MTH 310: Abstract Algebra - Notes

Debayan Deb

Spring 2015

Chapter 1

Review

1.1 Statements and Logic

A statement is a sentence which is either true or false.
For example,

- i. $\sqrt{2}$ is a rational number (False)
- ii. Exactly 1323 bald eagle were born in 2000 B.C. (Not a statement)
- iii. π is a real number (True)

Let P and Q be statements. The corresponding truth table with various operators looks like:

P	Q	P*and*Q
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	P*or*Q
T	T	T
T	F	T
F	T	T
F	F	F

P	*notP*
T	F
F	T

P	Q	P $\Longrightarrow$ Q
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	Q *or not* P
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	P $\Longleftrightarrow$ Q
T	T	T
T	F	F
F	T	F
F	F	T

P	Q	*not* Q $\Longrightarrow$ *not* P
T	T	T
T	F	F
F	T	T
F	F	T

P $\Longleftrightarrow$ Q means that P is true if and only if Q is true.
As we see from the tables above, P $\Longrightarrow$ Q $\Longleftrightarrow$ not Q $\Longrightarrow$ not P.
Also ((P and Q) or R) $\Longleftrightarrow$ ((P or R) and (Q or R)).

Theorem 1.1.1. *(Principal Substitution) Let $\Phi(x)$ be a formula involving a variable x. For an object d, let $\Phi(d)$ be the formula obtained from $\Phi(x)$ by replacing all occurances of x by d. If a and b are objects with $a = b$, then $\Phi(a) = \Phi(b)$. $\Phi(x)$ is then known as a well-defined function.*

1.2 Sets

A set is a collection of objects.
For example,
The set of integers $\mathbb{Z}$:= $\{..., -2, -1, 0, 1, 2, ...\}$.

1.4 Mathematical Induction

Theorem 1.4.1. *(Principal os Mathematical Induction) Suppose that for each $n \in \mathbb{N}$, a statement P(n) is given and that*
(i) P(0) is true.
(ii) If P(k) is true for some $k \in \mathbb{N}$, then P(k+1) is also true.
Then P(n) is true $\forall n \in \mathbb{N}$.

1.5 Equivalence Relation

Definition 1.5.1. Let $\sim$ be a relation on a set A (that is a relation from A and A). Then
(a) $\sim$ is called reflexive if a$\sim$a $\forall$a $\in$ A
(b) $\sim$ is called symmetric if b$\sim$a $\forall$a,b $\in$ A with a$\sim$b, i.e. a$\sim$b $\iff$ b$\sim$a
(c) $\sim$ is called transitive if a$\sim$c $\forall$a,b,c $\in$ A with a$\sim$b and b$\sim$c, i.e. (a$\sim$b) and (b$\sim$c) $\implies$ a$\sim$c
$\sim$ is called an equivalence relation if $\sim$ is reflexive, symmetric and transitive.

Examples:
(1) Consider the relation "$\leq$" on the real numbers.
Not symmetric because 1$\leq$2 but 2$\not\leq$1 and hence, "$\leq$" is not an equivalence relation.

(2) Consider the relation "=" on the real numbers.
"=" is an equivalence relation because it is reflexive, symmetric and transitive.

(3) Consider the relation "r$\sim$s if |r| = |s|".
"r$\sim$s if |r| = |s|" is an equivalence relation because it is reflexive, symmetric and transitive

Let a $\in \mathbb{Z}$. Then $[a]_n$ is the equivalence class with respect to "$\equiv$(mod n)".
Consider the relation "$\equiv$(mod 2)":

$$[1]_2 = \{b \in \mathbb{Z} \mid 1 \equiv b(mod2)\}$$
$$= \{b \in \mathbb{Z} \mid b\ is\ odd\}$$
$$[0]_2 = \{b \in \mathbb{Z} \mid 0 \equiv b(mod2)\}$$
$$= \{b \in \mathbb{Z} \mid b\ is\ even\}$$

