

gmail : ernestyalumni  
linkedin : ernestyalumni  
twitter : ernestyalumni  
wordpress.com: ernestyalumni

These notes are open-source, governed by the Creative Common license. Use of these notes is governed by the Caltech Honor Code: “No member of the Caltech community shall take unfair advantage of any other member of the Caltech community.”

CONTENTS

1. Things Past	1
2. Groups I	3
3. Commutative Rings I	8
4. Fields	14
5. Groups II	14
6. Commutative Rings II	15
7. Modules and Categories	15
8. Algebras	19
9. Advanced Linear Algebra	20
10. Homology	20
11. Commutative Rings III	20
References	21

1. THINGS PAST

1.1. Some Number Theory.

$$\mathbb{N} = \{n | n \in \mathbb{Z}, n \geq 0\}$$

**Definition 1.**  $p \in \mathbb{N}$ , prime if  $p \geq 2$ , and  $\nexists$  factorization  $p = ab$  where  $a < p, b < p, a, b \in \mathbb{N}$

*Date:* inverno 2012.

**Axiom 1. *Least Integer Axiom***  $\exists$  *smallest integer in every*  $C \subset \mathbb{N}, C \neq \emptyset$

**Theorem 1 (1.2).** (*Mathematical Induction*). *Let  $S(n)$  family of statements,  $\forall n \in \mathbb{Z}, n \geq m$ , where  $m$  some fixed integer. If*

- (i)  $S(m)$  *true*
- (ii)  $S(n)$  *true implies*  $S(n + 1)$  *true*

then  $S(n)$  true  $\forall n \in \mathbb{Z}, n \geq m$

*Proof.* Let  $C$  be set of all integers  $n \geq m$  for which  $S(n)$  false.  
If  $C = \emptyset$  done.  
Otherwise,  $\exists$  smallest integer  $k$  in  $C$ .

By (i),  $k > m$   
But statement  $S(k - 1)$  (EY !!!)  $S(k - 1)$  true.  
But by (ii),  $S(k)$  true.  
Contradiction that  $k \in C$

**Theorem 2** (1.3). (*Second Form of Induction*). Let  $S(n)$  family of statements,  $\forall n \in \mathbb{Z}, n \geq m$ , where  $m$  some fixed integer.  
If

- (i)  $S(m)$  true
- (ii) if  $S(k)$  true  $\forall k$  with  $m \leq k < n$ , then  $S(n)$  itself true

then  $S(n)$  true  $\forall n \in \mathbb{Z}, n \geq m$

*Proof.* Let  $C$  be set of all integers  $n \geq m$  for which  $S(n)$  false.  
If  $C = \emptyset$  done.  
Otherwise,  $\exists$  smallest integer  $j$  in  $C$ .

By (i),  $j > m$   
Then  $S(j - 1)$  true,  $S(j - 2)$  true,  $\dots$   $S(m + 1)$  true, otherwise contradiction.  
By (ii),  $S(j)$  true. Contradiction.

**Theorem 3** (1.4). (*Division Algorithm*)  $\forall a, b \in \mathbb{Z}, a \neq 0, \exists !q, r \in \mathbb{Z}$  s.t.

$$b = qa + r \text{ and } 0 \leq r < |a|$$

*Proof.* Consider  $n \in \mathbb{Z}, b - na \in \mathbb{Z}$   
Let  $C = \{b - na | n \in \mathbb{Z}\} \cap \mathbb{N}$ .  
 $C \neq \emptyset$  (otherwise, consider  $b - na < 0, b < na$ , then contradiction)  
By Least Integer Axiom,  $\exists$  smallest  $r \in C, r = b - na$ .  
define  $q = n$  when  $r = b - na$ .

Suppose  $qa + r = q'a + r'$   
 $(q - q')a = r' - r$ ,  $0 \leq r' < |a|$ . Now  $0 \leq |r' - r| < |a|$   
 $|(q - q')a| = |r' - r|$   
if  $|q - q'| \neq 0, |(q - q')a| \geq |a|$   
 $\implies q = q', r = r'$

Conclude both sides are 0

**Definition 2.**  $a, b \in \mathbb{Z}$ ,  $a$  **divisor** of  $b$  if  $\exists d \in \mathbb{Z}$  s.t.  $b = ad$ .  
 $a$  **divides**  $b$  or  $b$  multiple of  $a$ , denote

$$a|b$$

$a|b$  iff  $b$  has remainder  $r = 0$  after dividing by  $a$

**Theorem 4** (1.14). (*Euclidean Algorithm*) Let  $a, b \in \mathbb{Z}^+$   
 $\exists$  algorithm finds gcd,  $d = (a, b)$  and finds  $s, t \in \mathbb{Z}$  with  $d = sa + tb$

$\square$  *Proof.*  $b = qa + r$  where  $0 \leq r < a$   
 $a = q'r + r'$  where  $0 \leq r' < r$   
 $r = q''r' + r''$  where  $0 \leq r'' < r'$

$\square$

**Lemma 1** (1.53). If  $\sim$  equivalence relation on set  $X$ , then  $x \sim y$  iff  $[x] = [y]$

*Proof.* If  $x \sim y$ , then if  $z \in [x], z \sim x$ , and so  $z \sim y$ , so  $[x] \subseteq [y]$ . Likewise (by label symmetry),  $[y] \subseteq [x] \implies [y] = [x]$ .  
If  $[x] = [y]$ , then  $x \in [x]$ , by reflexivity,  $x \sim x$ .  $x \in [x] = [y]$ . So  $x \sim y$

$\square$

**Proposition 1** (1.54). If  $\sim$  equivalence relation on set  $X$ , then equivalence classes form a partition.  
If given partition  $\{A_i | i \in I\}$  of  $X$ ,  $\exists$  equivalence relation  $\sim$  on  $X$  s.t. equivalence classes are the  $A_i$ .

*Proof.* Assume equivalence relation  $\sim$  on  $X$ .  
 $\forall x \in X, x \in [x]$ , since  $x$  reflexive ( $x \sim x$ ), so  $[x] \subseteq X, [x] \neq \emptyset$  and  $\bigcup_{x \in X} [x] = X$ .

$\square$

Suppose  $a \in [x] \cap [y]$ , so  $a \sim x$ . Then  $x \sim y$ . By Lemma 1.53, ( $x \sim y$  iff  $[x] = [y]$ ), then  $[x] = [y]$ . So  $\{[x]\}$  partition  $X$ .  
 $a \sim y$

If  $\{A_i | i \in I\}$  partition of  $X$ .

If  $x, y \in X$ , define  $x \sim y$  if  $\exists i \in I$  s.t.  $x \in A_i, y \in A_i$ .  $x \sim y$  is clearly reflexive and symmetric.  
 $y \in A_i$

Suppose  $x \sim y, y \sim z$ , so  $\exists i, j \in I$ , s.t.  $x, y \in A_i, y, z \in A_j$ . Since  $y \in A_i \cap A_j$ , so  $i = j$  (since  $A_i, A_j$  pairwise disjoint by definition of partition).

So  $x \sim z$  since  $x, z \in A_i$   
If  $x \in X$ , then  $x \in A_i$ , for some  $i$ .  
If  $y \in A_i$ , then  $y \sim x$ , and  $y \in [x]$ , so  $A_i \subseteq [x]$   
Let  $z \in [x]$ , so  $z \sim x$ . Then  $\exists j$  s.t.  $x \in A_j$  and  $z \in A_j$ , then  $x \in A_j \cap A_i \implies i = j$  by pairwise disjointness, so  $z \in A_i$ , so  $[x] \subseteq A_i$ .  
 $\implies [x] = A_i$   
 $\square$

Exercises. **Exercise 1.1.** First, knowing that the law of exponents works for real (complex) numbers (if you really want to, look into Apostol’s Calculus Volume 1

$$\frac{1}{6}n(n+1)(2n+1) = \frac{1}{6}n(2n^2+3n+1) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{n}{6}$$

Now I think the point of this exercise and exercises 1.2, 1.3 is to apply what one learns about proving things by induction in the corresponding section.

$n = 1.$   $1 = \frac{1}{6}1(2)(3)$

Assume  $n$ th case.

$$\begin{aligned} \frac{1}{6}(n+1)(n+2)(2(n+1)+1) &= \frac{1}{6}(n+1)(n+2)(2n+1+2) = \frac{1}{6}n(n+1)(2n+1+2) + \frac{1}{3}(n+1)(2n+1+2) = \\ &= 1^2 + \cdots + n^2 + \frac{1}{3}n(n+1) + \frac{1}{3}(n+1)(2n+3) = 1^2 + \cdots + n^2 + (n+1)^2 \end{aligned}$$

**Exercise 1.11.** Let  $p_1, p_2, \dots$  be list of primes in ascending order:  $p_1 = 2, p_2 = 3, p_3 = 5 \dots$

cf.

**Exercise 1.68.** Let  $f : X \rightarrow Y$   
 $V, W \subseteq Y$

(i)  $f^{-1}(VW) = f^{-1}(V)f^{-1}(W).$   $f^{-1}(V \bigcup W) = f^{-1}(V) \bigcup f^{-1}(W)$

Suppose  $x \in f^{-1}(VW).$

Then  $f(x) \in VW.$  Then  $f(x) \in V$  and  $f(x) \in W.$  Then  $x \in f^{-1}(V)$  and  $x \in f^{-1}(W).$   $x \in f^{-1}(V)f^{-1}(W).$

if  $x \in f^{-1}(V)f^{-1}(W)$  then  $x \in f^{-1}(V)$  and  $x \in f^{-1}(W).$  Then  $f(x) \in V$  and  $f(x) \in W.$  So  $f(x) \in VW,$  with  $f(x)$  in it  $(VW).$

Then  $x \in f^{-1}(VW).$

$f^{-1}(VW) = f^{-1}(V)f^{-1}(W)$

Suppose  $x \in f^{-1}(V \bigcup W).$  Then  $f(x) \in V \bigcup W.$  Then  $f(x) \in V$  or  $f(x) \in W.$  Then  $x \in f^{-1}(V)$  or  $x \in f^{-1}(W).$  Then  $x \in f^{-1}(V) \bigcup f^{-1}(W).$

Suppose  $x \in f^{-1}(V) \bigcup f^{-1}(W).$  Then  $x \in f^{-1}(V)$  or  $x \in f^{-1}(W).$  Then  $f(x) \in V$  or  $f(x) \in W.$   $f(x) \in V \bigcup W.$  So  $x \in f^{-1}(V \bigcup W).$

## 2. GROUPS I

### 2.1. Introduction.

### 2.2. Permutations.

**Definition 3.** permutation of set  $X$  is a bijection from  $X$  to  $X$  (itself)

**Definition 4.**  $S_X$  = family of all permutations of set  $X$ , **symmetric group** on  $X$   
When  $X = \{1 \dots n\}, S_X \equiv S_n$  symmetric group of  $n$  letters

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & j & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(j) & \dots & \alpha(n) \end{pmatrix}$$

**Definition 5.** Let  $i_1 \dots i_r$  distinct integers in  $\{1 \dots n\}$

If  $\alpha \in S_n$

$$\alpha(i_1) = i_2 \dots \alpha(i_r) = i_1$$

$\alpha$   $r$ -cycle

$$\alpha = (i_1 \quad i_2 \quad \dots \quad i_r)$$

```
sage: S_3 = SymmetricGroup(3)
sage: for perm in S_3.list():
....:     print perm.tuple()
....:
(1, 2, 3)
(2, 1, 3)
(2, 3, 1)
(3, 1, 2)
(1, 3, 2)
(3, 2, 1)
```

```
sage: S_9 = SymmetricGroup(9)
sage: S_9([6,4,7,2,5,1,8,9,3])
(1,6)(2,4)(3,7,8,9)
sage: alpha = S_9([6,4,7,2,5,1,8,9,3])
sage: alpha
(1,6)(2,4)(3,7,8,9)
sage: alpha.tuple()
(6, 4, 7, 2, 5, 1, 8, 9, 3)
```

Notice that while Rotman [1] defines that “we multiply permutations from right to left, because multiplication here is composite of functions; that is, to evaluate  $\alpha\beta(1)$ , we compute  $\alpha(\beta(1))$ ”, in Sage Math, it’s the other way. This makes sense because in math, we think in terms of operations acting from the left, while in Sage Math, based on Python, function call are chained together from left to right.

