NOTES AND SOLUTIONS TO ADVANCED MODERN ALGEBRA BY JOSEPH ROTMAN

ERNEST YEUNG - MÜNCHEN

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

Contents

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 $a < p, b < p, a, b \in \mathbb{N}$

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*

Date: inverno 2012.

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 $C = \{b - na | n \in \mathbb{Z}\} \bigcap \mathbb{N}$.
$C \neq \emptyset$ (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 $\begin{matrix} qa + r = q'a + r' \\ (q - q')a = r' - r \end{matrix}$, $0 \leq r' < |a|$. 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 $d = sa + tb$

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

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 $x \sim y$ □

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 $\bigcup_{x \in X} [x] = X$.

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

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. $\begin{matrix} x \in A_i \\ y \in A_i \end{matrix}$. $x \sim y$ is clearly reflexive and symmetric.

Suppose $x \sim y$, $y \sim z$, so $\exists\, i, j \in I$, s.t. $\begin{matrix} x, y \in A_i \\ y, z \in A_j \end{matrix}$. Since $y \in A_i \bigcap A_j$, 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 $x \in A_j \bigcap A_i \implies i = j$ by pairwise disjointness, so $z \in A_i$, so $[x] \subseteq A_i$.
$\implies [x] = A_i$ □

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 nth case.

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

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 $f : X \to Y$
$V, W \subseteq Y$

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

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

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 $\alpha \in S_n$

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

α 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

$$\sigma = (1\,2)(1\,3\,4\,2\,5)(2\,5\,1\,3)$$

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).

$1 \in G$, $S \subset G$. $\Longrightarrow \exists\, a \in G$, 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)
$G = T \coprod S \coprod \{e\}$, $\quad |G| = k + 2m + 1 = 2n$. $k = 2(n - m) - 1$, 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* $aH \bigcap bH \neq \emptyset$, $aH = bH$
(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 $aH \bigcap bH \neq \emptyset$, then $aH = bH$.

(iii) Consider $\begin{aligned} H &\to aH \\ h &\mapsto ah \end{aligned}$, since $a^{-1} \in G$, then mapping is injective.
$\forall\, x \in aH$, $x = ah'$ 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

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

$\mathrm{GL}(2, \mathbb{R})$ is a group. Clearly, $\mathrm{SL}(2, \mathbb{R}) \subseteq \mathrm{GL}(2, \mathbb{R})$.
Use Prop. 2.30, $H \subseteq G$ is a subgroup iff $H \neq 0$ and $\forall\, x, y \in H$, then $xy^{-1} \in H$.
$1 \in \mathrm{SL}(2, \mathbb{R})$. $\det 1 = 1$. So $SL(2, \mathbb{R}) \neq 0$ as well.
Let $x, y \in \mathrm{SL}(2, \mathbb{R})$. $xy^{-1} \in \mathrm{GL}(2, \mathbb{R})$, since $\mathrm{GL}(2, \mathbb{R})$ a group and $x, y^{-1} \in \mathrm{GL}(2, \mathbb{R})$. $\det(xy^{-1}) = \det x \det y^{-1} = 1$ since $\det y = 1$.
Then $xy^{-1} \in \mathrm{SL}(2, \mathbb{R}) \implies \mathrm{SL}(2, \mathbb{R}) < \mathrm{GL}(2, \mathbb{R})$.

(ii) $1 \in \mathrm{GL}(2, \mathbb{Q})$ since $1 \in \mathbb{Q}$. Also $\mathrm{GL}(2, \mathbb{Q}) \neq 0$.
Let $x, y \in \mathrm{GL}(2, \mathbb{Q})$.
Let $y = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ $y^{-1} = \frac{1}{eh - fg} \begin{bmatrix} h & -f \\ -g & e \end{bmatrix}$. $xy^{-1} \in \mathrm{GL}(2, \mathbb{Q})$ 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 $\varphi : 2^G \to 2^G$?

Consider right coset Ha. $a^{-1} \in G$ since G group. $a^{-1}H$ is a left coset. φ 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 $aH = bH$. φ 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 $f : G \to H$ homomorphism.*

(i) *$kerf$ subgroup of G*
imf subgroup of H
(ii) *If $x \in kerf$, $\forall\, a \in G$*

$$axa^{-1} \in kerf$$

(iii) *f injection iff $kerf = 1$*

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

$$\begin{aligned} & f(x)f(y) = f(xy) \in \mathrm{im} f \\ & f(x^{-1})f(x) = f(x^{-1}x) = f(1) = 1 \\ & 1 = f(1), \text{ since } 1f(x) = f(1)f(x) = f(x) \end{aligned}$$

(ii)

$$\begin{gathered} f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)1(f(a))^{-1} = 1 \\ axa^{-1} \in \ker f \end{gathered}$$

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

$$f(a)f(b^{-1}) = f(ab^{-1}) = f(a)f(b^{-1}) = 1 \Longrightarrow ab^{-1} = 1 \qquad \boxed{a = b}$$

□

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

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

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

If G abelian, every subgroup is a normal subgroup.

