over a PID)

Let R be a PID and $0 \neq p \in R$ a non-unit. TFAE:

1. *p is prime;*
2. *$R/\langle\ p\ \rangle$ is a field;*
3. *$R/\langle\ p\ \rangle$ is an integral domain.*

Proof

(1) $\implies$ (2): *Consider a non-zero element* $a + \langle\ p\ \rangle \in R/\langle\ p\ \rangle$. *Clearly then,* $a \notin \langle\ p\ \rangle$ *and so* $p \nmid a$. *Consider*

$$A = \{ra + sp : r, s \in R\},$$

which is (quite clearly so) an ideal in R. *Since* R *is a PID,* $\exists d \in R$ *such that* $A = \langle\ d\ \rangle$. *Since* $p \in A$ [2], *we have* $d \mid p$. *Since* p *is prime,* p *is irreducible*[3], *and so* $d \sim p$ *or* $d \sim 1$ *by Proposition 92. If* $d \sim p$, *then* $\langle\ p\ \rangle = \langle\ d\ \rangle = A \implies p \mid a$, *which contradicts the fact that* $p \nmid a$.

And so we are left with $d \sim 1$. *It follows that* $A = \langle\ 1\ \rangle = R$. *In particular, we have* $1 \in A$, *and say then* $ba + cp = 1$ *for some* $b, c \in R$. *It so follows that*

$$(b + \langle\ p\ \rangle)(a + \langle\ p\ \rangle) = ba + \langle\ p\ \rangle = 1 + \langle\ p\ \rangle \in R/\langle\ p\ \rangle.$$

Therefore $a + \langle\ p\ \rangle$ *is a unit and so* $R/\langle\ p\ \rangle$ *is a field.*

(2) $\implies$ (3): *By Proposition 74, every field is an integral domain.*

(3) $\implies$ (1): *Suppose* $p \mid ab \in R$. *Then*

$$(a + \langle\ p\ \rangle)(b + \langle\ p\ \rangle) = ab + \langle\ p\ \rangle = 0 + \langle\ p\ \rangle.$$

Since $R/\langle\ p\ \rangle$ *is an integral domain, WLOG, say we have that* $a + \langle\ p\ \rangle = 0 + \langle\ p\ \rangle$. *Then* $a \in \langle\ p\ \rangle \implies p \mid a$. *Otherwise, we would have* $p \mid b$. □

[2] Since R is a PID, it is a integral domain and so $0 \in R$. Then $0 \cdot a + 1 \cdot p = p \in A$.

[3] By Proposition 93.

Conseuqently, alongside with Proposition 77 and Proposition 78, we have:

Corollary 103 (Non-Zero Prime Ideals in a PID are Maximal)

Every non-zero prime ideal of a PID is maximal.[4]

[4] In other words, in a PID, maximal ideals are prime ideals and vice versa (see Corollary 79.)

Note

The results of Theorem 102 may fail if we are simply in a UFD.

Example 33.1.2

$R = \mathbb{Z}[x]$ is a UFD. Consider the principal ideal $\langle\ x\ \rangle \subseteq R$. Then $R/\langle\ x\ \rangle \cong \mathbb{Z}$, which we know is an integral domain but not a field. $\therefore \langle\ x\ \rangle$ is a prime ideal in $\mathbb{Z}[x]$ but not maximal.

33.1.2 Gauss' Lemma

Definition 60 (Content)

*If R is a UFD and if $0 \neq f(x) \in R[x]$, the greatest common divisor of the non-zero coefficients of $f(x)$ is called the **content** of $f(x)$, and denoted by* $\mathrm{c}(f)$.

Definition 61 (Primitive Polynomials)

*If R is a UFD and if $0 \neq f(x) \in R[x]$, then if $\mathrm{c}(f) \sim 1$, we say that $f(x)$ is a **primitive polynomial**, or simply say that $f(x)$ is **primitive**.*

Example 33.1.3

In $\mathbb{Z}[x]$, we have

$$\begin{aligned} \textit{(primitive)} &: \mathrm{c}(6 + 10x^2 + 15x^3) \sim 1; \\ \textit{(non-primitive)} &: \mathrm{c}(6 + 9x^2 + 15x^3) \sim 3. \end{aligned}$$

34 Lecture 34 Jul 23rd 2018

34.1 Factorizations in Integral Domains (Continued 4)

34.1.1 Gauss' Lemma (Continued)

Lemma 104 (Role of the Content)

Let R be a UFD and let $0 \neq f(x) \in R[x]$.