So Rotman has

$$\sigma = (12)(13425)(2513)$$

while

```
sage: S_5 = SymmetricGroup(5)
sage: S_5((1,2))
(1,2)
sage: S_5((2,5,1,3))*S_5((1,3,4,2,5))*S_5((1,2))
(1,4)(3,5)
sage: sigma = S_5((2,5,1,3))*S_5((1,3,4,2,5))*S_5((1,2))
sage: sigma.tuple()
(4, 2, 5, 1, 3)
```

whereas, if we did this, we’d get something different than desired:

```
sage: S_5((1,2))*S_5((1,3,4,2,5))*S_5((2,5,1,3))
(3,4,5)
sage: (S_5((1,2))*S_5((1,3,4,2,5))*S_5((2,5,1,3))).tuple()
(1, 2, 4, 5, 3)
```

2.3. Groups.

**Definition 6.** group  $G$  is a set equipped with binary operation  $*$  s.t.

- (1) associative  $\forall x, y, z \in G, x * (y * z) = (x * y) * z$
- (2)  $\exists e \in G$ , called identity, with  $e * x = x * e \quad \forall x \in G$
- (3)  $\forall x \in G, \exists$  inverse  $x^{-1} \in G$  s.t.  $x * x^{-1} = e = x^{-1} * x$

**Definition 7.**  $G$  abelian if commutativity  $x * y = y * x \quad \forall x, y \in G$

**Definition 8.** Let  $G$  group, let  $a \in G$ ,  
If  $a^k = 1$ , for some  $k \geq 1$ , then the smallest such exponent  $k \geq 1$  is order of  $a$ .  
If  $\nexists k, a$  has infinite order

**Proposition 2** (2.27). If  $G$  finite group,  $\forall x \in G$  has finite order

*Proof.* cf. Example 2.26

If  $G$  finite group,  $a \in G$ ,  
Consider subset  $\{1, a, a^2 \dots a^n \dots\}$   
Since  $G$  finite,  $\exists m, n \in \mathbb{Z}, m > n$  s.t.  $a^m = a^n$  (i.e. there must be repetition)

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

Thus, if  $G$  finite group,  $a \in G, \exists k \geq 1$  s.t.  $a^k = 1$

*Exercises.* **Exercise 2.17.**  $a_2^{-1} a_1^{-1} a_1 a_2 = e$

Assume  $n - 1$  case.

$$a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1} a_1 a_2 \dots a_{n-1} a_n = a_n^{-1} e a_n = e$$

**Exercise 2.27 .**

cf. <http://math.stanford.edu/~akshay/math109/hw2.pdf>

Let  $S$  = elements of  $G$  of order greater than 2.  
Note, only 1 has order 1, and  $a \in G$  has order 2 only if  $a = a^{-1}$ , then

$$S = \{a|a \in G, a^2 \neq 1\}$$

if  $s \in S, \quad s^{-1} \neq s$   
so

$$S = \bigcup_{s \in S} \{s, s^{-1}\}$$

Note that  $\forall \{s, s^{-1}\}, \quad s \neq s^{-1}$  (distinct)  
Since  $s^{-1}$  unique ( $s^{-1}s = bs = 1, \quad s^{-1} = b$ ), then for  $\{x_1, x_1^{-1}\}, \{x_2, x_2^{-1}\} \subset S$ ,

$x_1, x_2$  equal or distinct.  
Thus  $|S|$  even (number of elements in  $S$ , or “order”, is even).

$1 \in G, S \subset G. \implies \exists a \in G$ , s.t.  $a^2 = 1$ . At least 1  $a$  must exists.  
There can be an odd number of  $a$ ’s.  
Precisely, let  $T = \{a|a \in G, a^2 = 1\}, |T| = k$  (number of elements in  $T$ )  
 $G = T \coprod S \coprod \{e\}, \quad |G| = k + 2m + 1 = 2n. \quad k = 2(n - m) - 1$ , so  $k$  odd.

**2.4. Lagrange’s Thm.** Example 2.29  $A_n \leq S_n, |A_n| = n!/2$ , and  $A_n$  consists of all even permutations (sign +1).

```
sage: A_3 = AlternatingGroup(3)
sage: A_3.cardinality()
3
sage: for a in A_3.list(): print a.tuple()
(1, 2, 3)
(2, 3, 1)
(3, 1, 2)
sage: for a in A_3.list(): print a.sign()
1
1
1
```

Easy to prove a subset is a subgroup with this:

**Proposition 3** (2.30).  $H \subseteq G$  subgroup iff  $H \neq 0$  and  $\forall x, y \in H$ , then  $xy^{-1} \in H$

*Proof.* If  $H$  subgroup,  $xy^{-1} \in H$  since  $y^{-1} \in H$  (by def.) and  $1 \in H$ , so  $H \neq 0$ .  
If  $H \neq 0$ , and  $\forall x, y \in H$ , then  $xy^{-1} \in H$ , then  $yy^{-1} = 1 \in H, 1y^{-1} = y^{-1} \in H, \quad \forall y \in H$ ,  
If  $x, y \in H, y^{-1} \in H$ , so  $xy = x(y^{-1})^{-1} \in H$

**cyclic subgroup, generator** of  $G$

e.g.

```
sage: S_3.list()[1]
(1,2)
sage: S_3.subgroup( S_3.list()[1] ).list()
[(), (1,2)]
```

**Definition 9.**  $H$  subgroup of  $G$ , coset  $aH = \{ah|h \in H\}$ . left cosets.  
 $Ha = \{ha|h \in H\}$  right cosets.

Example 2.39

- (i)
- (ii)
- (iii) 

```
sage: H = S_3.subgroup( S_3.list()[1] )
sage: H
Subgroup of (Symmetric group of order 3! as a permutation group) generated by [(1,2)]
sage: H.list()
[(), (1,2)]
```

“Notice that now Sages results will be backwards compared with the text.” [2]

```
sage: H = S_3.subgroup( S_3.list()[1] )

sage: S_3.cosets(H,side='right')
[((), (1,2)], [(2,3), (1,3,2)], [(1,2,3), (1,3)]]

[((), (1,2)], [(2,3), (1,2,3)], [(1,3,2), (1,3)]]
sage: S_3.cosets(H,side='left')[1][1].tuple()
```

**Lemma 2** (2.40). *Let  $H \leq G$ ,  $\forall a, b \in G$*

- (i)  $aH = bH$  iff  $b^{-1}a \in H$  ; in particular  $aH = H$  iff  $a \in H$
- (ii) if  $aH \cap bH \neq \emptyset$ ,  $aH = bH$
- (iii)  $|aH| = |H| \quad \forall a \in G$

*Proof.* (i) If  $b^{-1}a \in H$ , consider  $x \in aH$ . Consider  $bh'$  where  $h' = b^{-1}ah \in H$ , since  $H$  closed.  $bh' \in bH$  and  $x = ah = bh'$ . So  $x \in bH$ .

Consider  $x \in bH$ .  $x = bh$  for some  $h \in H$ .  $b^{-1}a \in H$ , so  $a^{-1}b = (b^{-1}a)^{-1} \in H$ , since  $H$  is a subgroup with inverses. Consider  $ah' \in aH$ , where  $h' = a^{-1}bh$ . Then

$$x = bh = ah' \in aH \text{ so } bH \subseteq aH$$

$\implies bH = aH$ .

If  $aH = bH$ , the  $\forall x \in aH$ ,  $x = ah$  for some  $h \in H$  and  $x = bh'$  for some  $h' \in H$ .  $b^{-1}ah = h'$  or  $b^{-1}a = h'h^{-1}$  since  $H$  closed,  $h'h^{-1} \in H$ , so  $b^{-1}a \in H$

- (ii)  $\forall a, b \in G$ , suppose  $a \sim b$ , if  $b^{-1}a \in H$ . Then  $aH = bH$  from above.

$a \sim a$  means  $a^{-1}a = 1 \in H$  (since  $H \leq G$ )

$b \sim a$  means  $a^{-1}b \in H$  since  $(b^{-1}a)^{-1} = a^{-1}b \in H$

If  $b \sim c$  as well, so  $c^{-1}b \in H$ ,  $c^{-1}b(b^{-1}a) = c^{-1}a \in H$ . So  $a \sim c$ .

Thus  $\sim$  is an equivalence relation. Then  $[a]$  form a partition of  $G$ .  $[a]$  happens to be  $aH$  (indeed,  $1 \in H$ , so  $a \in aH$ ).

By def. of partition, if  $aH \cap bH \neq \emptyset$ , then  $aH = bH$ .

- (iii) Consider  $H \rightarrow aH$ , since  $a^{-1} \in G$ , then mapping is injective.

$$h \mapsto ah$$

$\forall x \in aH$ ,  $x = ah'$  for some  $h' \in H$ . Then  $h' \mapsto ah' = x$ . It's surjective.

Then  $\exists$  isomorphism (bijective mapping) between  $H$  and  $aH$ .  $\implies |H| = |aH|$

EY : 20150917: If  $H \leq G$ , cosets of  $H$  in  $G$  form a partition of  $G$ .

**Theorem 5** (2.41). (Lagrange's Thm.) If  $H \leq G$ , then  $|H|$  is a divisor of  $|G|$

*Proof.* Let  $\{a_1H, a_2H \dots a_tH\}$  be distinct cosets of  $H$  that partition  $G$ .

$$\implies G = \coprod_{i=1}^t a_iH$$

$$\implies |G| = \sum_{i=1}^t |a_iH| = \sum_{i=1}^t |H| = t|H| \implies \frac{|G|}{|H|} = t$$

**Exercise 2.29.**

- (i) If  $Ha = Hb$ ,

Then  $\exists h_1, h_2 \in H$  s.t.  $h_1a = h_2b$  since  $H$  subgroup.

$$ab^{-1} = h_2h_1^{-1} \in H$$

For  $h_1a \in Ha$ ,  $h_1a = h_1hb \in Hb$

For  $h_2b \in Hb$ ,  $h_2b = h_2h^{-1}a \in Ha$ .  $Ha = Hb$

Thus, for right cosets  $Ha, Hb$ ,

$$Ha = Hb \text{ iff } ab^{-1} \in H$$

- (ii)  $a \sim b$  if  $ab^{-1} \in H$

$a \sim a$  if  $aa^{-1} = e \in H$  since  $H$  subgroup.

If  $a \sim b$ ,  $(ab^{-1})^{-1} = ba^{-1} \in H$  since  $H$  subgroup, so  $b \sim a$ .

$ab^{-1}, bc^{-1} \in H$ .  $H$  subgroup, so  $ac^{-1} \in H$ . So  $a \sim c$ .  $a \sim b$  an equivalence relation.

For  $[a]$ , if  $a \sim b$ ,  $ab^{-1} \in H$  so  $Ha = Hb$ , so  $[a] = Ha$ , since  $ea = a$  and  $ha = b$ .

**Exercise 2.30.**

- (i) define **special linear group** by

$$\text{SL}(2, \mathbb{R}) = \{A \in \text{GL}(2, \mathbb{R}) | \det(A) = 1\}$$

$\text{GL}(2, \mathbb{R})$  is a group. Clearly,  $\text{SL}(2, \mathbb{R}) \subseteq \text{GL}(2, \mathbb{R})$ .

Use Prop. 2.30,  $H \subseteq G$  is a subgroup iff  $H \neq 0$  and  $\forall x, y \in H$ , then  $xy^{-1} \in H$ .

$1 \in \text{SL}(2, \mathbb{R})$ .  $\det 1 = 1$ . So  $\text{SL}(2, \mathbb{R}) \neq 0$  as well.

Let  $x, y \in \text{SL}(2, \mathbb{R})$ .  $xy^{-1} \in \text{GL}(2, \mathbb{R})$ , since  $\text{GL}(2, \mathbb{R})$  a group and  $x, y^{-1} \in \text{GL}(2, \mathbb{R})$ .  $\det(xy^{-1}) = \det x \det y^{-1} = 1$  since  $\det y = 1$ .

Then  $xy^{-1} \in \text{SL}(2, \mathbb{R}) \implies \text{SL}(2, \mathbb{R}) < \text{GL}(2, \mathbb{R})$ .

- (ii)  $1 \in \text{GL}(2, \mathbb{Q})$  since  $1 \in \mathbb{Q}$ . Also  $\text{GL}(2, \mathbb{Q}) \neq 0$ .

Let  $x, y \in \text{GL}(2, \mathbb{Q})$ .

Let  $y = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$   $y^{-1} = \frac{1}{eh-fg} \begin{bmatrix} h & -f \\ -g & e \end{bmatrix}$ .  $xy^{-1} \in \text{GL}(2, \mathbb{Q})$  as  $\forall$  entry is in  $\mathbb{Q}$ , since  $\mathbb{Q}$  closed under addition, multiplication,

and division, and  $\det(xy^{-1}) = \det x \det y^{-1} = \frac{\det x}{\det y} \neq 0$

**Exercise 2.37.** Consider  $\varphi : aH \mapsto Ha^{-1}$ .

EY:20150918 is it true that  $\varphi : 2^G \rightarrow 2^G$  ?

Consider right coset  $Ha$ .  $a^{-1} \in G$  since  $G$  group.  $a^{-1}H$  is a left coset.  $\varphi$  surjective,  $\varphi(a^{-1}H) = H(a^{-1})^{-1} = Ha$

Suppose  $\varphi(aH) = \varphi(bH) \implies Ha^{-1} = Hb^{-1}$ .  $a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$ , by Exercise 2.29 (right cosets  $Ha = Hb$  iff  $ab^{-1} \in H$ ).  $(a^{-1}b)^{-1} = b^{-1}a \in H$  then, since  $H \leq G$ .

Lemma 2, i.e. Lemma 2.40, says  $aH = bH$  iff  $b^{-1}a \in H$ , and so  $aH = bH$ .  $\varphi$  injective.