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

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

(Trying stuff: 20130116)

$\alpha = (1 \quad 2 \quad 3) \qquad \alpha(1 \quad 2)\alpha^{-1} = (1 \quad 2 \quad 3)(1 \quad 2)(3 \quad 2 \quad 1) = (2 \quad 3) \notin H$
$\alpha^{-1} = (3 \quad 2 \quad 1)$

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

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

Proof. (i) γ_g homomorphism since

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

Now

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

so

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

so γ_g bijective. γ_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 $z^{-1}(zg)z^{-1} = z^{-1}gzz^{-1}$
$Z(G)$ normal subgroup $gz^{-1} = z^{-1}g$

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

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

$$\begin{aligned} & f(ab) = b^{-1}a^{-1} = f(b)f(a) = f(ba) \\ & f(aa^{-1}) = aa^{-1} = e = f(a^{-1})f(a) = f(a^{-1}a) = f(e) \end{aligned}$$

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 $f : G \to H$ 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.

$$\boxed{\text{so if } a \in G \text{ has infinite order, } f(a) \text{ has infinite order}}$$

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

$$\boxed{\text{if } a \in G,\, a^n = 1 \text{ , and } \nexists\, h \in H \text{ s.t. } h^n = 1, \text{ then } G \ncong H}$$

(ii) EY 20131227

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

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

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, $G = \{f : \mathbb{R} \to \mathbb{R} | f(x) = ax+b, \, a \neq 0\}$ clearly isomorphic to $\{\begin{bmatrix} a & b \\ c & 1 \end{bmatrix}$

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. $K \lhd G$)

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.

Definition 12 (quotient group)**.**
quotient group $G \mod K \equiv G/K$ -

if $G/K =$ family of all left cosets of subgroups $K \subset G =$
$$= \{gK | g \in G, K = \{gk | k \in K\}$$
and

$K =$ normal subgroup of G, i.e. $K \lhd G$, and so
$$aKbK = abK \qquad \forall\, a,b \in G,$$
so G/K group.

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

Proof. Define **natural map** $\pi : G \to G/K$
$$\pi(a) = aK$$
$$aKbK = abK = \pi(a)\pi(b) = \pi(ab) \qquad \text{so } \pi \text{ surjective homomorphism}$$

K identity element in G/K
$$\text{ker}\pi = \{a \in G | \pi(a) = K\} = \{a \in G | aK = K\} = K$$
By Lemma 2.40(i) □

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

then $kerf \lhd G$
$$G/kerf \cong imf$$

i.e. if $kerf = K$, $\varphi : G/K \to imf \leq H$*, then φ isomoprhism.*
$$aK \mapsto f(a)$$

□

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/K \arrow[ur, "\varphi"] & \end{tikzcd}$$

$$\varphi\pi = f$$

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

if $aK = bK$, then $a = bk$ for some $k \in K$, so
$$\varphi(ak) = f(a) = f(bk) = f(b)f(k) = f(b)1 = f(b) = \varphi(bK), \quad \text{since } k \in K = \text{ker}f\ (f(k) = 1)$$
φ well-defined

□

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

φ homomorphism.

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

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

φ surjective onto $\text{im}f$

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

$$1 = f(b)^{-1}f(a) \overset{f \text{ homomorphism}}{=} f(b^{-1})f(a) = f(b^{-1}a)$$
$$b^{-1}a \in \ker f = K$$
$$b^{-1}aK = K \qquad aK = bK \text{ so } \varphi \text{ injective}$$

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

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

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

f homomorphism.

f surjective (because a generator of G)

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

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

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, $H \lhd G$, then HK subgroup, $H \cap K \lhd K$*

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

Proof. Since $H \lhd G$, 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 $\varphi : G \to S_n$ with $\ker\varphi \leq H$*

Definition 13. if set X, group G, then G acts on X if $\exists$ function $G \times X \to X$, 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 $\alpha_g : G \to G$ 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 α consists of all permutations of S_n having same cycle structure as α.
$z \in$ 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, $aHa^{-1} = \{aha^{-1} | h \in H, a \in G\}$
$H \to G$
$h \mapsto aha^{-1}$ $\qquad aha^{-1} = ah'a^{-1}$ so injection. conjugate subgroups of G are isomorphic.