Consider the relation "≡(mod 5)":

$$
\begin{aligned}
[0]_5 &= \{5k \mid k \in \mathbb{Z}\} \\
&= \{..., -10, -5, 0, 5, 10, ...\} \\
[1]_5 &= \{5k+1 \mid k \in \mathbb{Z}\} \\
&= \{..., -9, -4, 1, 6, 11, ...\} \\
[2]_5 &= \{5k+2 \mid k \in \mathbb{Z}\} \\
&= \{..., -8, -3, 2, 7, 12, ...\} \\
[3]_5 &= \{5k+3 \mid k \in \mathbb{Z}\} \\
&= \{..., -7, -2, 3, 8, 13, ...\} \\
[4]_5 &= \{5k+4 \mid k \in \mathbb{Z}\} \\
&= \{..., -6, -1, 4, 9, 14, ...\}
\end{aligned}
$$

Let $\sim$ be an equivalence relation on the set A and $a, b \in A$. The the following statements are equivalent:

(a) a∼b
(b) b∈[a]
(c) [a]∩[b]≠ ϕ
(d) [a]=[b]
(e) a∈[b]
(f) b∼a
where [a]:= $\{b \in A \mid a \sim b\}$

Proof. 1. (a) $\Longrightarrow$ (b). Suppose that a∼b. Since, [a]:= $\{b \in A \mid a \sim b\}$ $\Longrightarrow$ b ∈[a].

2. (b) $\Longrightarrow$ (c). Suppose that b∈[a]. Since, $\sim$ is reflexive, b∼b. So, b∈[b]. Thus, b∈ $[a] \cap [b]$. Therefore, [a]∩[b]≠ ϕ.

3. (c) $\Longrightarrow$ (d). Suppose that [a]∩[b]≠ ϕ, then ∃c such that c∈[a]∩[b]. Let d∈[a]. Then, a∼d and since, c∈[a], a∼c, and also, c∼a. So, by transitivity, c∼d, we know that c∈[b] $\Longrightarrow$ c∼b $\Longrightarrow$ d∈[b] $\Longrightarrow$ [a]⊆[b].

4. (d) $\Longrightarrow$ (e). Suppose that [a]=[b]. Since, a is reflexive, a∼a, so a∈[a]. Since, [a] = [b], a∈[b].

5. (e) $\Longrightarrow$ (f). Suppose a∈[b]. Also, [b]:= $\{e \in A \mid b \sim e\}$. So, b∼a.

6. (f) $\Longrightarrow$ (a) by symmetricity. □

Chapter 3

Rings

3.1 Definitions and Examples of Rings

Definition 3.1.1. A ring is a triple (R, +, *) such that

(i) R is a set

(ii) '+' is a function (called Ring Addition) and RxR is a subset of the domain of "+". For (a,b)∈RxR, a+b denotes the image of (a,b) under '+'

(iii) '*' is a function (called Ring Multiplication) and RxR is a subset of the domain of "*". For (a,b)∈RxR, a*b (and also ab) denotes the image of (a,b) under '*'

and such that the following axioms hold:

(Ax1) a+b∈R for all a,b∈R (closure of addition)

(Ax2) a+(b+c) = (a+b)+c for all a,b,c∈R (associative addition)

(Ax3) a+b = b+a for all a,b∈R (commutative addition)

(Ax4) ∃ an element in R, denoted by 0_R(called the zero-R) such that a = a + 0_R and a = 0_R + a for all a∈R (additive identity)

(Ax5) For each a∈R, there exists an element in R, denoted by -a (negative a) such that a + (-a) = 0_R (additive inverse)

(Ax6) ab∈R for all a,b∈R (closure of multiplication)

(Ax7) a(bc) = (ab)c for all a,b,c∈R (associative multiplication)

(Ax8) a(b+c) = ab + bc for all a,b,c∈R (distributive laws)

Examples:

($\mathbb{Q}$,+,*) is a ring

($\mathbb{N}$,+,*) is a not ring as it does not have 0_R

($M_2(\mathbb{R})$,+,*) is a ring, where $M_2(\mathbb{R})$ is a 2x2 matrix over $\mathbb{R}$

Definition 3.1.2. Let R be a ring. Then R is called commutative if

(Ax9) ab = ba for all a,b∈R (commutative multiplication)