□ Thus there is a bijection between left cosets and right cosets. Then the number of left cosets is equal to the number of right cosets.

2.5. Homomorphisms.

**Proposition 4** (2.56). *Let  $f : G \rightarrow H$  homomorphism.*

- (i)  $\ker f$  subgroup of  $G$   
 $\operatorname{im} f$  subgroup of  $H$
- (ii) If  $x \in \ker f, \forall a \in G$

$$axa^{-1} \in \ker f$$

- (iii)  $f$  injection iff  $\ker f = 1$

*Proof.* (i) Let  $x, y \in \ker f$   $f(xy) = f(x)f(y) = 1 \cdot 1 = 1$   $xy \in \ker f$   
Let consider  $x^{-1}$ .  $f(x^{-1})f(x) = f(x^{-1}x) = 1 = 0$   
Consider 1.  $f(1) = 1$  since  $f(1) = f(1 \cdot 1) = f(1)f(1)$ , so  $f(1) = 1$   
 $f(x^{-1}x) = f(x^{-1})f(x) = 1$ , so  $(f(x))^{-1} = f(x^{-1})$

$$f(x)f(y) = f(xy) \in \operatorname{im} f$$

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

$$1 = f(1), \text{ since } 1f(x) = f(1)f(x) = f(x)$$

- (ii)

$$f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)1(f(a))^{-1} = 1$$

$$axa^{-1} \in \ker f$$

- (iii) If  $f$  injective, if  $f(x) = 1, x = 1$ , so  $\ker f = 1$   
If  $\ker f = 1$ , consider  $f(a) = f(b)$

$$f(a)f(b^{-1}) = f(ab^{-1}) = f(a)f(b^{-1}) = 1 \implies ab^{-1} = 1 \quad \boxed{a = b}$$

**Definition 10.** subgroup  $K$  of  $G$  **normal subgroup** if  $k \in K, g \in G, gkg^{-1} \in K$ .  $K \triangleleft G$ .

**Definition 11.** If  $a \in$  group  $G$ , conjugate of  $a = gag^{-1} \in G$

**Proposition 5** (2.56). *Let  $f : G \rightarrow H$  be a homomorphism.  $\ker f$  is a normal subgroup i.e. if  $x \in \ker f$  and if  $a \in G$ , then  $axa^{-1} \in \ker f$ .*

If  $G$  abelian, every subgroup is a normal subgroup.

$$h \in H \quad ghg^{-1} = gg^{-1}h = h \in H$$

cyclic subgroup  $H = \langle (1\ 2) \rangle$  of  $S_3$ ,  $H = \{(1), (1, 2)\}$  not normal subgroup.

(Trying stuff: 20130116)

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(1) & \alpha(2) & \alpha(3) \end{pmatrix} \quad \alpha(1\ 2)\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(1) & \alpha(2) & \alpha(3) \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \notin H$$

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

$$K = \langle (1\ 2\ 3) \rangle$$

**Proposition 6** (2.58). (i) conjugation  $\gamma_g : G \rightarrow G$  isomorphism  
(ii) conjugate elements have same order

*Proof.* (i)  $\gamma_g$  homomorphism since

$$\gamma_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \gamma_g(a)\gamma_g(b)$$

Now

$$\gamma_g\gamma_h(a) = \gamma_ghah^{-1} = ghah^{-1}g^{-1} = \gamma_{gh}a$$

so

$$\gamma_g\gamma_{g^{-1}}(a) = \gamma_e a = a = \gamma_{g^{-1}}\gamma_g a$$

so  $\gamma_g$  bijective.  $\gamma_g$  isomorphism

- (ii) conjugation is an isomorphism and preserves order of the each element, by Exercise 2.42.

□

Example 2.59.

Center of group  $G, Z(G)$

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

$Z(G)$  subgroup  $z^{-1}(zg)z^{-1} = z^{-1}gz z^{-1}$

$Z(G)$  normal subgroup  $gz^{-1} = z^{-1}g$

$$gzg^{-1} = zgg^{-1} = z \in Z(G)$$

2.5.1. Exercises. **Exercise 2.41.**  $G$  abelian.

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

$$f(aa^{-1}) = aa^{-1} = e = f(a^{-1})f(a) = f(a^{-1}a) = f(e)$$

so  $f$  homomorphism.

□

If  $f(a) = a^{-1}$ , homomorphism,

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

so  $ab = ba$

**Exercise 2.42.**

- (i) Let  $f : G \rightarrow H$  isomorphism.  
if  $a \in G$  has infinite order,  
Suppose  $f(a)$  finite order, i.e.  $\exists$  smallest  $k \in \mathbb{Z}$  s.t.  $f(a)^k = 1$   
 $f(a)^k = f(a^k) = 1$ .  $f$  isomorphism so  $a^k = 1$ . Contradiction.

so if  $a \in G$  has infinite order,  $f(a)$  has infinite order

If  $a$  has finite order  $n, f(a^n) = (f(a))^n = f(1) = 1$ .

$\implies$  if  $a$  has finite order  $n, f(a)$  has finite order  $n$ .

if  $G$  has element  $a$  of some order  $n$ , suppose  $f$  isomorphism.  
 $f(a)^n = 1$ , i.e.  $f(a)$  order of  $n$ .  $f(a) \in H$   
Contradiction.

if  $a \in G, a^n = 1$ , and  $\nexists h \in H$  s.t.  $h^n = 1$ , then  $G \not\cong H$

- (ii) EY 20131227

**Exercise 2.46.** Consider  $\left\{\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{R})\right\}$

$$\begin{bmatrix} a & b \\ 1 & 1 \end{bmatrix} \begin{bmatrix} c & d \\ & 1 \end{bmatrix} = \begin{bmatrix} ac & ad + b \\ & 1 \end{bmatrix}$$

$$\begin{bmatrix} \frac{1}{a} & \frac{-b}{a} \\ & 1 \end{bmatrix} \begin{bmatrix} a & b \\ & 1 \end{bmatrix} = 1$$

$$\begin{bmatrix} a & b \\ & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{a} & \frac{-b}{a} \\ & 1 \end{bmatrix} = 1$$

Matrices are associative and  $1 = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$  is identity to any  $GL(2, \mathbb{R})$  matrix.

By identifying entries  $a, b$  to  $f(x) = ax + b$  and vice versa,  $G = \{f : \mathbb{R} \rightarrow \mathbb{R} | f(x) = ax + b, a \neq 0\}$  clearly isomorphic to  $\left\{\begin{bmatrix} a & b \\ c & 1 \end{bmatrix}\right.$

So  $G$  also a group. Note,

$$fg(x) = a(cx + d) + b = acx + ad + b$$

### 2.6. Quotient Groups.

**Lemma 3** (2.65). *normal subgroup  $K$  iff s.t.  $gK = Kg \quad \forall g \in G$*

*Proof.* Suppose  $K$  normal subgroup (if  $k \in K, \forall g, gkg^{-1} \in K$ )

$$gK = g(g^{-1}kg) = kg \text{ so } gK \subset Kg$$

$$kg = (gkg^{-1})g = gk \text{ so } Kg \subset gK$$

$$gK = Kg$$

Suppose  $gK = Kg. \forall g \in G$

$$gkg^{-1} = kgg^{-1} = k \in K$$

So  $K$  normal subgroup (i.e.  $K \triangleleft G$ )

**Theorem 6** (2.67). *Let  $G/K = \{gK | g \in G, K \text{ subgroup}\}$ , set of all left cosets of subgroup  $K$ . if  $K$  normal subgroup,  $G/K$  group under  $aKbK = (ab)K$  operation*

*Proof.* If  $K$  normal subgroup,

$$(aK)(bK) = a(Kb)K = abKK = abK$$

so product of 2 cosets of  $K$  operation well-defined.

cosets of  $K$  are associative.  $K$  associative.

identity:  $K = 1K. (1K)(bK) = bK = (bK)(1K)$

inverse:  $a^{-1}K. (a^{-1}K)(aK) = 1K = (aK)(a^{-1}K)$   $G/K$  group.

**Corollary 1** (2.69).  $\forall$  normal subgroup  $K \triangleleft G, K = \ker f, f$  some homomorphism.

*Proof.* Define **natural map**  $\pi : G \rightarrow G/K$

$$\pi(a) = aK$$

$$aKbK = abK = \pi(a)\pi(b) = \pi(ab) \quad \text{so } \pi \text{ surjective homomorphism}$$

$K$  identity element in  $G/K$

$$\ker \pi = \{a \in G | \pi(a) = K\} = \{a \in G | aK = K\} = K$$

By Lemma 2.40(i)

□

**Theorem 7** (2.70). *(First Isomorphism Thm.) If  $f : G \rightarrow H$  homomorphism,*

*then  $\ker f \triangleleft G$*

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

*i.e. if  $\ker f = K, \quad \varphi : G/K \rightarrow \operatorname{im} f \leq H$ , then  $\varphi$  isomoprhism.*

$$aK \mapsto f(a)$$

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow \pi & \nearrow \varphi & \\ G/K & & \end{array}$$

$$\varphi\pi = f$$

*Proof.* By Prop. 2.56(ii),  $K = \ker f$  normal subgroup of  $G$

if  $aK = bK$ , then  $a = bk$  for some  $k \in K$ , so

$$\varphi(ak) = f(a) = f(bk) = f(b)f(k) = f(b)1 = f(b) = \varphi(bK), \quad \text{since } k \in K = \ker f \text{ } (f(k) = 1)$$

□  $\varphi$  well-defined

$$\varphi(aKbK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK)$$

$\varphi$  homomorphism.

$\operatorname{im} \varphi \leq \operatorname{im} f$  clearly.

Let  $y \in \operatorname{im} f. y = f(a)$ , some  $a \in G \quad y = f(a) = \varphi(aK) \quad \operatorname{im} f \leq \operatorname{im} \varphi$

$\varphi$  surjective onto  $\operatorname{im} f$

If  $\varphi(aK) = \varphi(bK), f(a) = f(b)$

□

$$1 = f(b)^{-1}f(a) \stackrel{f \text{ homomorphism}}{=} f(b^{-1})f(a) = f(b^{-1}a)$$

$$b^{-1}a \in \ker f = K$$

$$b^{-1}aK = K \quad aK = bK \text{ so } \varphi \text{ injective}$$

So  $\varphi$  isomorphism,  $G/\ker f \simeq \text{im} f$

Example 2.7.1. Let  $G = \langle a \rangle$  cyclic group of order  $m$

Define  $f : \mathbb{Z} \rightarrow G$   
 $f(n) = a^n \quad \forall n \in \mathbb{Z}$

$f$  homomorphism.

$f$  surjective (because a generator of  $G$ )

$$\ker f = \{n \in \mathbb{Z} | a^n = 1\} = \langle m \rangle \quad (\text{Thm. 2.24})$$

1st. isomorphism Thm.  $\implies \mathbb{Z}/\langle m \rangle \simeq G$

every cyclic group of order  $m$  is isomorphic to  $\mathbb{Z}/\langle m \rangle$

Example 2.72.  $\mathbb{R}/\mathbb{Z}$

define  $f : \mathbb{R} \rightarrow S^1$   
 $x \mapsto e^{2\pi i x}$

$f$  homomorphism:  $f(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x} e^{2\pi i y} = f(x)f(y)$

$f$  surjective.

$\ker f = \mathbb{Z}$

$\mathbb{R}/\mathbb{Z} \cong S^1$

**Theorem 8** (2.7.4). (*second Isomorphism Thm.*) If  $H, K$  subgroups of  $G$ ,  $H \triangleleft G$ , then  $HK$  subgroup,  $H \cap K \triangleleft K$

$$K/(H \cap K) \cong HK/H$$

*Proof.* Since  $H \triangleleft G$ , Prop. 2.66 shows  $HK$  subgroup.

2.7. **Group Actions.**

**Theorem 9** (2.87). (*Cayley*)  $\forall$  group  $G \simeq$  subgroup of symmetric group  $S_G$   
If  $|G| = n$ ,  $G \simeq$  isomorphic to subgroup  $S_n$

*Proof.*

**Theorem 10** (2.88). (*Representation on Cosets*) Let  $G, H$  subgroup of  $G$  having finite index  $n$ . Then  $\exists$  homomorphism  $\varphi : G \rightarrow S_n$  with  $\ker \varphi \leq H$

**Definition 12.** if set  $X$ , group  $G$ , then  $G$  acts on  $X$  if  $\exists$  function  $G \times X \rightarrow X$ , denoted  $(g, x) \mapsto gx$  s.t.