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

stabilizer of H is $N_G(H) = \{g \in G | gHg^{-1} = H\}$ $\quad$ 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 14. 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) $\exists\, 0 \in R$, $0 + x = x + 0$, $\forall\, x \in R$
(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 15. $S \subset R$ 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 16. 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 $1 = 0$. $1a = a,\ \ \forall\, a \in R$. $0a = a = 0$. 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 $R \to R$ 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

$$\mathcal{F}(\mathbb{R}) := \{ f | f : \mathbb{R} \to \mathbb{R}, \forall\, f, g \in \mathcal{F}(\mathbb{R}), \begin{aligned} & f + g = (f+g)(a) = f(a) + g(a) \\ & f \cdot g = (f \cdot g)(a) = f(a)g(a) \end{aligned} \forall\, a \in \mathbb{R} \}$$

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 17. 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 18. $u \in$ 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 19. **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.
$\Longrightarrow$ 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 $1 \in \mathbb{Z}[i]$.

$$\begin{aligned} & \forall\, a, b \in \mathbb{Z}[i],\ a = a_1 + a_2 i,\ b = b_1 + b_2 i,\ a - b = a_1 - b_1 + (a_2 - b_2)i \in \mathbb{Z}[i] \\ & \forall\, a, b \in \mathbb{Z}[i],\ ab = a_1 b_1 - a_2 b_2 + (a_1 b_2 + a_2 b_1)i \in \mathbb{Z}[i] \end{aligned}$$

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

3.3. **Polynomials.**

Definition 20. sequence $\sigma = (s_0 \dots s_i \dots)$ polynomial if $\exists\, m \geq 0, \; s_i = 0, \; \forall\, i > m$

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 σ of degree $m \leq n$, τ degree n

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

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

$\sigma + \tau \in R[x]$ 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

$$f(x) = s_0 + s_1 x + s_2 x^2 + \dots + s_n x^n$$

Definition 21. 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

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

$k[x]$ 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" comparision: if

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

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

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

(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

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

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

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

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 $g - qf \in k[x]$ $\forall q \in k[x]$
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,

$$\text{LT} : k[x] \to k[x]$$
$$\text{LT}(f) = s_n x^n$$

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

$h = 0$ or deg$(h) <$ deg(r)

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

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

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

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

$$\Longrightarrow \text{deg}(r) < \text{deg}(f)$$

□

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,

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

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

common divisor is $c(x) \in k[x]$ s.t. $\begin{array}{l} c(x)|f(x) \\ c(x)|g(x) \end{array}$

If $f(x), g(x) \in k[x]$, $\begin{array}{l} f \neq 0, \\ g \neq 0 \end{array}$
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 23. if A, R (commutative) rings, (ring) homomorphism is
$f : A \to R$ 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 $f : A \to R$

Example 3.40

(i)
(ii)
(iii)
(iv) R commutative ring, $a \in R$. Define
evaluation homomorphism
$e_a : R[x] \to R$
$e_a(f(x)) = f(a)$ 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 24. **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

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

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 $f : A \to R$ ring homomorphism,*
then $\ker f$ ideal in A
$\operatorname{im} f$ subring of R

if $A, R \neq$ 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.

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

$\ker f$ 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
$f(1) = 1 \in \operatorname{im} f$

if $\begin{array}{l} c = f(a) \\ d = f(b) \end{array}$ i.e. $c, d \in \operatorname{im} f$, $c + d = f(a + b)$

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

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

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

$\operatorname{im} f$ a subring

$\square$

Definition 25. 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 $\varphi : A \to R$ isomorphism, $\psi : R \to A$ its inverse.
$a = \psi(\varphi(a))$ so $\forall\, a \in \mathrm{im}\psi$, ψ surjective.
Suppose $\psi(r) = \psi(s)$

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

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

$a = b$ so $r = s$ by φ. ψ injective.
ψ bijective. ψ isomorphism.
(ii)
(iii)

Exercise 3.41.