1. *$f(x)$ can be written as*

$$f(x) = \mathrm{c}(f) f_1(x)$$

   where $f_1(x)$ is primitive.

2. *If $0 \neq b \in R$, then $\mathrm{c}(bf) = b\,\mathrm{c}(f)$.*

Proof

1. *Let $c = \mathrm{c}(f) \sim \gcd(a_0, a_1, ..., a_m)$, where we let $f(x) = a_m x^m + \ldots + a_0$. Since c is the gcd, for $0 \leq i \leq m$, write*

$$a_i = cb_i.$$

   Then $f(x) = cf_1(x)$ where

$$f_1(x) = b_m x^m + \ldots + b_0.$$

   Then by Proposition 97, we have

$$c \sim \gcd(a_0, a_1, ..., a_m) \sim \gcd(cb_0, ..., cb_m) \sim c \gcd(b_0, ..., b_m).$$

It follows that $\gcd(b_0, ..., b_m) \sim 1$ *and so* $f_1(x)$ *is primitive.*

2. *This is an immediate result from Proposition 97.*

□

Lemma 105 (Non-Trivial Irreducible Polynomials are Primitive)

Let R *be a UFD and* $l(x) \in R[x]$ *be irreducible with* $\deg l \geq 1$. *Then* $\mathrm{c}(l) \sim 1$.

Proof

By Lemma 104, we can write

$$l(x) = \mathrm{c}(l) l_1(x)$$

for some $l_1(x) \in R[x]$. *Since* $l(x)$ *is irreducible, by Proposition 92, we have either* $\mathrm{c}(l) \sim 1$ *or* ł$_1(x) \sim 1$. *However, since* $\deg l = \deg l_1 \geq 1$, *we have that* $l_1(x) \not\sim 1$ *and so* $\mathrm{c}(l) \sim 1$. □

Example 34.1.1

The polynomial $2x + 4 \in \mathbb{Q}[x]$ *is irreducible*[1]. *However, the polynomial* $2x + 4 \in \mathbb{Z}[x]$ *is not irreducible. For instance,*

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

but both 2 *and* $(x + 2)$ *are not units of* $\mathbb{Z}[x]$.

[1] Any factorization of $2x + 4$ in $\mathbb{Q}[x]$ will always result in one of the factors being a unit.

Theorem 106 (Gauss' Lemma)

Let R *be a UFD. For any non-zero* $f(x), g(x) \in R[x]$, *we have*

$$\mathrm{c}(fg) \sim \mathrm{c}(f)\,\mathrm{c}(g)$$

Proof

By Lemma 104, let

$$f(x) = \mathrm{c}(f) f_1(x)$$
$$g(x) = \mathrm{c}(g) g_1(x),$$

where $f_1(x)$ and $g_1(x)$ are primitive. Then by part (2) of Lemma 104, we have

$$\mathrm{c}(fg) = \mathrm{c}(\mathrm{c}(f) f_1 \, \mathrm{c}(g) g_1) = \mathrm{c}(f)\,\mathrm{c}(g)\,\mathrm{c}(f_1 g_1).$$

From here, if $(f_1 g_1) \sim 1$, our proof is complete. Thus, it suffices to show that $f(x)g(x)$ is primitive when $f(x)$ and $g(x)$ are primitive, i.e. $\mathrm{c}(f) \sim 1\,\mathrm{c}(g)$.

Suppose that we have that $f(x)$ and $g(x)$ are primitive but $f(x)g(x)$ is not primitive. Since R is a UFD, by Theorem 98, $\exists p \in R$ such that p divides each coefficient of $f(x)g(x)$. Write

$$f(x) = a_0 + a_1 x + \ldots a_m x^m$$
$$g(x) = b_0 + b_1 x + \ldots b_n x^n.$$

Since $f(x)$ and $g(x)$ are primitive, p does not divide each a_i or each b_j [2]*. Then $\exists k, s \in \mathbb{N} \cup \{0\}$ such that*

[2] Otherwise, $f(x)$ and $g(x)$ would not be primitives since if p does divide all of the coefficients, then $\mathrm{c}(f) \not\sim 1$ or $\mathrm{c}(g) \not\sim 1$, i.e. they are not primitives.