- (i)  $(gh)x = g(hx)$ ,  $\forall g, h \in G, x \in X$

- (ii)  $1x = x$ ,  $\forall X$

□

**Example 2.91**  $G$  acts on itself by conjugation: i.e.  $\forall g \in G$ , define  $\alpha_g : G \rightarrow G$  to be conjugation

$$\alpha_g(x) = gxg^{-1}$$

$X$  a  $G$ -set if  $G$  acts on  $X$ . If  $G$  acts on  $X$ ,  $x \in X$ , then **orbit** of  $x$ ,  $\mathcal{O}(x) = \{gx | g \in G\} \subseteq X$ .  
**stabilizer** of  $x$ ,  $G_x = \{g \in G | gx = x\} \leq G$

**Example 2.92**

- (i) By Cayley's Thm.,  $G$  acts on *itself* by translations:  $\tau_g : a \mapsto ga$  If  $a \in G$ , then  $\mathcal{O}(a) = G$ , for if  $b \in G$ ,  $b = (ba^{-1})a = \tau_{ba^{-1}}(a)$ .  
Stabilizer  $G_a$  of  $a \in G$  is  $\{1\}$  for if  $a = \tau_g(a) = ga$ , then  $g = 1$   
 $G$  acts *transitively* on  $X$  if  $\exists$  only 1 orbit

**Example 2.93**  $G$  acts on itself by conjugation.

$$\mathcal{O}(x) = \{y \in G | y = axa^{-1}, a \in G\} \equiv \text{conjugacy class of } x \equiv x^G$$

e.g. Thm. 2.9 shows if  $\alpha \in S_n$ , conjugacy class of  $\alpha$  consists of all permutations of  $S_n$  having same cycle structure as  $\alpha$ .  
 $z \in$  center  $Z(G)$  iff  $z^G = \{z\}$ , i.e. no other element in  $G$  conjugate to  $z$

If  $x \in G$ , stabilizer  $G_x$  of  $x$  is  $C_G(x) = \{g \in G | gxg^{-1} = x\}$   
centralizer of  $x$  in  $G$  is subgroup of  $G$  of all  $g \in G$  that commute with  $x$ .

**Example 2.94**  $\forall$  group  $G$  acts on set  $X$  of all its subgroups, by conjugation: if  $a \in G$ ,  $a$  acts on  $H \mapsto aHa^{-1}$ , where  $H \leq G$ .

conjugate of  $H$  is subgroup of  $G$ ,  $aHa^{-1} = \{aha^{-1} | h \in H, a \in G\}$   
 $H \rightarrow G$   
 $h \mapsto aha^{-1} \quad aha^{-1} = ah'a^{-1}$  so injection. conjugate subgroups of  $G$  are isomorphic.

orbit of subgroup  $H$  consists of all its conjugates  
 $\{\mathcal{O}(H)=\{H\}\}$  iff  $H \triangleleft G$  i.e.  $aHa^{-1} = H \quad \forall a \in G$

stabilizer of  $H$  is  $N_G(H) = \{g \in G | gHg^{-1} = H\}$  normalizer of  $H$  in  $G$

□

**Example 2.95**  $G = D_8$  Dihedral group

*Exercises.* **Exercise 2.100.** How many flags are there with  $n$  stripes each of which can be colored any one of  $q$  given colors?

**Hint** parity of  $n$  is relevant.

Parity of  $n$  matters, means if  $n = 2N$ ,  $N \in \mathbb{Z}$  or  $n = 2N + 1$ , matters, i.e.  $n$  even or  $n$  odd, respectively.

□

cf. <http://www.cs.virginia.edu/~krw7c/Burnsides.pdf>

3. COMMUTATIVE RINGS I

3.1. **Introduction.**



3.2. First Properties.

**Definition 13.** commutative ring  $R$  is a set with 2 binary operations, addition and multiplication, s.t.

- (i)  $R$  abelian group under addition
- (ii) (commutativity)  $ab = ba \quad \forall a, b \in R$  (this isn't there for noncommutativity)
- (iii) (associativity)  $a(bc) = (ab)c \quad \forall a, b, c \in R$
- (iv)  $\exists 1 \in R$  s.t.  $1a = a \quad \forall a \in R$  (many names used: one, unit, identity)
- (v) (distributivity)  $a(b + c) = ab + ac \quad a, b, c \in R$  (this splits up into 2 distributivity laws for noncommutativity)

To reiterate, abelian group under addition  $R$  (is defined as)

- (1) associative  $\forall x, y, z \in R, x + (y + z) = (x + y) + z$
- (2)  $\exists 0 \in R, 0 + x = x + 0, \quad \forall x \in R$
- (3)  $\forall x \in R, \exists (-x) \in R$  s.t.  $x + (-x) = 0 = (-x) + x$

abelian, if commutativity:  $x + y = y + x$ .

Example 3.1

- (i)  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  In Sage Math:

```
sage: ZZ
Integer Ring
sage: ZZ.is_commutative()
True
sage: QQ
Rational Field
sage: QQ.is_commutative()
True
sage: RR
Real Field with 53 bits of precision
sage: RR.is_commutative()
True
sage: CC
Complex Field with 53 bits of precision
sage: CC.is_commutative()
True
```

- (ii)  $\mathbb{I}_m \equiv \mathbb{Z}_m \equiv \mathbb{Z}/m\mathbb{Z}$  (many different notations used)

```
sage: Integers(5)
Ring of integers modulo 5
sage: Integers(5).is_commutative()
True
```

Integers(5) is  $\mathbb{Z}_5 \equiv \mathbb{Z}/5\mathbb{Z}$ .

- (iii) ring of **Gaussian integers**  $\mathbb{Z}[i] := \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}, i^2 = -1\}$

**Proposition 7** (3.2). (i)  $0 \cdot a = 0 \quad \forall a \in R$

- (ii) if  $1 = 0, R = \{0\}$ .  $R$  zero ring.

(iii)

(iv)

(v)

- (vi) binomial theorem holds: if  $a, b \in R$ , then

$$(a + b)^n = \sum_{r=0}^n \binom{n}{r} a^r b^{n-r}$$

*Proof.* (i) 0 is addition identity.  $0 + 0 = 0$

$$0 \cdot a + 0 \cdot a = (0 + 0)a = 0a$$

$$0 \cdot a + 0 \cdot a - 0 \cdot a = 0 \cdot a - 0 \cdot a = 0 = 0 \cdot a$$

(ii)

$$a = 1 \cdot a = 0 \cdot a = 0$$

**Definition 14.**  $S \subset R$  subring of  $R$  if

- (i)  $1 \in S$

- (ii)  $\forall a, b \in S$ , then  $a - b \in S$

- (iii)  $\forall a, b \in S$ , then  $ab \in S$

**Definition 15. domain** (often called integral domain) is a commutative ring  $R$  s.t.

$1 \neq 0$

$\forall a, b, c \in R$ , if  $ca = cb, c \neq 0$ , then  $a = b$

(EY: domain has  $1 \neq 0$  and cancellation)

**Proposition 8** (3.5). nonzero commutative ring  $R$  domain iff  $\forall a, b \in R, a, b \neq 0, ab \neq 0$

```
sage: QQ.is_integral_domain()
True
sage: ZZ.is_integral_domain()
True
sage: QQ.is_integral_domain()
True
sage: RR.is_integral_domain()
True
sage: CC.is_integral_domain()
True
sage: Integers(5).is_integral_domain()
True
sage: Integers(4).is_integral_domain()
False
```

*Proof.* if  $R$  domain, consider  $a, b \neq 0$ . Suppose  $ab = 0$ .  $ab = 0 = a0$  so  $b = 0$ . Contradiction.

If  $\forall a, b \in R, a, b \neq 0, ab \neq 0$ ,

Consider  $a(b - c) = ab - ac = 0$  or  $ab = ac$ . Then  $a = 0$  or  $b - c = 0$

If  $b = c$  done.

Suppose  $1 = 0$ .  $1a = a, \quad \forall a \in R$ .  $0a = a = 0$ . But then  $R$  zero ring. Zero ring is not a domain.

Then  $1 \neq 0$

**Proposition 9** (3.6). commutative ring  $\mathbb{I}_m \equiv \mathbb{Z}/m\mathbb{Z}$  domain iff  $m$  prime.

*Proof.* If  $m = ab$ , where  $1 < a, b < m$ ,

then  $[a], [b] \neq [0]$  in  $\mathbb{I}_m \equiv \mathbb{Z}/m\mathbb{Z}$ , but  $[a][b] = [m] = [0]$ . If  $\mathbb{I}_m \equiv \mathbb{Z}/m\mathbb{Z}$  domain, on prime (number).

If  $m$  prime,  $[a][b] = [ab] = [0]$ , then  $m|ab$ , and Euclid's Lemma gives  $m|a$  or  $m|b$ .

Example 3.7.

- (i)  $\mathcal{F}(\mathbb{R})$  - set of all functions  $R \rightarrow R$  equipped with pointwise addition and pointwise multiplication.
- $\forall f, g \in \mathcal{F}(\mathbb{R}), \text{ define } \begin{aligned} f + g : a &\mapsto f(a) + g(a) \\ fg : a &\mapsto f(a)g(a) \end{aligned}$
- $\mathcal{F}(\mathbb{R})$  commutative ring.  
So
- $$\mathcal{F}(\mathbb{R}) := \{f|f : \mathbb{R} \rightarrow \mathbb{R}, \forall f, g \in \mathcal{F}(\mathbb{R}), \begin{aligned} f + g &= (f + g)(a) = f(a) + g(a) \\ f \cdot g &= (f \cdot g)(a) = f(a)g(a) \end{aligned} \forall a \in \mathbb{R}\}$$
- is a commutative ring, with  
zero element,  $0 \equiv a \mapsto 0 \forall a \in \mathbb{R}$  i.e.  $0(a) = 0$   
unit,  $1 \equiv a \mapsto 1 \forall a \in \mathbb{R}$  i.e.  $1(a) = 1$   
 $\mathcal{F}(\mathbb{R})$  is not a domain.
- (ii)  $C^\infty(\mathbb{R}) \subsetneq \mathcal{F}(\mathbb{R})$  is a subring of  $\mathcal{F}(\mathbb{R})$  (that's what the notation  $\subsetneq$  means, that it's a proper subring)

**Definition 16.** Let  $a, b \in R$ , commutative ring  
 $a|b \equiv a$  **divides**  $b$  in  $R$  (or  $a$  **divisor** of  $b$  or  $b$  multiple of  $a$ ) if  $\exists c \in R$  s.t.  $b = ca$

**Definition 17.**  $u \in$  commutative ring  $R$  unit if  $u|1$  in  $R$ , i.e.  $\exists v \in R$  with  $uv = 1$  (EY:  $u|1$  is  $1/u$  and  $u$  unit if it has a multiplicative inverse)

**Definition 18. field**  $F$  commutative ring,  $1 \neq 0, \forall a \neq 0, a$  unit, i.e.  $a^{-1} \in F, a^{-1}a = 1$

```
sage: ZZ.is_field()
False
sage: QQ.is_field()
True
sage: RR.is_field()
True
sage: CC.is_field()
True
sage: Integers(5).is_field()
True
sage: Integers(4).is_field()
False
```

**Exercises. Exercise 3.1.** Suppose  $\exists 1'$

$1'a = a = 1a$  so

$$1 = 1'1 = 11' = 1'$$

since we could commute in a commutative ring.

**Exercise 3.2.**

- (i) Let  $x, y, z \in \mathbb{Z}$ .  $\mathbb{Z}$  commutative ring as it's an abelian group under addition, with the existence of an additive inverse, subtraction.  
Treat subtraction as a binary group operation.
- $$\begin{aligned} (xy)z &= (x - y)z = (x - y) - z = x - y - z \\ x(yz) &= x - (yz) = x - (y - z) = x - y + z \end{aligned}$$
- (ii)  $\mathbb{Z}/2$  Suppose  $x - y - z = x - y + z$  (from above, part (i))  
Suppose  $z = 0$ . Done. Otherwise,  $-z = z$ . So  $z = 1$  and  $-1 \sim 1$  for  $\mathbb{Z}/2$  Done.

**Exercise 3.3.**

- (i)  $R$  domain.  
Recall, domain has  $1 \neq 0$  and cancellation.  
 $a^2 = a = a \cdot 1$ . So  $a = 1$  Otherwise  $a = 0$
- (ii)  $f^2 = f$

$$f(x) = \begin{cases} 1 & \text{if } x \geq b \\ 0 & \text{if } a \leq x \leq b \\ -1 & \text{if } x \leq a \end{cases}$$

$f^2 = f \quad \forall x \in \mathbb{R}$ , pointwise, but  $a, b \in \mathbb{R}$  arbitrary.

**Exercise 3.8.**

- (i) Suppose  $a, b, c \in S$  and  $ca = cb$  for  $c \neq 0$ . Since  $a, b, c \in S, a, b, c \in R$  and  $ca, cb \in S \subset R$ , so  $a = b$ .  
Since  $1 \in S, 1 - 1 = 0 \in S$ . Since  $1, 0 \in S \subset R$  and  $1 \neq 0$  since  $R$  domain.  
 $\implies$  If  $R$  domain,  $S$  subring of  $R$ , then  $S$  domain (commutative ring,  $1 \neq 0$ , and cancellation).
- (ii) Clearly  $1 \neq 0$  for  $\mathbb{C}$ . If  $za = zb, \forall z \neq 0, \exists z^{-1} = \frac{1}{x+iy}$ , for  $z = x + iy$ , so  $a = b$ .  $\mathbb{C}$  domain.  
Now  $1 \in \mathbb{Z}[i]$ .

$$\forall a, b \in \mathbb{Z}[i], a = a_1 + a_2i, b = b_1 + b_2i, a - b = a_1 - b_1 + (a_2 - b_2)i \in \mathbb{Z}[i]$$

$$\forall a, b \in \mathbb{Z}[i], ab = a_1b_1 - a_2b_2 + (a_1b_2 + a_2b_1)i \in \mathbb{Z}[i]$$

$\mathbb{Z}[i]$  subring of  $\mathbb{C}$ . So  $\mathbb{Z}[i]$  domain.