Suppose $I \bigcap J = 0$

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 26. 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.
$$a^{2^{n-1}} = 1,\ bab^{-1} = a^{-1} \text{ and } b^2 = a^{2^{n-2}}$$

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

$$\forall \text{ group } G, \forall\, f : X \to G, \exists!\text{ homomorphism } \begin{aligned} &\varphi : F \to G \\ &\varphi(x) = f(x)\, \forall\, x \in X \end{aligned}$$

$$\begin{tikzcd} F \arrow[dr, dashed, "\varphi"] & \\ X \arrow[u, "i \equiv \text{inclusion}"] \arrow[r, "f"'] & G \end{tikzcd}$$

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 $T : V \to W$, s.t. $T(v_i) = u_i \quad \forall\, i$

$$\begin{tikzcd} V \arrow[dr, dashed, "T"] & \\ X \arrow[u] \arrow[r, "f"'] & W \end{tikzcd}$$

Definition 28. if X subset of group F,
then F free group with basis X if

$$\forall \text{ group } G, \forall\, f : X \to G, \exists!\text{ homomorphism } \begin{aligned} &\varphi : F \to G \\ &\varphi(x) = f(x) \quad \forall\, x \in X \end{aligned}$$

Definition 29. 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 $a \in X \bigcup X^{-1}$
deletion of a subword of w of form aa^{-1}, changing $w = Aaa^{-1}B \mapsto AB$

Definition 30. $w \to w'$ 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
$$u = w_1 \to w_2 \to \cdots \to w_n = v$$
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 31. **semigroup** is set having associative operation.
monoid is semigroup S having identity q.
homomorphism (semigroups) $f : S \to S'$ s.t. $f(xy) = f(x)f(y)$
homomorphism (monoids) $f : S \to S'$ 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 $f : X_1 \to X_2$, then $\exists$ isomorphism $\varphi : F_1 \to F_2$.*
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 $f : X \to G$ (e.g. take X underlying set of G, and $f = 1_G$).
Let F free group with basis X.

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

$$\begin{tikzcd} F \arrow[dr, dashed, "\varphi"] & \\ X \arrow[u, "i"] \arrow[r, "f"] & G \end{tikzcd}$$

φ surjective because f i.e.

$$\begin{tikzcd} {[x_i]} \arrow[dr, dashed, "\varphi"] & \\ x_i \arrow[u, "i"] \arrow[r, "f"] & f(x_i) = g_i = \varphi([x_i]) \end{tikzcd}$$

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

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

□

Definition 32. **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 33. 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 34. R-module is (additive) abelian group M,

equipped with scalar multiplication
$$\begin{aligned} R \times M &\to M \\ (r,m) &\mapsto rm \end{aligned}$$

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

(i) $r(m + m') = rm + rm'$
(ii) $(r + r')m = rm + r'm$
(iii) $(rr')m = r(r'm)$
(iv) $1m = m$

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
$$\begin{aligned} \mathbb{Z} \times M &\to M \\ (r,m) &\mapsto rm \equiv m^r \end{aligned}$$
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
$$\begin{aligned} R \times R &\to R \\ (a,b) &\mapsto ab \end{aligned}$$
For reference, recall some of the properties of a commutative ring:
$$\begin{aligned} & ab = ba \\ & a(bc) = (ab)c \\ & 1a = a \\ & a(b + c) = ab + ac \end{aligned}$$
$\forall$ ideal I in R is an R-module,

for if $\begin{matrix} i \in I \\ r \in R \end{matrix}$, then $ri \in I$.
$0 \in I$
$\forall\, a, b \in I$, $a + b \in I$
If $a \in I$, $r \in R$, then $ra \in I$.
(iv)

(v) Let linear $T : V \to V$, V finite-dim. vector space over field k.
Recall $k[x] \equiv$ set of polynomials with coefficients in k.

Define $\begin{aligned} & k[x] \times V \to V \\ & f(x)v = \left(\sum_{i=0}^m c_i x^i \right) v = \sum_{i=0}^m c_i T^i(v) \end{aligned} \quad \forall\, f(x) = \sum_{i=0}^m c_i x^i \in k[x]$

$\Longrightarrow$ denote $k[x]$-module V^T.

Special case: Let $A \in \text{Mat}_k(n,n)$, let linear $\begin{aligned} & T : k^n \to k^n. \\ & T(w) = Aw \end{aligned}$

vector space k^n is $k[x]$-module if we define scalar multiplication $\begin{aligned} & k[x] \times k^n \to k^n \\ & f(x)w = \left(\sum_{i=0}^m c_i x^i \right) w = \sum_{i=0}^m c_i A^i w \end{aligned} \quad \forall\, f(x) = \sum_{i=0}^m c_i x^i \in k[x]$

In $(k^n)^T$, $xw = T(w)$
In $(k^n)^A$, $xw = Ax$
$T(w) = Ax$ and so $(k^n)^T = (k^n)^A$ (EY : 20151015 because of induction?)

Definition 35. if ring R, R-modules M, N, then function $f : M \to N$ 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 $T : V \to V$, 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.