Definition 3.1.3. Let R be a ring. We say that R is a ring with identity if ∃

an element, denoted by 1_R(called one-R) such that
(Ax10) a = 1_R*a = a*1_R for all a∈R. (multiplicative identity)

Examples:
(a) (ℤ,+,*) is a commutative ring with identity.
(b) (ℚ,+,*) is a commutative ring with identity.
(c) (ℂ,+,*) is a commutative ring with identity.
(d) (ℝ,+,*) is a commutative ring with identity.
(e) Let 2ℤ be the set of even integers. Then (2ℤ,+,*) is a commutative ring without identity.
(f) Let n∈ ℤ and n >1. The set M_n(ℝ of nxn matrices with real coefficients together with the usual addition and multiplication of matrices is a **non-commutative ring with identity**.

Definition 3.1.4. An **integral domain** is a commutative ring R with identity $1_R \neq 0_R$ that satisfies:
(Ax11) whenever a,b∈R and ab=0_R, then a=0_R or b=0_R.

Example: (ℤ,+,*) is an integral domain

Definition 3.1.5. A **field** is a commutative ring R with identity $1_R \neq 0_R$ that satisfies:
(Ax12) for each a≠ 0_R in R, the equation ax=1_R has a solution in R.

Example: (ℝ,+,*) is a field.

Theorem 3.1.1. *Let R and S be rings. Define addition and multiplication on the Cartesian product RxS = $\{(r,s) \mid r \in R, s \in S\}$ by*
(r,s) + (r',s') = (r+r',s+s') and
(r,s)(r',s') = (rr',ss')
for all r,r'∈R, s,s'∈S. Then,
1. *RxS is a ring.*
2. *0_{RxS} = (0_R,0_S).*
3. *-(r,s) = (-r,-s) for all r∈R, s∈S*
4. *if R and S are both commutative, then so is RxS.*
5. *if R and S both have an identity, then RxS has an identity and 1_{RxS} = (1_R,1_S).*

Subrings

If R is a ring and S is a subset of R, then S may or may not be a ring under the operations in R.
In the ring ℤ of integers, for example, the set of even numbers is a ring, but the set of off numbers is not.

Definition 3.1.6. When a subset of a ring R is itself a ring under the addition and multiplication in R, then we sat that S is a **subring** of R.

Example:
(a) $\mathbb{Z}$ is a subring of ring $\mathbb{Q}$
(b) $\mathbb{Q}$ is a subring of ring $\mathbb{R}$
(c) Since $\mathbb{Q}$ is itself a field, $\mathbb{Q}$ is a **subfield** of ring $\mathbb{R}$

Theorem 3.1.2. *Suppose that R is a ring and that S is a subset of R, such that*
(i) S is closed under addition (if $a,b \in S$, then $a+b \in S$)
(ii) S is closed under multiplication (if $a,b \in S$, then $ab \in S$)
(iii) $0_R \in S$
(iv) If $a \in S$, then the solution of the equation $a + x = 0_R$ is in S. Then S is a subring of R.

3.2 Basic Properties of Rings

Theorem 3.2.1. *For any element in a ring R, the equation* $a + x = 0_R$ *has a unique solution.*

Proof. We know that a + x = 0_R has at least one solution, say *u*, by Axiom 5. If "*v*" is also a solution then a + v = 0_R and a + u = 0_R, so that
v = 0_R + v = (a + u) + v = (u + a) + v = u + (a + v) = u + 0_R = u.
So, v = u and u is the only solution. □

-a is the unique element in R such that a + (-a) = (-a) + a = 0_R.

Theorem 3.2.2. *If a + b = a + c in a ring R, then b = c.*

Proof. Adding -a to both sides of a + b = a + c and then associativity and negatives, we see that
-a + (a + b) = -a + (a + c)
(-a + a) + b = (-a + a) + c
0_R + b = 0_R + c
b = c □

Theorem 3.2.3. *For any elements a and b or a ring R,*
(1) $a*0_R = 0_R$
(2) a(-b) = -(ab) = (-a)b*
(3) -(a+b) = (-a)+(-b)
(4) -(a-b) = -(a) + b
(5) (-a)(-b) = ab
(6) $(-1_R)*a = -a$

Proof. (1) Since $0_R + 0_R = 0_R$ and $a*(0_R + 0_R) = a*0_R + a*0_R$,
$a*(0_R + 0_R) = a*0_R + 0_R$.
From Theorem 3.2.2, if $a*0_R + a*0_R = a*0_R + 0_R$, then $a*0_R = 0_R$.