**3.3. Polynomials.**

**Definition 19.** sequence  $\sigma = (s_0 \dots s_i \dots)$  polynomial if  $\exists m \geq 0, \quad s_i = 0, \quad \forall i > m$

**Notation.** If  $R$  commutative ring, then set of all polynomials with coefficients in  $R$  denoted by  $R[x]$

**Proposition 10** (3.14). *If  $R$  commutative ring, then  $R[x]$  commutative ring that contains  $R$  as subring.*

*Proof.* define addition:

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1 \dots s_i + t_i, \dots s_m + t_m, t_{m+1} \dots t_n)$$

without loss of generality, assume  $\sigma$  of degree  $m \leq n, \tau$  degree  $n$

define  $\sigma\tau = (c_0, c_1 \dots)$

$$c_k = \sum_{i+j=k} s_it_j = \sum_{i=0}^k s_it_{k-i}$$

$\sigma + \tau \in R[x]$  since  $s_i + t_i \in R, t_i \in R$

$$\sigma + \tau = \tau + \sigma$$

(by each entry,  $s_i, t_i \in R$  and  $R$ , commutative ring, is abelian in addition)

also since  $\forall s_i \in R, \exists -s_i \in R, 0 \in R$ , then

$$\begin{aligned}\sigma + (-\sigma) &= 0 \\ \sigma + 0 &= \sigma \text{ with } 0 = (0, 0, \dots)\end{aligned}$$

$$r\sigma = (rs_0 \dots rs_m, 0 \dots) \in R[x]$$

since

$$(\sigma + \tau) + \omega = (\dots(s_i + t_i) + w_i \dots) = (\dots s_i + (t_i + w_i) \dots) = \sigma + (\tau + \omega)$$

So  $R[x]$  abelian group in addition.

$$\sum_{i=0}^k s_i t_{k-i} = \sum_{j=0}^k s_{k-j} t_j = \sum_{j=0}^k t_j s_{k-j}$$

since  $s_{k-j}, t_j \in R$ , commutative ring.

So

$$\sigma\tau = \tau\sigma$$

Now

$$(\sigma(\tau\omega))_l = \sum_{i+j=l} s_i (tw)_j = \sum_{i+j=l} \sum_{a+b=j} s_i (t_a w_b) = \sum_{i+a+b=l} s_i t_a w_b = \sum_{j+b=l} \sum_{i+a=j} (s_i t_a) w_b = \sum_{j+b=l} (st)_j w_b = ((\sigma\tau)w)_l$$

$R \subset R[x]$  since polynomials of degree 0 are  $R$ .

□

(standard) notation

$$f(x) = s_0 + s_1x + s_2x^2 + \dots + s_nx^n$$

**Definition 20.** Let field  $k$ . fraction field  $k[x]$ ,  $k(x)$ , is called **field of rational functions over  $k$**

**Proposition 11** (3.19). *If field  $k$ , elements of  $k(x)$  have form  $f(x)/g(x)$ , where  $f(x), g(x) \in k[x]; g(x) \neq 0$*

*Proof.* Recall Thm. 3.13. If  $R$  domain, then  $\exists$  field  $F$  containing  $R$  as a subring; moreover  $F$  chosen s.t.  $\forall f \in F, \exists a, b \in R$  with  $b \neq 0$  and  $f = ab^{-1}$ .

$0, 1 \in k[x]$  and clearly  $0 \neq 1$

If  $ca = cb$  and  $c \neq 0$ , then  $a = b$  since

$$\begin{aligned}\left(\sum_{i=0}^{p_c} c_i x^i\right) \left(\sum_{j=0}^{p_a} a_j x^j\right) &= \left(\sum_{i=0}^{p_c} c_i x^i\right) \left(\sum_{j=0}^{p_b} b_j x^j\right) = \sum_{i=0}^{p_c} \sum_{j=0}^{p_a} c_i a_j x^{i+j} = \sum_{i=0}^{p_c} \sum_{j=0}^{p_b} c_i b_j x^{i+j} \\ &\implies \sum_{i=0}^{p_c} c_i x^i \left(\sum_{j=0}^{p_a} a_j x^j - \sum_{j=0}^{p_b} b_j x^j\right) = 0 \implies a = b\end{aligned}$$

$k[x]$  domain if  $k$  field.

field  $k(x) = \frac{f(x)}{g(x)}$ , where  $f(x), g(x) \in k[x]; g(x) \neq 0$ .

*Exercises.* **Exercise 3.21.**

(i)

(ii) 

```
sage: Integers(4)[x]
Univariate Polynomial Ring in x over Ring of integers modulo 4
sage: x
x
sage: (2*x+1)**2-1 in Integers(4)[x]
True
```

**Exercise 3.24.** Let  $R$  be commutative ring; let  $f(x) \in R[x]$ .

(i) Given  $(x-a)^2 | f(x); f(x) = (g) \cdot (x-a)^2 \equiv g(x)(x-a)^2$ ,  
(a) we can try to strategy of “term-by-term” comparison: if

$$f(x) = \sum_{i=0}^n s_i x^i; \quad f'(x) = \sum_{j=1}^n j s_j x^{j-1}$$

$$g(x) = \sum_{i=0}^m b_i x^i$$

$$g(x)(x-a) = \sum_{i=0}^m (b_i x^{i+1} - ab_i x^i) = -ab_0 + \sum_{i=1}^m (b_{i-1} - ab_i) x^i + b_m x^{m+1} = \sum_{i=0}^{m+1} s_i x^i$$

(b) Better yet, if we can treat polynomials as polynomials, after proving that even if  $R$  is only a commutative ring (not necessarily a field), then this differentiation operation obeys the so-called product rule and then

$$f'(x) = g'(x)(x-a)^2 + g(x)2(x-a) = (x-a)(g'(x)(-a) + 2g(x)) \implies \boxed{x-a | f'(x)}$$

(ii) Given  $x-a | f(x)$ , and so  
 $x-a | f'(x)$

$$(x-a)g(x) = f(x)$$

$$f'(x) = g(x) + (x-a)g'(x) = (x-a)h(x)$$

$$(x-a)f'(x) = (x-a)g(x) + (x-a)^2g'(x) = (x-a)^2h(x) = f(x) + (x-a)^2g'(x)$$

$$\implies f(x) = (x-a)^2(h(x) - g'(x)) \implies \boxed{(x-a)^2 | f(x)}$$

□

3.4. Greatest Common Divisors.

**Theorem 11** (3.21). (*Division Algorithms*) Assume  $k$  field,  $f(x), g(x) \in k[x]$ ,  $f(x) \neq 0$   
Then  $\exists!$   $q(x), r(x) \in k[x]$  s.t.  $g(x) = q(x)f(x) + r(x)$  and either  $r(x) = 0$  or  $\deg(r) < \deg(f)$

*Proof.* If  $f|g$ , then  $g = qf$  for some  $q$  and  $r = 0$ . Done.

If  $f \nmid g$ , then consider all  $g - qf \in k[x] \quad \forall q \in k[x]$   
By least integer axiom,  $\exists r = g - qf \in k[x]$  s.t.  $\deg(r) \leq \deg(g - qf)$

Let  $f(x) = s_n x^n + \cdots + s_1 x + s_0$   
 $r(x) = t_m x^m + \cdots + t_1 x + t_0$

$s_n \neq 0$ , so  $s_n$  unit ( $k$  field), so  $\exists s_n^{-1} \in k$   
If  $\deg(r) \geq \deg(f)$ , define

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} f(x)$$

Define

**leading term**  $LT$ ,

$$\begin{aligned} LT : k[x] &\rightarrow k[x] \\ LT(f) &= s_n x^n \end{aligned}$$

$$\implies h = r - \frac{LT(r)}{LT(f)} f$$

$$h = 0 \text{ or } \deg(h) < \deg(r)$$

$$\text{If } h = 0, \text{ then } r = \frac{LT(r)}{LT(f)} f \text{ and } g = qf + r = \left( q + \frac{LT(r)}{LT(f)} \right) f, \text{ contradicting } f \nmid g$$

$$\text{If } h \neq 0, \text{ then } \deg(h) < \deg(r), \text{ and}$$

$$\begin{aligned} g - qf &= r = h + \frac{LT(r)}{LT(f)} f \\ g - \left[ q + \frac{LT(r)}{LT(f)} \right] f &= h \end{aligned}$$

Contradicting  $r$  being polynomial of least degree since  $\deg(h) < \deg(r)$

$$\implies \deg(r) < \deg(f)$$

**Lemma 4** (3.23). Let  $f(x) \in k[x]$ , where  $k$  field. Let  $u \in k$   
Then  $\exists q(x) \in k[x]$  s.t.

$$f(x) = q(x)(x - u) + f(u)$$

*Proof.* By division algorithm,  $f(x) = q(x)(x - u) + r \quad \deg(r) < (x - u)$ , so  $r$  constant.

$$f(u) = 0 + r \text{ so } r = f(u)$$

**Proposition 12** (3.24). If  $f(x) \in k[x]$ ,  $k$  field, then  
a root of  $f(x)$  in  $k$  iff  $x - a|f(x)$  in  $k[x]$

*Proof.* If a root of  $f(x)$ , then  $f(a) = 0$ . By Lemma 3.23,

$$f(x) = q(x)(x - a) + f(a) = q(x)(x - a) \implies \frac{f(x)}{x - a} = q(x)$$

$$\text{if } f(x) = g(x)(x - a), f(a) = g(a)(a - 0) = 0$$

□

**Theorem 12** (3.25). Let  $k$  field, let  $f(x) \in k[x]$

If  $\deg(f(x)) = n$ , then  $f(x)$  has at most  $n$  roots in  $k$

*Proof.* If  $n = 0$ , then  $f(x) = a_0 \neq 0$ , and so number of roots in  $k$  is 0  
Let  $n > 0$ . If  $f(x)$  has no roots in  $k$ , then  $0 \leq n$ . Done.

Assume  $\exists a \in k$ , a root of  $f(x)$ .

By Prop. 3.24 or **12**,  $f(x) = q(x)(x - a)$ ,  $q(x) \in k[x]$ ,  $\deg q(x) = n - 1$ .

If  $\exists$  root  $b \in k$ ,  $b \neq a$ , then  $0 = f(b) = q(b)(b - a)$

$b - a \neq 0$ , so  $q(b) = 0$  ( $k$  field, so  $k$  domain, so cancellation law applies). So  $b$  root of  $q(x)$

$\deg(q) = n - 1$ , so by induction hypothesis,  $q(x)$  has at most  $n - 1$  roots in  $k$

$f(x)$  has at most  $n$  roots in  $k$ .

□

**Definition 21.** If  $f(x), g(x) \in k[x]$ ,  $k$  field, then

**common divisor** is  $c(x) \in k[x]$  s.t.  $c(x)|f(x)$   
 $c(x)|g(x)$

□

If  $f(x), g(x) \in k[x]$ ,  $f \neq 0$ ,

$$g \neq 0$$

define **greatest common division** gcd to be monic common divisor having largest degree.

denote notation  $(f, g)$

Recall that monic is  $f(x) \in k[x]$  if its leading coefficient is 1

□ **leading coefficient** of  $f(x) \in k[x]$ , is coefficient of highest power of  $x$  occurring in  $f(x)$ .

3.5. **Homomorphisms.** Just as homomorphisms are used to compare groups, so are homomorphisms used to compare commutative rings.

**Definition 22.** if  $A, R$  (commutative) rings, (ring) homomorphism is  $f : A \rightarrow R$  s.t.

- (i)  $f(1) = 1$
- (ii)  $f(a + a') = f(a) + f(a')$
- (iii)  $f(aa') = f(a)f(a')$

A homomorphism that is also a bijection is called an isomorphism. commutative rings  $A$  and  $R$  are called isomorphic, denoted  $A \cong R$ , if  $\exists$  isomorphism  $f : A \rightarrow R$

Example 3.40

- (i)
- (ii)
- (iii)
- (iv)  $R$  commutative ring,  $a \in R$ . Define **evaluation homomorphism**  
 $e_a : R[x] \rightarrow R$   
 $e_a(f(x)) = f(a)$  i.e. if  $f(x) = r_i x^i$ , then  $f(a) = r_i a^i$   
 $e_a$  ring homomorphism

$$\begin{aligned} e_a(1(x)) &= 1(a) = a \\ e_a((f + g)(x)) &= e_a(f(x) + g(x)) = f(a) + g(a) = (f + g)(a) = e_a(f(x)) + e_a(g(x)) \\ e_a((fg)(x)) &= (fg)(a) = f(a)g(a) = e_a f(x)e_a g(x) \end{aligned}$$

**Definition 23.** ideal  $I \subset R$  s.t.

- (i)  $0 \in I$
- (ii)  $\forall a, b \in I, a + b \in I$
- (iii) if  $a \in I, r \in R$ , then  $ra \in I$

proper ideal  $I$ -ideal  $I \neq R$

Example 3.49.