Define $\begin{aligned} & \varphi : V \to k^n \\ & \varphi(v_i) = e_i \end{aligned}$

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

$\Longrightarrow \varphi(xv) = x\varphi(v) \quad \forall\, v \in V$
By induction on $\deg(f)$, $\varphi(f(x)v) = f(x)\varphi(v) \quad \forall\, f(x) \in k[x] \quad \forall\, v \in V$
$\Longrightarrow \varphi$ is $k[x]$-map
$\Longrightarrow \varphi$ is $k[x]$-isomorphism of V^T and $(k^n)^A$.

Proposition 16 (7.3)**.** *Let vector space over field k, V, let linear $T, S : V \to V$*
Then $k[x]$-modules V^T, V^S are $k[x]$-isomorphic iff $\exists$ vector space isomorphism $\varphi : V \to V$ s.t. $S = \varphi T \varphi^{-1}$.

Proof. If $\varphi : V^T \to V^S$ 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 $\varphi(xv) = x\varphi(v)$

$$\begin{aligned} xv &= T(v) \\ x\varphi(v) &= S(\varphi(v)) \\ \Longrightarrow \varphi \circ T(v) &= S \circ \varphi(v) \Longrightarrow \varphi \circ T = S \circ \varphi \end{aligned}$$

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

Conversely, if given isomorphism $\varphi : V \to V$ 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 36. 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, $\forall\, w \in W$, $xw = T(w) \in W \Longrightarrow T(W) \subseteq W$
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 $c_i T^i(w) \in W$ □

$\Longrightarrow$ **invariant subspace** W, is submodule W of V^T s.t. $T(W) \subseteq W$

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

then $\exists$ R-isomorphism $\begin{aligned} & \varphi : M/kerf \to imf \\ & \varphi : m + kerf \mapsto f(m) \end{aligned}$

Proof. Let $[m] \in M/\text{ker}f$
$\varphi([m]) = f(m)$

Now

$$\begin{aligned} \varphi^{-1} &: \text{im}f \to M/\text{ker}f \\ \varphi^{-1} &: y = f(m) \mapsto [m] \end{aligned}$$

and φ^{-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

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

□

Another look at this theorem:

Theorem 16 (1st Isomorphism Theorem (Modules) Thm. 7.8 of Rotman (201) [1]). *If $f : M \to N$ is R-map of modules, then $\exists$ R-isomorphism s.t.*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & N \\ M/kerf \arrow[ur, "\varphi = \cong"'] & \end{tikzcd}$$

$$\begin{aligned} &\varphi : M/kerf \to imf \\ &\varphi : m + kerf \mapsto f(m) \end{aligned} \tag{1}$$

Proof. View M, N as abelian groups.

Recall natural map $\pi : M \to M/N$
$m \mapsto m + N$

Define φ s.t. $\varphi\pi = f$.

(φ well-defined). Let $m + \ker f = m' + \ker f$, $m, m' \in M$, then $\exists\, n \in \ker f$ s.t. $m = m' + n$.

$$\varphi(m + \ker f) = \varphi\pi(m) = f(m) = f(m' + n) = f(m') + f(n) = \varphi\pi(m') + 0 = \varphi(m' + \ker f)$$

$\Longrightarrow \varphi$ well-defined.

(φ surjective). Clearly, $\operatorname{im}\varphi \subseteq \operatorname{im} f$.
Let $y \in \operatorname{im} f$. So $\exists\, m \in M$ s.t. $y = f(m)$. $f(m) = \varphi\pi(m) = \varphi(m + \ker f) = y$. So $y \in \operatorname{im}\varphi$. $\operatorname{im} f \subseteq \operatorname{im}\varphi$.
$\Longrightarrow \varphi$ surjective.

(φ injective) If $\varphi(a + \ker f) = \varphi(b + \ker f)$, then

$$\varphi\pi(a) = \varphi\pi(b) \text{ or } f(a) = f(b) \text{ or } 0 = f(a) - f(b) = f(a-b) \text{ so } a - b \in \ker f (a-b) + \ker f = \ker f \text{ so } a + \ker f = b + \ker f$$

φ isomorphism.

φ R-map. $\varphi(r(m+N)) = \varphi(rm + N) = f(rm)$.
Since f R-map, $f(rm) = rf(m) = r\varphi(m+N)$. φ is R-map indeed.

□

Theorem 17 (2nd Isomorphism Theorem (Modules) Thm. 7.9 of Rotman (2011) [1]). *If S, T are submodules of module M, i.e. $S, T \in M$, then $\exists$ $R-$isomorphism*

$$\begin{tikzcd} S \arrow[r, "h"] \arrow[d, "\pi|_S"] & (S+T)/T = imh \\ S/(S\cap T) = S/kerh \arrow[ur, "\cong"'] & \end{tikzcd}$$

$$S/(S \cap T) \to (S+T)/T \tag{2}$$

Proof. Let natural map $\pi : M \to M/T$.
So $\ker \pi = T$.