(2) By definition, -(ab) is the unique solution of the equation
ab + x = 0_R, and so any other solution of this equation must be equal to -(ab). But x = a(-b) is a solution because, by distributive law and (1),
ab + a(-b) = a[b + (-b)] = a[0_R] = 0_R.
Therefore, a(-b) = -(ab).
The rest of the parts are proved in similar fashion.

(3) By definition, -(a+b) is the unique solution of (a+b) + x = 0_R,
but (-a) + (-b) is also a solution:
(a+b) + [(-a) + (-b)] = b + [a + (-a)] + (-b) = (b + 0_R) + (-b) = b + (-b) = 0_R.
Therefore, by uniqueness, -(a+b) = (-a) + (-b).

(4) By definition, -(a - b) = -(a + (-b)) and by (4) and -(-a) = a,
-(a-b) = -(a + (-b)) = (-a) + (-(-b)) = (-a) + b.

(5) By -(-a) = a and repeated use of (2),
(-a)(-b) = -[a(-b)] = -[-(ab)] = ab.

(6) By (2),
(-1_R)*a = -(1_R*a) = -(a) = -a. □

Definition 3.2.1. An element a in a ring R with identity is called a **unit** if $\exists u \in R$: au = 1_R = ua. In this case, the element u is called the **multiplicative inverse** of a and is denoted by a^{-1}.

Example:
(1) In $\mathbb{Q}$: All numbers are units
(2) In $\mathbb{Z}$: -1 and 1 are the only units

Theorem 3.2.4. *Every field F is an integral domain if a field is a commutative ring with* 1_R.

Proof. $\forall a \in F, a^{-1}$ exists. We need to show that if ab = 0_R, then either a = 0_R or b = 0_R.
Let ab = 0_R. We know that a^{-1} exists. So, (a^{-1})(ab) = (a^{-1}a)b = 1_Rb = b. But, (a^{-1})(ab) = (a^{-1})*0_R = 0_R. So, b = 0_R. □

Definition 3.2.2. An element a in a ring R is a **zero divisor** if
(1) a$\neq 0_R$
(2) $\exists b \neq 0_R, b \in R$: $ab = 0_R$ *or* $ba = 0_R$.

Finding units in $\mathbb{Z}_{12}$ trick:
If greatest-common-divisor(a,12) = 1, then a is a unit,
else if greatest-common-divisor(a,12) >1, then a is a zero divisor.

Theorem 3.2.5. *Every finite integral domain R is a field.*

Proof. Since R is a commutative ring with identity 1_R, we only need to show $\forall a \neq 0_R$, the equation ax = 1_R has a solution.

Let $a_1, a_2, ..., a_n$ be the elements of R. Suppose $a_t \neq 0_R$. Then, $a_ta_1, a_ta_2, ..., a_ta_n$ is also R. If $a_i \neq a_j$, then we must have $a_ta_i \neq a_ta_j$ (because if $a_ta_i = a_ta_j \implies a_i = a_j$. ($a_ta_i - a_ta_j = 0_R, a_t(a_i - a_j) = 0_R \implies a_t = 0_R$ *or* $a_i = a_j$, *but* $a_t \neq 0_R$, *so* $a_i = a_j$).
Therefore, $a_ta_1, a_ta_2, ..., a_ta_n$ are n distinct elements of R. However, R has exactly n elements all together, and so these must be all the elements of R in some order. For some j, $a_ta_j = 1_R$. Therefore, ax = 1_R has a solution and R is a field. □

Sample Exercise: Let R be a ring such that $x^2 = x \ \forall x \in R$. Prove that R is commutative.
Solution:

We have to show that xy = yx $\forall x, y \in R$
$x^2 = x$
x + x = 2x
$(x + x)^2$ = $(2x)^2$ = $4x^2$ = 4x
However, $(2x)^2$ = 2x. So, 2x = 4x $\implies$ 2x = 0_R.