If  $b_1, b_2, \dots, b_n \in R$ , then set of all linear combinations

$$I = \{r_1 b_1 + r_2 b_2 + \dots + r_n b_n | r_i \in R \quad \forall i\}$$

is an ideal in  $R$ .

write  $I = (b_1, b_2, \dots, b_n)$  and call  $I$  ideal generated by  $b_1, b_2, \dots, b_n$

in particular, if  $n = 1$ ,

$$I = (b) = \{rb | r \in R\}$$

is an ideal in  $R$ , consists of all multiples of  $b$ , and is called principal ideal generated by  $b$

$R, \{0\}$  are always principal ideals  $R = (1), \{0\} = (0)$   
in  $\mathbb{Z}$ , even integers form principal ideal  $(2)$

**Proposition 13** (3.50). if  $f : A \rightarrow R$  ring homomorphism,  
then  $\ker f$  ideal in  $A$   
 $\text{im } f$  subring of  $R$

if  $A, R \neq \text{zero rings}$ , then  $\ker f$  proper ideal.

*Proof.*  $f(0) = 0$  so  $0 \in \ker f$

If  $f(a) = f(b) = 0$ ,  
 $f(a + b) = f(a) + f(b) = 0$ .  $a + b \in \ker f$   
i.e.  $\ker f$  additive subgroup of  $A$ .

$$f(ra) = f(r)f(a) = f(r)0 = 0 \quad ra \in \ker f$$

$\ker f$  ideal.

If  $R$  not zero ring,  $1 \neq 0$ ,  
 $f(1) = 1 \neq 0$  and so for  $1 \in A$   
 $1 \notin \ker f$ , so  $\ker f$  proper ideal

$1 \in A$ , so  
 $f(1) = 1 \in \text{im } f$

if  $c = f(a)$  i.e.  $c, d \in \text{im } f$ ,  $c + d = f(a + b)$   
 $d = f(b)$

$a + b \in A$  so  $c + d \in \text{im } f$

$$cd = f(a)f(b) = f(ab)$$

$ab \in A$  so  $cd \in \text{im } f$

$\text{im } f$  a subring

□

**Definition 24.** domain  $R$  **principal ideal domain** (PID) if every ideal in  $R$  is a principal ideal

Example 3.55

- (i) the ring of integers is a PID
- (ii) every field is a PID, by Example 3.51 (ii)

Exercises. Exercise 3.39.

- (i) Let  $\varphi : A \rightarrow R$  isomorphism,  $\psi : R \rightarrow A$  its inverse.  
 $a = \psi(\varphi(a))$  so  $\forall a \in \text{im}\psi$ ,  $\psi$  surjective.  
Suppose  $\psi(r) = \psi(s)$

$r, s \in R$ , so  $\varphi(a) = r$  as  $\varphi$  isomorphism.  
 $\varphi(b) = s$

$\psi\varphi(a) = a = \psi(\varphi(b)) = b$

$a = b$  so  $r = s$  by  $\varphi$ .  $\psi$  injective.  
 $\psi$  bijective.  $\psi$  isomorphism.

(ii)

(iii)

Exercise 3.41.

Suppose  $I \cap J = 0$

Consider  $i \in I$   
 $j \in J$

Clearly  $i - j \neq 0$  and  $i - j \in R$   
Let  $r \neq 0$ ,  $r \in R$

$r(i - j) \neq 0$  by Prop. 3.5.

Let  $r = i$  as  $I \subset R$

$i(i - j) = i^2 - ij$

But, as a commutative ring and  $I$  an ideal,  
 $i(i - j) \in I$ . so that  $i^2 - ij \in I$ . So  $-ij \in I$ .  
But as  $-i \in I \subset R$ ,  $-ij \in J$ ,  $ij \neq 0$ . Contradiction.

4. FIELDS

5. GROUPS II

5.1.

5.2.

5.3.

5.4.

5.5. Presentations. “How can we describe a group?” (Rotman)

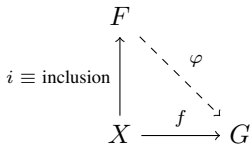
Motivation: describe groups as being generated subject to certain relations. EY: useful for “large groups” instead of enumerating all possible elements.

**Definition 25.** group of **generalized quaternions**  $\mathbb{Q}_n$ ,  $n \geq 3$ ,  $|\mathbf{Q}_n| = 2^n$  (group of order  $2^n$ ), generated by 2 elements  $a, b$  s.t.

$a^{2^{n-1}} = 1$ ,  $bab^{-1} = a^{-1}$  and  $b^2 = a^{2^{n-2}}$

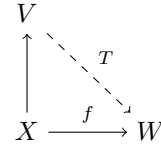
**Definition 26.** If  $X$  subset of group  $F$ ,  
then  $F$  **free group** with basis  $X$  if

$\forall$  group  $G$ ,  $\forall f : X \rightarrow G$ ,  $\exists!$  homomorphism  $\varphi : F \rightarrow G$   
 $\varphi(x) = f(x) \forall x \in X$



Note: modeled on Thm. 3.9.2 Rotman or

**Theorem 13.** Let  $X = v_1 \dots v_n$  basis of vector space  $V$ .  
If  $W$  vector space and  $u_1 \dots u_n$  list in  $W$ , then  $\exists!$  linear transformation  $T : V \rightarrow W$ , s.t.  $T(v_i) = u_i \quad \forall i$



**Definition 27.** if  $X$  subset of group  $F$ ,  
then  $F$  free group with basis  $X$  if

$\forall$  group  $G$ ,  $\forall f : X \rightarrow G$ ,  $\exists!$  homomorphism  $\varphi : F \rightarrow G$   
 $\varphi(x) = f(x) \quad \forall x \in X$

**Definition 28.** Let  $A, B$  be words on  $X$ , possibly  $A, B$  empty, i.e.  $A = 1$  or  $B = 1$ . Let  $w = AB$ .  
An **elementary** operation is either an **insertion** or **deletion**.  
insertion, change  $w = AB \mapsto Aaa^{-1}B$  for some  $a \in X \cup X^{-1}$   
deletion of a subword of  $w$  of form  $aa^{-1}$ , changing  $w = Aaa^{-1}B \mapsto AB$

**Definition 29.**  $w \rightarrow w'$  denote  $w'$  arising from  $w$  by elementary operation.  
words  $u, v$  on  $X$  are equivalent, denoted by  $u \sim v$ , if  $\exists$  words  $u = w_1, w_2 \dots w_n = v$  and elementary operations

$u = w_1 \rightarrow w_2 \rightarrow \dots \rightarrow w_n = v$

denote equivalence class of word  $w$  by  $[w]$

Note  $xx^{-1} \sim 1$ ,  $[xx^{-1}] = [1] = [x^{-1}x]$   
 $x^{-1}x \sim 1$ .

**Definition 30.** **semigroup** is set having associative operation.

**monoid** is semigroup  $S$  having identity  $q$ .

homomorphism (semigroups)  $f : S \rightarrow S'$  s.t.  $f(xy) = f(x)f(y)$

homomorphism (monoids)  $f : S \rightarrow S'$  s.t.  $f(xy) = f(x)f(y)$  and  $f(1) = 1$

cf. Rotman, **Advanced Modern Algebra** Thm. 5.72

**Theorem 14.** If  $X$  set, then set  $F$  of all equivalence classes of words on  $X$  with operation  $[u][v] = [uv]$  is free group with basis  $\{[x] | x \in X\}$ .

Moreover,  $\forall [v] \in F$  has normal form:  $\forall [u] \in F, \exists !$  reduced word  $w$  s.t.  $[u] = [w]$

cf. Rotman, **Advanced Modern Algebra** Prop. 5.73

**Proposition 14.** (1) Let  $X_1$  basis of free group  $F_1$ . If  $\exists$  bijection  $f : X_1 \rightarrow X_2$ , then  $\exists$  isomorphism  $\varphi : F_1 \rightarrow F_2$ .

$X_2$  basis of free group  $F_2$

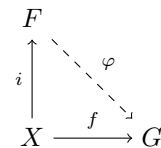
(2) If  $F$  free group with basis  $X$ , then  $F$  generated by  $X$ .

**Proposition 15.**  $\forall$  group  $G$ , is a quotient of a free group.

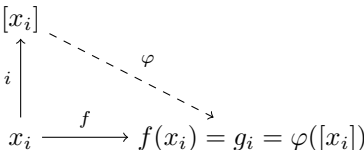
*Proof.* Let  $X$  set s.t.  $\exists$  bijection  $f : X \rightarrow G$  (e.g. take  $X$  underlying set of  $G$ , and  $f = 1_G$ ).

Let  $F$  free group with basis  $X$ .

$\exists$  homomorphism  $\varphi : F \rightarrow G$ . Thus, from definition of a free group



$\varphi$  surjective because  $f$  i.e.



$\forall g \in G, g = f(x)$  and  $\varphi([x_i]) = \varphi(i(x_i)) = f(x_i) = g$ , i.e.

Thus  $G \cong F/\ker\varphi$ .

□

**Definition 31.** **presentation** of group  $G \equiv G \equiv (X|R)$ , set  $X$ , set of words on  $X \equiv R$ ,  $G = F/N$ ;  $F$  free group with basis  $X$ ,  $N$  normal subgroup generated by  $R$ , i.e. subgroup generated by all conjugates of elements of  $R$ .

set  $X$  called **generators**, set  $R$  **relations**.

**Definition 32.** group  $G$  **finitely generated** if it has presentation  $(X|R)$  with  $X$  finite

group  $G$  **finitely presented** if it has presentation  $(X|R)$  with both  $X, R$  finite

## 6. COMMUTATIVE RINGS II

## 7. MODULES AND CATEGORIES

### 7.1. Modules.

**Definition 33.**  $R$ -module is (additive) abelian group  $M$ ,

equipped with scalar multiplication  $R \times M \rightarrow M$

$$(r, m) \mapsto rm$$

s.t.  $\forall m, m' \in M, \forall r, r', 1 \in R$

$$(i) \quad r(m + m') = rm + rm'$$

$$(ii) \quad (r + r')m = rm + r'm$$

$$(iii) \quad (rr')m = r(r'm)$$

$$(iv) \quad 1m = m$$

Example 7.1

(i)  $\forall$  vector space over field  $k$  is a  $k$ -module. (by inspection of the axioms for a vector space, associativity, distributivity!)

(ii)  $\forall$  abelian group is a  $\mathbb{Z}$ -module, by laws of exponents (Prop. 2.23)

Indeed, for

$$\mathbb{Z} \times M \rightarrow M$$

$$(r, m) \mapsto rm \equiv m^r$$

and so

$$r(m \cdot m') \equiv (m \cdot m')^r = m^r(m')^r = rm + rm'$$

(since  $M$  abelian)

(iii) For commutative ring, scalar multiplication, defined to be given multiplication of elements of  $R$

$$R \times R \rightarrow R$$

$$(a, b) \mapsto ab$$

For reference, recall some of the properties of a commutative ring:

$$ab = ba$$

$$a(bc) = (ab)c$$

$$1a = a$$

$$a(b + c) = ab + ac$$

$\forall$  ideal  $I$  in  $R$  is an  $R$ -module,

for if  $i \in I$ , then  $ri \in I$ .

$$r \in R$$

$$0 \in I$$

$$\forall a, b \in I, a + b \in I$$

If  $a \in I, r \in R$ , then  $ra \in I$ .

(iv)

(v) Let linear  $T : V \rightarrow V$ ,  $V$  finite-dim. vector space over field  $k$ .

Recall  $k[x] \equiv$  set of polynomials with coefficients in  $k$ .

$$\begin{array}{l} \text{Define } k[x] \times V \rightarrow V \\ f(x)v = \left(\sum_{i=0}^m c_i x^i\right)v = \sum_{i=0}^m c_i T^i(v) \quad \forall f(x) = \sum_{i=0}^m c_i x^i \in k[x] \\ \implies \text{denote } k[x]\text{-module } V^T. \end{array}$$

Special case: Let  $A \in \text{Mat}_k(n, n)$ , let linear  $T : k^n \rightarrow k^n$ .

$$T(w) = Aw$$

vector space  $k^n$  is  $k[x]$ -module if we define scalar multiplication

$$\begin{array}{l} k[x] \times k^n \rightarrow k^n \\ f(x)w = \left(\sum_{i=0}^m c_i x^i\right)w = \sum_{i=0}^m c_i A^i w \end{array}$$

$$\forall f(x) =$$

$$\begin{array}{l} \sum_{i=0}^m c_i x^i \in k[x] \\ \text{In } (k^n)^T, xw = T(w) \\ \text{In } (k^n)^A, xw = Ax \\ T(w) = Ax \text{ and so } (k^n)^T = (k^n)^A \text{ (EY : 20151015 because of induction?)} \end{array}$$

**Definition 34.** if ring  $R$ ,  $R$ -modules  $M, N$ , then function  $f : M \rightarrow N$  is  $R$ -homomorphism (or  $R$ -map) if  $\forall m, m' \in M, \forall r \in R$ ,

- (i)  $f(m + m') = f(m) + f(m')$
- (ii)  $f(rm) = rf(m)$

EY : 20151015 isn't this just a homomorphism that is linear in  $R$ ?