Define $h := \pi|_S$, so $h : S \to M/T$, so $\ker h = S \cap T$,

$$(S+T)/T = \{(s+t) + T | a \in S + T, s \in S, t \in T\}$$

i.e. $(S+T)/T$ consists of all those cosets in M/T having a representation in S.

By 1st. isomorphism theorem,

$$S/S \cap T \xrightarrow{\cong} (S+T)/T$$

□

Theorem 18 (3rd Isomorphism Theorem (Modules) Thm. 7.10 of Rotman (2011) [1]). *If $T \subseteq S \subseteq M$ is a tower of submodules, then $\exists$ R-isomorphism*

$$\begin{tikzcd} M/T \arrow[r, "g"] \arrow[d, "\pi"] & M/S \\ (M/T)/(S/T) = (M/T)/kerg \arrow[ur, "\cong"'] & \end{tikzcd}$$

$$(M/T)/(S/T) \to M/S \tag{3}$$

Proof. Define $g : M/T \to M/S$ to be **coset enlargement**, i.e.

$$g : M + T \mapsto m + S \tag{4}$$

g well-defined: if $m + T = m' + T$, then $m - m' \in T \subseteq S$, and $m + S = m' + S \Longrightarrow g(m+T) = g(m'+T)$

$\ker g = S/T$ since

$$\begin{aligned} &g(s+T) = s + S = S \qquad (S/T \subseteq \ker g) \\ &g(m+T) = m + S = 0 = S = s + S, \text{ so } m = s \Longrightarrow \ker g \subseteq S/T \end{aligned}$$

$\operatorname{im} g = M/S$ since

$$\begin{aligned} &g(m+T) = m + S \Longrightarrow \operatorname{im} g \subseteq M/S \\ &m + S = g(m+T) \end{aligned}$$

Then by 1st isomorphism, and commutative diagram, done. □

Definition 37. exact sequence if $\operatorname{im} f_{n+1} = \ker f_n \quad \forall\, n$, for sequence of R-maps (i.e. homomorphisms linear in R) and R-modules

$$\dots \to M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \to \dots$$

Proposition 17 (7.20). *(i) $0 \to A \xrightarrow{f} B$ exact iff f injective*
(ii) $B \xrightarrow{g} C \to 0$ exact iff g surjective
(iii) $0 \to A \xrightarrow{h} B \to 0$ exact iff h isomorphism

Proof. (i) $\text{im}(0 \to A) = 0$ if assume $0 \to A \xrightarrow{f} B$ exact, $\ker f = 0$, and so f injective
Conversely, if f injective, $\ker f = 0$ and $\text{im}(0 \to A) = 0 = \ker f$. So sequence is exact.
(ii) $\ker(C \to 0) = C$
if $B \xrightarrow{g} C \to 0$ exact, $\text{im}g = C$ and so g surjective.
Conversely, given $g : B \to C$,
$\exists$ exact sequence $B \xrightarrow{g} C \to C/\text{im}g$ (cf. Exercise 7.13) since

$$\ker(C \to C/\text{im}g) = \text{im}g$$

if g surjective, $\text{im}g = C$, and so $B \xrightarrow{g} C \to 0$ exact.
(iii) from (i), $0 \to A \xrightarrow{h} B$ exact iff h injective
from (ii), $A \xrightarrow{h} B \to 0$ exact iff h surjective.
$\implies h$ isomorphism iff $0 \to A \xrightarrow{h} B \to 0$

Definition 38. short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact sequence.

Proposition 18 (7.21). *(i) If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ short exact sequence, then $A \cong \text{im}f$ and $B/\text{im}f \cong C$*
(ii)

Proof. (i) f injective, so $A \to \text{im}f$ isomorphism.
By first isomorphism thm., $B/\ker g \cong \text{im}g$.
$\text{im}g = C$ since g surjective
$\text{im}f = \ker g$ by exactness.
$\implies B/\text{im}f \cong C$
(ii)

Definition 39. short exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ *split* if $\exists$ map $j : C \to B$, s.t. $pj = 1_C$

Proposition 19 (7.22). *if exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ 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 $C = \text{im}p$
Thus $B = \text{im}i + \text{im}j$

If $ia = x = jc$, then $p(x) = pia = 0$, since $pi = 0$ for $\text{im}i = \ker p$
$px = pjc = c$ since $pj = 1_C$.
Thus $x = jc = j(0) = 0$.
So $B \cong A \oplus C$ □

Exercises.