- *$p \nmid a_k$ but $p \mid a_i$ for $0 \leq i < k$ and*
- *$p \nmid b_s$ but $p \mid b_j$ for $0 \leq j < s$.*

Note that the coefficient of x^{k+s} in $f(x)g(x)$ is

$$c_{k+s} = \sum_{i+j=k+s} a_i b_j.$$

From the two bullet points, we have that p divides all a_i and b_j with $i + j = k + s$ except $a_k b_s$. It follows that $p \nmid c_{k+s}$, which contradicts the fact that p divides all coefficient of $f(x)g(x)$. Therefore, $f(x)g(x)$ is primitive. □

Theorem 107 (Reducibility in the Field of Fractions)

Let R be a UFD whose field of fractions is F [3]*. If $l(x) \in R[x]$ is irreducible in $R[x]$, then $l(x)$ is irreducible in $F[x]$.*

The contrapositive of this theorem is rather interesting: If $f(x) \in F[x]$ is reducible, then $f(x)$ is also reducible in $R[x]$!

[3] Note that we regard $R \subseteq F$ as a subring of F, as per usual.

Proof

Let $l(x) \in R[x]$ be irreducible. Suppose $l(x) = g(x)h(x) \in F[x]$ for some $g(x), h(x) \in F[x]$. If a and b [4] *are the products of the denominators of the coefficients of $g(x)$ and $h(x)$, respectively, then*

[4] They are both in F.

$$\left.\begin{aligned} g_1(x) &= ag(x) \\ h_1(x) &= bh(x) \end{aligned}\right\} \in R[x].$$

Then $abl(x) = g_1(x)h_1(x)$ is a factorization in $R[x]$. Since $l(x)$ is irreducible in $R[x]$, we have that $\mathrm{c}(l) \sim 1$ by Lemma 105. Then by Theorem 106, we have

$$ab \sim ab\,\mathrm{c}(l) \sim \mathrm{c}(abl) \sim \mathrm{c}(g_1 h_1) \sim \mathrm{c}(g_1)\,\mathrm{c}(h_1). \tag{34.1}$$

By Lemma 104, write

$$\begin{aligned} g_1(x) &= \mathrm{c}(g_1)g_2(x) \\ h_1(x) &= \mathrm{c}(h_1)h_2(x) \end{aligned}$$

where $g_2(x), h_2(x) \in R[x]$ are primitive. Then we have

$$abl(x) = g_1(x)h_1(x) = \mathrm{c}(g_1)\,\mathrm{c}(h_1)g_2(x)h_2(x).$$

Then by Equation (34.1), we have

$$l(x) \sim g_2(x)h_2(x).$$

Since $l(x)$ is irreducible in $R[x]$, it follows, WLOG, that $g_2(x) \sim 1$, which then

$$ag(x) = g_1(x) = \mathrm{c}(g_1)g_2(x) = \mathrm{c}(g_1)v$$

for some unit $v \in R$. And so

$$g(x) = a^{-1}\,\mathrm{c}(g_1)v$$

is also a unit. Therefore, we have that

$$l(x) = g(x)h(x) \in F[x]$$

implies that either $g(x)$ or $h(x)$ is a unit, i.e. $l(x)$ is irreducible in $F[x]$. □

35 Lecture 35 Jul 25th 2018

35.1 Factorizations in Integral Domains (Continued 5)

35.1.1 Gauss' Lemma (Continued 2)

We have shown in Example 33.1.1 that $\mathbb{Z}[x]$ is not a PID. Our goal now is the show that, in spite of that, $\mathbb{Z}[x]$ is a UFD.

Note

Recall the following results from the recent lectures: Let R be a UFD with F being its field of fractions. We have

- $l(x) \in R[x]$ *is irreducible* $\implies \mathrm{c}(l) \sim 1$ *(Lemma 105);*
- $\mathrm{c}(fg) \sim \mathrm{c}(f)\,\mathrm{c}(g)$ *(Lemma 104);*
- $l(x)$ *is irreducible in* $R[x] \implies l(x)$ *is irreducible in* $F[x]$ *(Theorem 107).*

Note

Recall that the contrapositive of Theorem 107 is: if $l(x)$ is reducible in $F[x]$, then $l(x)$ is reducible in $R[x]$.