Example 7.2.

- (i)
- (ii)
- (iii)
- (iv)
- (v) Let linear  $T : V \rightarrow V$ , let  $v_1 \dots v_n$  be basis of  $V$ , let  $A$  be matrix of  $T$  relative to this basis.  
Let  $e_1 \dots e_n$  be standard basis of  $k^n$ .

$$\begin{array}{l} \text{Define } \varphi : V \rightarrow k^n \\ \varphi(v_i) = e_i \end{array}$$

$$\begin{array}{l} \varphi(xv_i) = \varphi(T(v_i)) = \varphi(v_j a_{ji}) = a_{ji} \varphi(v_j) = a_{ji} e_j \\ x\varphi(v_i) = A\varphi(v_i) = Ae_i \end{array}$$

$$\implies \varphi(xv) = x\varphi(v) \quad \forall v \in V$$

$$\text{By induction on } \deg(f), \varphi(f(x)v) = f(x)\varphi(v) \quad \forall f(x) \in k[x] \quad \forall v \in V$$

$$\implies \varphi \text{ is } k[x]\text{-map}$$

$$\implies \varphi \text{ is } k[x]\text{-isomorphism of } V^T \text{ and } (k^n)^A.$$

**Proposition 16 (7.3).** *Let vector space over field  $k$ ,  $V$ , let linear  $T, S : V \rightarrow V$*

*Then  $k[x]$ -modules  $V^T, V^S$  are  $k[x]$ -isomorphic iff  $\exists$  vector space isomorphism  $\varphi : V \rightarrow V$  s.t.  $S = \varphi T \varphi^{-1}$ .*

*Proof.* If  $\varphi : V^T \rightarrow V^S$  is a  $k[x]$ -isomorphism,

$$\varphi(f(x)v) = f(x)\varphi(v) \quad \forall v \in V, \forall f(x) \in k[x]$$

if  $f(x) = x$ , then  $\varphi(xv) = x\varphi(v)$

$$xv = T(v)$$

$$x\varphi(v) = S(\varphi(v))$$

$$\implies \varphi \circ T(v) = S \circ \varphi(v) \implies \varphi \circ T = S \circ \varphi$$

$\varphi$  isomorphism, so  $S = \varphi \circ T \circ \varphi^{-1}$

Conversely, if given isomorphism  $\varphi : V \rightarrow V$  s.t.  $S = \varphi T \varphi^{-1}$ , then  $S\varphi = \varphi T$ .

$$S\varphi(v) = \varphi T(v) = \varphi(xv) = x\varphi(v)$$

Then by induction,  $\varphi(x^n v) = x^n \varphi(v)$  (for  $S^n \varphi(v) = x^n \varphi(v) = (\varphi T \varphi^{-1})^n \varphi(v) = \varphi T^n v = \varphi(x^n v)$ ).

By induction on  $\deg(f)$ ,  $\varphi(f(x)v) = f(x)\varphi(v)$ .

□

**Definition 35.** if  $R$ -module  $M$ , the submodule  $N$  of  $M$ , denoted  $N \subseteq M$ , is additive subgroup  $N$  of  $M$ , closed under scalar multiplication  $rn \in N$  whenever  $n \in N, r \in R$

Example 7.7

- (i)
- (ii)
- (iii)
- (iv) submodule of  $W$  of  $V^T$ ,  $k[x]$ -module  $V^T$ , where linear  $T$ , is subspace  $W$  of  $V$ , s.t.  $T(W) \subseteq W$ .

*Proof.* if given submodule  $W, \forall w \in W, xw = T(w) \in W \implies T(W) \subseteq W$

ig given subspace  $W$  of  $V$ ,  $W$  additive subgroup  $W$  of  $V^T$ .

$$\forall w \in W, \quad f(x)w = \sum_{i=0}^m c_i x^i w = \sum_{i=0}^m c_i T^i w \in W$$

since  $T(W) \subseteq W$  and  $c_i T^i(w) \in W$

□

$$\implies \textbf{invariant subspace } W, \text{ is submodule } W \text{ of } V^T \text{ s.t. } T(W) \subseteq W$$

**Theorem 15** (First Isomorphism Theorem). *If  $f : M \rightarrow N$   $R$ -map of modules (i.e. homomorphism linear in  $R$ ),*

*then  $\exists$   $R$ -isomorphism  $\varphi : M/\ker f \rightarrow \text{im } f$*

$$\varphi : m + \ker f \mapsto f(m)$$

*Proof.* Let  $[m] \in M/\ker f$

$$\varphi([m]) = f(m)$$

Now

$$\varphi^{-1} : \text{im } f \rightarrow M/\ker f$$

$$\varphi^{-1} : y = f(m) \mapsto [m]$$

and  $\varphi^{-1}$  is well-defined on domain  $\text{im } f$ , since  $\forall y \in \text{im } f, \exists m \in M$ , s.t.  $f(m) = y$ .

Now

$$\varphi^{-1}\varphi([m]) = [m]$$



This is well defined, since

$$\varphi^{-1}\varphi(m + v_0) = \varphi^{-1}(f(m)) = [m]$$

Also

$$\varphi\varphi^{-1}(y) = \varphi[m] = f(m) = y$$

**Definition 36. exact sequence** if  $\text{im}f_{n+1} = \ker f_n \quad \forall n$ , for sequence of  $R$ -maps (i.e. homomorphisms linear in  $R$ ) and  $R$ -modules

$$\cdots \rightarrow M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \rightarrow \cdots$$

**Proposition 17** (7.20). (i)  $0 \rightarrow A \xrightarrow{f} B$  exact iff  $f$  injective

(ii)  $B \xrightarrow{g} C \rightarrow 0$  exact iff  $g$  surjective

(iii)  $0 \rightarrow A \xrightarrow{h} B \rightarrow 0$  exact iff  $h$  isomorphism

*Proof.* (i)  $\text{im}(0 \rightarrow A) = 0$  if assume  $0 \rightarrow A \xrightarrow{f} B$  exact,  $\ker f = 0$ , and so  $f$  injective  
Conversely, if  $f$  injective,  $\ker f = 0$  and  $\text{im}(0 \rightarrow A) = 0 = \ker f$ . So sequence is exact.

(ii)  $\ker(C \rightarrow 0) = C$

if  $B \xrightarrow{g} C \rightarrow 0$  exact,  $\text{img} = C$  and so  $g$  surjective.

Conversely, given  $g : B \rightarrow C$ ,

$\exists$  exact sequence  $B \xrightarrow{g} C \rightarrow C/\text{img}$  (cf. Exercise 7.13) since

$$\ker(C \rightarrow C/\text{img}) = \text{img}$$

if  $g$  surjective,  $\text{img} = C$ , and so  $B \xrightarrow{g} C \rightarrow 0$  exact.

(iii) from (i),  $0 \rightarrow A \xrightarrow{h} B$  exact iff  $h$  injective

from (ii),  $A \xrightarrow{h} B \rightarrow 0$  exact iff  $h$  surjective.

$\implies h$  isomorphism iff  $0 \rightarrow A \xrightarrow{h} B \rightarrow 0$

**Definition 37. short exact sequence**  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  is exact sequence.

**Proposition 18** (7.21). (i) If  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  short exact sequence, then

$$A \cong \text{im}f \text{ and } B/\text{im}f \cong C$$

(ii)

*Proof.* (i)  $f$  injective, so  $A \rightarrow \text{im}f$  isomorphism.

By first isomorphism thm.,  $B/\ker g \cong \text{img}$ .

$\text{img} = C$  since  $g$  surjective

$\text{im}f = \ker g$  by exactness.

$$\implies B/\text{im}f \cong C$$

(ii)

**Definition 38.** short exact sequence  $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$  split if  $\exists$  map  $j : C \rightarrow B$ , s.t.  $pj = 1_C$

**Proposition 19** (7.22). if exact sequence  $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$  split, then  $B \cong A \oplus C$

*Proof.* if  $b \in B$ , then  $p(b) \in C$

$b - j(p(b)) \in \ker p$ . Since  $p(b - j(p(b))) = p(b) - pj(p(b)) = p(b) - 1_C(p(b)) = 0$  since  $pj = 1_C$ .

By exactness,  $\ker p = \text{im}i$ ,  $\exists a \in A$  s.t.  $i(a) = b - j(p(b))$

Then  $\forall b \in B$ ,  $b = i(a) + j(p(b))$

Note that  $p$  surjective by exactness, and so  $C = \text{imp}$

Thus  $B = \text{im}i + \text{im}j$

If  $ia = x = jc$ , then  $p(x) = pia = 0$ , since  $pi = 0$  for  $\text{im}i = \ker p$

$px = pj c = c$  since  $pj = 1_C$ .

Thus  $x = jc = j(0) = 0$ .

So  $B \cong A \oplus C$

**Exercises.**

**Definition 39.** If  $f : M \rightarrow N$ , define **cokernel**, denoted  $\text{coker}f$ ,

$$(1) \quad \text{coker}f := N/\text{im}f$$

**Exercise 7.13.**

(i) if  $f : M \rightarrow N$  surjective,  $\text{im}f = N$ .  $\forall n \in N$ ,  $n = f(m)$  for some  $m \in M$ .

For  $[n] \in N/\text{im}f$ , then  $n + f(m) \in [n]$ .

Then  $n - f(m) = f(m) - f(m) = 0 \in [n]$

$$\text{coker}f = N/\text{im}f = 0$$

if  $\text{coker}f = 0$ ,  $\text{coker}f = N/\text{im}f = 0$ , then  $N = \text{im}f$  and so  $f$  surjective.

Thus,  $f : M \rightarrow N$  surjective iff  $\text{coker}f = 0$

(ii) If  $f : M \rightarrow N$ ,

$\ker(\ker f \rightarrow M) = 0 = \text{im}(0 \rightarrow \ker f)$  since  $\ker f \rightarrow M$  is inclusion

$\text{im}(\ker f \rightarrow M) = \ker f$  (by inclusion)

$\ker(N \rightarrow \text{coker}f) = \ker(N \rightarrow N/\text{im}f) = \text{im}f$

$\text{im}(N \rightarrow \text{coker}f) = \text{coker}f$

$\ker(\text{coker}f \rightarrow 0) = \text{coker}f \implies \text{im}(N \rightarrow \text{coker}f) = \ker(\text{coker}f \rightarrow 0)$

**Exercise 7.17.**

If given a short exact sequence  $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$  that splits, then  $B \cong A \oplus C$ , i.e.  $B = \text{im}i \oplus \text{im}j$  where  $j : C \rightarrow B$  s.t.  $pj = 1_C$  (by definition of a short exact sequence that splits).

Thus  $\forall b \in B$ ,  $b = i(a) + j(c)$ .

Define  $q$  to be the projection onto  $A$ :

$$q : B \rightarrow A$$

$$q(b) = a \text{ s.t. } qj = 0$$

Notice this analogy, with this case where the short exact sequence splits:

$$\text{im}i = \ker p$$

$$\text{im}j = \ker q$$

Now  $qi(a) = a \implies qi = 1_A$ .