Definition 40. If $f : M \to N$, define **cokernel**, denoted $\text{coker}f$,

$$\text{coker}f := N/\text{im}f \tag{5}$$

Exercise 7.13.

(i) if $f : M \to N$ 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, $f : M \to N$ surjective iff $\text{coker}f = 0$
(ii) If $f : M \to N$,
$\ker(\ker f \to M) = 0 = \text{im}(0 \to \ker f)$ since $\ker f \to M$ is inclusion
$\text{im}(\ker f \to M) = \ker f$ (by inclusion)
$\ker(N \to \text{coker}f) = \ker(N \to N/\text{im}f) = \text{im}f$
$\text{im}(N \to \text{coker}f) = \text{coker}f$
$\ker(\text{coker}f \to 0) = \text{coker}f \implies \text{im}(N \to \text{coker}f) = \ker(\text{coker}f \to 0)$

Exercise 7.17.

If given a short exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ that splits, then $B \cong A \oplus C$, i.e. $B = \text{im}i \oplus \text{im}j$ where $j : C \to B$ 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:

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

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 $\exists\, q : B \to A$ with $qi = 1_A$,

Thus,

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

$$
\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "1"] & B \arrow[r, "p"] \arrow[l, bend left, "q"] \arrow[d, "{(q,p)}"] & C \arrow[r] \arrow[d, "1"] & 0 \\
0 \arrow[r] & A \arrow[r, "{(1, p\circ i)}"'] & A \oplus C \arrow[r] & C \arrow[r] & 0
\end{tikzcd}
$$

$$
\begin{tikzcd}
0 \arrow[r, mapsto] & a \arrow[r, mapsto, "i"] \arrow[d, mapsto, "1"] & i(a) = b \arrow[r, mapsto, "p"] \arrow[l, bend left, mapsto, "q"] \arrow[d, mapsto, "{(q,p)}"] & pi(a) = 0 = p(b) \arrow[r, mapsto] \arrow[d, mapsto, "1"] & 0 \\
0 \arrow[r, mapsto] & a \arrow[r, mapsto, "{(1, p\circ i)}"'] & (q(b), p(b)) = (a, c) \arrow[r, mapsto] & p(b) \arrow[r, mapsto] & 0
\end{tikzcd}
$$

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

Let bijections $\alpha : A \to A'$, $\quad \alpha : a \mapsto (a,1)$, denote $A' \bigcup B' \equiv A \coprod B$.
$\beta : B \to B' \quad \beta : b \mapsto (b,2)$

From Rotman, pp. 447,

Definition 41. coproduct $A \coprod B \equiv C \in \text{Obj}(\mathcal{C})$

In my notation,

coproduct

$$
\begin{gathered}
(\mu_1, A_1 \coprod A_2) \\
(\mu_2, A_1 \coprod A_2)
\end{gathered} \tag{6}
$$

where injection (morphisms)

$$
\begin{gathered}
\mu_1 : A_1 \to A_1 \coprod A_2 \\
\mu_2 : A_1 \to A_1 \coprod A_2
\end{gathered} \tag{7}
$$

s.t.

$$\forall A \in \text{Obj}\mathbf{A}, \forall f_1, f_2 \in \text{Mor}\mathbf{A} \text{ s.t. } \begin{aligned} f_1 &: A_1 \to A \\ f_2 &: A_2 \to A \end{aligned}$$

then

$$
\begin{gathered}
\exists ! [f_i] \equiv [f_1, f_2] \in \text{Mor}\mathbf{A},\ [f_1, f_2] : A_1 \coprod A_2 \to A \text{ s.t.} \\
[f_1, f_2]\mu_1 = f_1 \\
[f_1, f_2]\mu_2 = f_2
\end{gathered} \tag{8}
$$

i.e.

$$
\begin{tikzcd}
 & & A \\
A_1 \arrow[urr, "f_1"] \arrow[rr, "\mu_1"] & & A_1 \coprod A_2 \arrow[u, dashed, "{[f_1, f_2]}"'] \\
A_2 \arrow[uurr, "f_2"] \arrow[urr, "\mu_2"'] & &
\end{tikzcd} \tag{9}
$$

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) $\mu_j : A_j \to \coprod_{i \in I} A_i$

s.t.