In other words, for $f(x) \in R[x]$, if $f(x) = g(x)h(x) \in F[x]$, then $\exists \tilde{g}(x), \tilde{h}(x) \in R[x]$ such that

$$f(x) = \tilde{g}(x)\tilde{h}(x) \in R[x].$$

Example 35.1.1

$2x^2 + 7x + 3 \in \mathbb{Z}[x]$, *which we observe that*

$$\begin{aligned} 2x^2 + 7x + 3 &= \left(x + \frac{1}{2} \right)(2x + 6) \\ &= (2x+1)(x+3). \end{aligned}$$

We want to take advantage of the fact that $\mathbb{Q}[x]$ is a UFD to show that $\mathbb{Z}[x]$ is also a UFD.

Recall from Example 34.1.1 that $2x + 4 \in \mathbb{Q}[x]$ is irreducible, but is reducible in $\mathbb{Z}[x]$. Therefore, we have that the converse of Theorem 107 is not true.

Proposition 108

Let R be a UFD with field of fractions F. TFAE:

1. *$f(x)$ is irreducible in $R[x]$;*
2. *$f(x)$ is primitive and irreducible in $F[x]$.*

Proof

$(1) \implies (2)$ *follows from Lemma 105, Theorem 106 and Theorem 107.*

$(2) \implies (1)$*: Suppose that $f(x)$ is primitive and irreducibile in $F[x]$ but reducible in $R[x]$. Then a non-trivial factorization of $f(x) \in R[x]$ must take the form $f(x) = dg(x)$ with $d \in R$ and $d \not\sim 1$* [1]*. Since $d \mid f(x)$, $d \not\sim 1$ must then divide each of the coefficients of $f(x)$, which contradicts the assumption that $f(x)$ is primitive.* $\square$

[1] Note that we cannot have both factors to have degree ≥ 1, otherwise this would be a non-trivial factorization in $F[x]$, contradicting the irreducibility of $f(x)$ in $F[x]$.

Theorem 109 (Polynomial Ring of a UFD is also a UFD)

If R is a UFD, then the polynomial ring $R[x]$ is also a UFD.

Proof

By Theorem 95, since R is a UFD and hence satisfies ACCP [2]*, we have $R[x]$ also satisfies ACCP. Then by Theorem 98, to complete the*

[2] See note on page 192.

proof, it suffices to show that every irreducible element $l(x) \in R[x]$ *is prime. To show that an irreducible element* $l(x) \in R[x]$ *is prime, we need to show that if* $l(x) \mid f(x)g(x)$ *in* $R[x]$*, then* $l(x) \mid f(x)$ *or* $l(x) \mid g(x)$*.*

36 Index

37 List of Symbols

$M_n(\mathbb{R})$	set of $n \times n$ matrices over $\mathbb{R}$
$\mathbb{Z}_n^*$	set of integers modulo n; each element has its multiplicative inverse
S_n	symmetry group of degree n
D_{2n}	dihedral group of degree n; a subset of S_n
K_n	Klein n-group
A_n	alternating group of degree n; a subset of S_n
$F[x]$	polynomial ring over a field F
$\|D_{2n}\|$	order of the dihedral group; the size of the dihedral group
$\begin{pmatrix}1 & 2 & \dots & n\end{pmatrix}$	An n-cycle
$\det A$	determinant of matrix A
$GL_n(\mathbb{R})$	general linear group of degree n; the set that contains elements of $M_n(\mathbb{R})$ with non-zero determinant
$SL_n(\mathbb{R})$	special linear group of order n; the set that contains elements of $GL_n(\mathbb{R})$ with determinant of 1
$Z(G)$	center of group G
$\langle g \rangle$	cyclic group with generator g; principal ideal with generator g
$\langle h(x) \rangle$	principal ideal with generator $h(x) \in F[x]$
$n \mid d$	n divides d
$H \leq G$	H is a subgroup of G (used sparsely in this notebook)
$H \triangleleft G$	H is a normal subgroup of G
G/H	quotient group of G by $H \triangleleft G$
$\ker \alpha$	kernel of α
$\operatorname{im} \alpha$	image of α
$G^{(m)}$	group of elements of G with order m
$\operatorname{ch}(R)$	characteristic of the ring R
$\gcd(a, b)$	the greatest common divisor of a and b
$\mathrm{c}(f)$	the content of the polynomial $f(x)$