Conversely, if  $\exists q : B \rightarrow A$  with  $qi = 1_A$ ,

Thus,

if short exact sequence  $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$  splits iff  $\exists q : B \rightarrow A$  with  $qi = 1_A$ .

$$\begin{array}{ccccccc}
0 & \longrightarrow & A & \xleftarrow{i} & B & \xrightarrow{p} & C \longrightarrow 0 \\
& & \downarrow 1 & & \downarrow (q, p) & & \downarrow 1 \\
0 & \longrightarrow & A & \xrightarrow{(1, p \circ i)} & A \oplus C & \longrightarrow & C \longrightarrow 0 \\
\\ 
0 & \vdash & a & \xleftarrow{i} & i(a) = b & \xrightarrow{p} & pi(a) = 0 = p(b) \vdash \longrightarrow 0 \\
& & \downarrow 1 & & \downarrow (q, p) & & \downarrow 1 \\
0 & \vdash & a & \xrightarrow{(1, p \circ i)} & (q(b), p(b)) = (a, c) & \longrightarrow & p(b) \vdash \longrightarrow 0
\end{array}$$

**7.2. Categories.** We can force 2 overlapping subsets  $A, B$  to be disjoint by “disjointifying” them: e.g. consider  $(A \cup B) \times \{1, 2\}$ , consider

$$A' = A \times \{1\}.$$

$$B' = B \times \{2\}$$

$$\implies A' \cap B' = \emptyset$$

since  $(a, 1) \neq (b, 2) \quad \forall a \in A, \forall b \in B$ .

$$\begin{array}{ll}
\text{Let bijections } \alpha : A \rightarrow A', & \alpha : a \mapsto (a, 1), \text{ denote } A' \cup B' \equiv A \coprod B. \\
\beta : B \rightarrow B' & \beta : b \mapsto (b, 2)
\end{array}$$

From Rotman, pp. 447,

**Definition 40. coproduct**  $A \coprod B \equiv C \in \text{Obj}(\mathcal{C})$

In my notation,

**coproduct**

$$\begin{array}{l}
(2) \quad (\mu_1, A_1 \coprod A_2) \\
(\mu_2, A_1 \coprod A_2)
\end{array}$$

where injection (morphisms)

$$\begin{array}{l}
(3) \quad \mu_1 : A_1 \rightarrow A_1 \coprod A_2 \\
\mu_2 : A_1 \rightarrow A_1 \coprod A_2
\end{array}$$

s.t.

$$\begin{array}{l}
\forall A \in \text{Obj}\mathbf{A}, \forall f_1, f_2 \in \text{Mor}\mathbf{A} \text{ s.t. } f_1 : A_1 \rightarrow A \\
f_2 : A_2 \rightarrow A
\end{array}$$

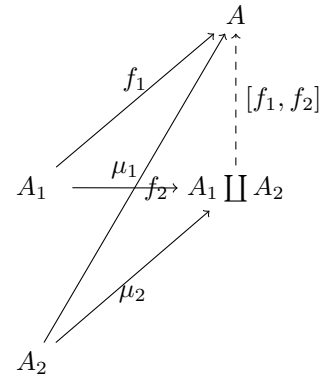
then

(4)

$$\begin{array}{l}
\exists ! [f_i] \equiv [f_1, f_2] \in \text{Mor}\mathbf{A}, [f_1, f_2] : A_1 \coprod A_2 \rightarrow A \text{ s.t.} \\
[f_1, f_2]\mu_1 = f_1 \\
[f_1, f_2]\mu_2 = f_2
\end{array}$$

i.e.

(5)



So to generalized, for  $i \in I$ , (finite set  $I$ ?)

**coproduct**  $(\mu_j, \coprod_{i \in I} A_i)_{j \in I}$ , where  
(family of) injection (morphisms)  $\mu_j : A_j \rightarrow \coprod_{i \in I} A_i$

s.t.

$$\forall A \in \text{Obj}\mathbf{A}, \forall f_i \in \text{Mor}\mathbf{A}, i \in I, f_i : A_i \rightarrow A$$

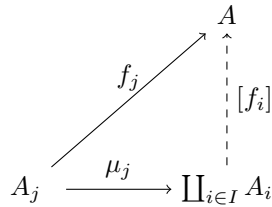
then

(6)

$$\begin{array}{l}
\exists ! [f_i] \equiv [f_i]_{i \in I} \in \text{Mor}\mathbf{A}, [f_i] : \coprod_{i \in I} A_i \rightarrow A \text{ s.t.} \\
[f_i]\mu_j = f_j \quad \forall j \in I
\end{array}$$

i.e.

(7)



For notation purposes only, recall that it’s denoted the sets  $\text{Hom}(A, B)$  in  ${}_R\mathbf{Mod}$  by

$$\text{Hom}_R(A, B)$$

i.e., in my notation, for  $A, B \in \text{Obj}_R\mathbf{Mod}$ ,  $\text{Hom}(A, B) \subset \text{Mor}({}_R\mathbf{Mod})$ ,  $\text{Hom}(A, B) \equiv \text{Hom}_R(A, B)$

cf. Thm. 7.32 of Rotman

**Theorem 16** (7.32, Rotman). *Let commutative ring  $R$ .*

*$\forall R$ -module  $A$ ,  $\forall$  family  $\{B_i | i \in I\}$  of  $R$ -modules,*

$$(8) \quad \text{Hom}_R(A, \coprod_{i \in I} B_i) \simeq \prod_{i \in I} \text{Hom}_R(A, B_i)$$

*via  $R$ -isomorphism*

$$\varphi : f \mapsto (p_i f)$$

*where  $p_i$  are projections of product  $\prod_{i \in I} B_i$*

*Proof.* Let  $a \in A$ ,  $f, g \in \text{Hom}_R(A, \prod_{i \in I} B_i)$ .

$$\varphi(f + g)(a) = (p_i(f + g))(a) = (p_i(f(a) + g(a))) = (p_i f + p_i g)(a)$$

$\varphi$  additive.

$\forall i, \forall r \in R, p_i r f = r p_i f$  (since product of  $R$ -modules,  $\prod_{i \in I} B_i$  is also an  $R$ -module of  $\text{Obj}_R \mathbf{Mod}$ , by def. of product).

$$\varphi r f \mapsto (p_i r f) = (r p_i f) = r(p_i f) = r \varphi(f)$$

So  $\varphi$  is  $R$ -map.

If  $(f_i) \in \prod_i \text{Hom}_R(A, B_i)$ , then  $f_i : A \rightarrow B_i \quad \forall i$

By Rotman's Prop. 7.31 (If family of  $R$ -modules  $\{A_i | i \in I\}$ , then direct product  $C = \prod_{i \in I} A_i$  is their product in  $_R \mathbf{Mod}$ ),

By def. of product,  $\exists ! R$ -map,  $\theta : A \rightarrow \prod_{i \in I} B_i$  s.t.  $p_i \theta = f_i \quad \forall i$

$$\begin{array}{ccc} & A & \\ & \swarrow f_i & \downarrow \theta \\ B_i & \xleftarrow{p_i} & \prod_{i \in I} B_i \end{array}$$

Then

$$f_i) = (p_i \theta) = \varphi(\theta)$$

, and so  $\varphi$  *surjective*.

Suppose  $f \in \ker \varphi$ , so  $\theta = \varphi(f) = (p_i f)$ . Thus  $p_i f = 0 \quad \forall i$

$$\begin{array}{ccc} & A & \\ & \swarrow 0 & \downarrow f \\ B_i & \xleftarrow{p_i} & \prod_{i \in I} B_i \end{array}$$

But 0-homomorphism also makes this diagram commute, so uniqueness of homomorphism  $A \rightarrow \prod B_i$  gives  $f = 0$ .

## 8. ALGEBRAS

### 8.1. Noncommutative Rings.

**Definition 41.** **left  $R$ -module**, for ring  $R$ , is (additive) abelian group  $M$ , equipped with scalar multiplication

$$(9) \quad \begin{array}{l} R \times M \rightarrow M \\ (r, m) \mapsto rm \end{array}$$

s.t.  $\forall m, m' \in M, \forall r, r', 1 \in R$

- (1)  $r(m + m') = rm + rm'$
- (2)  $(r + r')m = rm + r'm$
- (3)  $(rr')m = r(r'm)$
- (4)  $1m = m$

**Definition 42.** **right  $R$ -module**, for ring  $R$ , (additive) abelian group  $M$ , equipped with scalar multiplication.

$$(10) \quad \begin{array}{l} M \times R \rightarrow M \\ (m, r) \mapsto mr \end{array}$$

s.t.  $\forall m, m' \in M, \forall r, r', 1 \in R$ ,

- (1)  $(m + m')r = mr + m'r$
- (2)  $m(r + r') = mr + mr'$
- (3)  $m(rr') = (mr)r'$
- (4)  $m1 = m$

Denote left  $R$ -module  ${}_R M$

right  $R$ -module  $M_R$

Example 8.7.

**Definition 43.** If  $M$  is left  $R$ -module, then  $R$ -map

$$(11) \quad f : M \rightarrow M$$

is an  $R$ -**endomorphism** of  $M$

**Definition 44.** **Endomorphism ring**  $\text{End}_R(M)$

$$(12) \quad \text{End}_R(M) := \{R - \text{endomorphisms of } M\}$$

as a set,

$$(13) \quad \text{End}_R(M) = \text{Hom}_R(M, M)$$

**Definition 45.** representation of ring  $R$  is ring homomorphism  $\sigma$

$$(14) \quad \sigma : R \rightarrow \text{End}_{\mathbb{Z}}(M)$$

where  $M$  is an abelian group

**Proposition 20** (8.8).  $\forall$  representation  $\sigma : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ , where  $M$  abelian group equips  $M$  with structure of left  $R$ -module.

□ Conversely,  $\forall$  left  $R$ -module  $M$  determines representation  $\sigma : R \rightarrow \text{End}_{\mathbb{Z}}(M)$

*Proof.* Given homomorphism  $\sigma : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ , denote  $\sigma(r) \equiv \sigma_r$

$$\sigma(r) : M \rightarrow M$$

Define scalar multiplication

$$\begin{aligned} R \times M &\rightarrow M \\ rm &= \sigma_r(m) \quad \forall m \in M \end{aligned}$$

Indeed,

$$\begin{aligned} r(m + m') &= \sigma_r(m + m') = \sigma_r m + \sigma_r m' = rm + rm' \\ (r + r')m &= \sigma_{(r+r')}m = \sigma(r + r')m = (\sigma(r) + \sigma(r'))m = \sigma(r)m + \sigma(r')m = \sigma_r m + \sigma_{r'}m = rm + r'm \\ (rr')m &= \sigma_{rr'}m = \sigma(rr')m = \sigma(r)\sigma(r')m = \sigma_r(\sigma_{r'}m) = r(r'm) \\ 1m &= \sigma_1m = \sigma(1)m = m \end{aligned}$$

Assume  $M$  left  $R$ -module.

If  $r \in R$ , then  $m \mapsto rm$  defines endomorphism  $T_r : M \rightarrow M$

$$\begin{aligned} \sigma : R &\rightarrow \text{End}_{\mathbb{Z}}(M) \\ \sigma : r &\mapsto T_r \end{aligned}$$

$$\begin{aligned} \sigma(rr')m &= T_{rr'}m = (r + r')m = T_r(T_{r'}m) = \sigma(r)\sigma(r')m \\ \sigma(r + r')m &= T_{r+r'}m = (r + r')m = (T_r + T_{r'})m = \sigma(r)m + \sigma(r')m \end{aligned}$$

So  $\sigma$  is a homomorphism.

8.2. Chain Conditions.

**Definition 46.** if  $k$  commutative ring, then ring  $R$  is  **$k$ -algebra** if  $R$  is a  $k$ -module and if  $\forall a \in k, \forall r, s \in R$   
 $a(rs) = (ar)s = r(as)$   
scalars  $a \in k$  commute with everything in  $R \ni r, s$ ,

if  $R, S$   $k$ -algebras, ring homomorphism  $f : R \rightarrow S$  is  **$k$ -algebra** map if

$$f(ar) = af(r) \quad \forall a \in k, \forall r \in R$$

8.3. Semisimple Rings.

**Definition 47.**  $k$ -representation of group  $G$  is homomorphism

$$\sigma : G \rightarrow GL(V)$$

where  $V$  is vector space over field  $k$

9. ADVANCED LINEAR ALGEBRA

9.1.

9.2.

9.3.

9.4.

9.5.

9.6. Graded Algebras.

**Definition 48.**  $R$ -algebra  $A$  is graded  $R$ -algebra if  $\exists R$ -submodules  $A^p \quad \forall p \geq 0$ , s.t.

- (i)  $A = \sum_{p \geq 0} A^p$
- (ii)  $\forall p, q \geq 0$ , if  $x \in A^p$ , then  $xy \in A^{p+q}$ , i.e.  $A^p A^q \subseteq A^{p+q}$   
 $y \in A^q$

$x \in A^p$  is called **homogeneous** of **degree**  $p$

Example 9.94

- (i) polynomial ring  $A = R[x]$ , graded  $R$ -algebra if we define

$$A^p = \{rx^p | r \in R\}$$

- (ii) polynomial ring  $A = R[x_1, x_2, \dots, x_n]$  is graded  $R$ -algebra if we define

$$A^p = \{rx_1^{e_1}x_2^{e_2} \dots x_n^{e_n} | r \in R \text{ and } \sum e_i = p\}$$

i.e.  $A^p$  consists of all monomials of total degree  $p$

- (iii) in algebraic topology, assign sequence of (abelian) cohomology groups  $H^p(X, R)$  to space  $X$ ,  $R$  commutative ring,  $p \geq 0$ , define multiplication on  $\sum_{p \geq 0} H^p(X, R)$  cup product, making it a graded  $R$ -algebra

10. HOMOLOGY

11. COMMUTATIVE RINGS III

## REFERENCES

- [1] Joseph J. Rotman, **Advanced Modern Algebra** (Graduate Studies in Mathematics) 2nd Edition, American Mathematical Society; 2 edition (August 10, 2010), ISBN-13: 978-0821847411  
EY : Note that I used the first edition.
- [2] Thomas W. Judson, **Abstract Algebra Theory and Applications**; Robert A. Beezer, **Sage Exercises for Abstract Algebra**, August 12, 2015; <http://abstract.ups.edu/download/aata-20150812-sage-6.8.pdf>