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

then

$$
\begin{gathered}
\exists ! [f_i] \equiv [f_i]_{i \in I} \in \text{Mor}\mathbf{A},\ [f_i] : \coprod_{i \in I} A_i \to A \text{ s.t.} \\
[f_i]\mu_j = f_j \qquad \forall j \in I
\end{gathered} \tag{10}
$$

i.e.

$$
\begin{tikzcd}
 & A \\
A_j \arrow[ur, "f_j"] \arrow[r, "\mu_j"'] & \coprod_{i \in I} A_i \arrow[u, dashed, "{[f_i]}"']
\end{tikzcd} \tag{11}
$$

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 19 (7.32, Rotman)**.** *Let commutative ring R.*
$\forall$ R-module A, $\forall$ family $\{B_i | i \in I\}$ of R-modules,

$$\mathit{Hom}_R(A, \prod_{i\in I} B_i) \simeq \prod_{i\in I} \mathit{Hom}_R(A, B_i) \tag{12}$$

via R-isomorphism

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

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

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

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

φ 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 Obj_R**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 φ is R-map.

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

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 $_R$**Mod**),
By def. or product, $\exists\,!$ R-map , $\theta : A \to \prod_{i\in I} B_i$ s.t. $p_i\theta = f_i \quad \forall\, i$

$$\begin{tikzcd} & A \arrow[dl, "f_i"'] \arrow[d, dashed, "\theta"] \\ B_i & \prod_{i\in I} B_i \arrow[l, "p_i"] \end{tikzcd}$$

Then

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

, and so φ *surjective*.

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

$$\begin{tikzcd} & A \arrow[dl, "0"'] \arrow[d, "f"] \\ B_i & \prod_{i\in I} B_i \arrow[l, "p_i"] \end{tikzcd}$$

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

8. Algebras

8.1. Noncommutative Rings.

Definition 42. left R-module, for ring R, is (additive) abelian group M, equipped with scalar multiplication

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned} \tag{13}$$

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 43. right R-module, for ring R, (additive) abelian group M, equipped with scalar multiplication.

$$\begin{aligned} M \times R &\to M \\ (m, r) &\mapsto mr \end{aligned} \tag{14}$$

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 $_RM$
right R-module M_R

Example 8.7.

Definition 44. If M is left R-module, then R-map

$$f : M \to M \tag{15}$$

is an R-**endomorphism** of M

Definition 45. Endomorphism ring $\mathrm{End}_R(M)$

$$\mathrm{End}_R(M) := \{R - \text{endomorphisms of } M\} \tag{16}$$

as a set,

$$\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M) \tag{17}$$

Definition 46. representation of ring R is ring homomorphism σ

$$\sigma : R \to \mathrm{End}_{\mathbb{Z}}(M) \tag{18}$$

where M is an abelian group

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

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

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

Define scalar multiplication
$$R \times M \to M$$
$$rm = \sigma_r(m) \qquad \forall\, m \in M$$

Indeed,
$$r(m + m') = \sigma_r(m + m') = \sigma_r m + \sigma_r m' = rm + rm'$$
$$(r + r')m = \sigma_{(r+r')}m = \sigma(r + r')m = (\sigma(r) + \sigma(r'))m = \sigma(r)m + \sigma(r')m = \sigma_r m + \sigma_{r'} m = rm + r'm$$
$$(rr')m = \sigma_{rr'}m = \sigma(rr')m = \sigma(r)\sigma(r')m = \sigma_r(\sigma_{r'}m) = r(r'm)$$
$$1m = \sigma_1 m = \sigma(1)m = m$$

Assume M left R-module.
If $r \in R$, then $m \mapsto rm$ defines endomorphism $T_r : M \to M$
$$\sigma : R \to \text{End}_{\mathbb{Z}}(M)$$
$$\sigma : r \mapsto T_r$$
$$\sigma(rr')m = T_{rr'}m = (r + r')m = T_r(T_{r'}m) = \sigma(r)\sigma(r')m$$
$$\sigma(r + r')m = T_{r+r'}m = (r + r')m = (T_r + T_{r'})m = \sigma(r)m + \sigma(r')m$$

So σ is a homomorphism. □

8.2. Chain Conditions.

Definition 47. 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 $f : R \to S$ is
k-**algebra** map if
$$f(ar) = af(r) \quad \forall\, a \in k, \forall\, r \in R$$

8.3. Semisimple Rings.

Definition 48. k-**representation** of group G is homomorphism
$$\sigma : G \to GL(V)$$
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 49. 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 $\begin{array}{l} x \in A^p \\ y \in A^q \end{array}$, then $xy \in A^{p+q}$, i.e. $A^p A^q \subseteq A^{p+q}$

$x \in A^p$ 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 $A = R[x_1, x_2, \ldots x_n]$ is graded R-algebra if we define
$$A^p = \{r x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n} | r \in R \text{ and } \sum e_i = p\}$$
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