$(x + y)^2$ = x + y
$\implies$ x^2 + y^2 + xy + yx = x + y
$\implies$ x + y + xy + yx = x + y
$\implies$ xy + yx = 0_R
$\implies$ xy + yx - 2(xy) = 0_R
$\implies$ yx = xy

3.3 Isomorphisms and Homomorphisms

Definition 3.3.1. A ring R is **isomorphic** to a ring S (denoted by R≅S) if there is a function f:R→S such that

(i) f is injective

(ii) f is surjective

(iii) f(a+b) = f(a) + f(b) and f(ab) = f(a)f(b) $\forall a, b \in R$ The function f is called an isomorphism.

Definition 3.3.2. Let R and S be rings. A function f:R→S is said to be homomorphic if

f(a+b) = f(a) + f(b) and f(ab) = f(a)f(b) $\forall a, b \in R$

Hence, every isomorphism is a homomorphism.

Theorem 3.3.1. *Let f:R→S be a homomorphism of rings. Then*

(1) f(0_R) = 0_S

(2) f(-a) = -f(a) $\forall a \in R$

(3) f(a-b) = f(a) - f(b) $\forall a, b \in R$

If R is a ring with identity, and f is surjective then

(4) S is a ring with identity and f(1_R) = 1_S

(5) whenever there is a unit in R, then f(u) is a unit in S and f(u^{-1}) = $(f(u))^{-1}$.

Proof. (1) $\forall a \in R,\ a + 0_R = a$.

f(a + 0_R) = f(a) + f(0_R) (by homomorphism)

$\implies$ f(a) = f(a) + f(0_R). So, f(0_R) is the addition identity in S.

(2) f(a) + f(-a) = f(a-a) (by homomorphism)

= f(0_R) = 0_S.

Since, f(a)∈S, which is also a ring, f(a) has an additive inverse such that f(a) + (-f(a)) = 0_S. Hence, f(-a) = -f(a).

(3) f(a + (-b)) = f(a) + f(-b) = f(a) - f(b) (by (2))

(4) $\forall a \in R$, f(a) = f(a*1_R) = f(a)*f(1_R) (by homomorphism)

Then f(1_R) is the multiplicative identity in S and f(1_R) = 1_S.

(5) Since u is a unit in R, $\exists v \in R$ such that uv = 1_R = vu.

Hence by (4),

f(u)f(v) = f(uv) = f(1_R) = 1_S.

Similarly, vu = 1_R implies that f(v)f(u) = 1_S.

Therefore, f(u) is a unit in S where $(f(u))^{-1}$ = f(v).

Since, v = u^{-1}, $(f(u))^{-1}$ = f(u^{-1}). □

Corollary 3.3.1.1. If f:R→S is a homomorphism of rings, then the image of f is a subring of S.

Proof. We need to check if f(R) is a subring.
(Subring Ax3) $0_R \in S$
f(0_R) = 0_S. Hence, $0_S \in f(R)$
(Subring Ax1) f(a+b) = f(a) + f(b), where f(a)∈f(R) and f(b)∈f(R) (by homomorphism)
(Subring Ax2) f(ab) = f(a)f(b), where f(a)∈f(R) and f(b)∈f(R) (by homomorphism)
(Subring Ax4) Addition inverse holds by Theorem 3.3.1 (2)
Hence, f(R) is a subring. □

Questions:-
(1) Does homomorphism exist between $\mathbb{Q}$ *and* $\mathbb{Z}$?
Answer: $\mathbb{Q}$ has infinitely many units whereas $\mathbb{Z}$ has only two units: -1, 1. So no homomorphism exists.

(2) Prove $\mathbb{Z}_{12} \xrightarrow{f} \mathbb{Z}_3\ x\ \mathbb{Z}_4$.
Answer:
Identity of $\mathbb{Z}_{12}$ = 1
Identity of $\mathbb{Z}_3\ x\ \mathbb{Z}_4$ = (1,1)
Hence, f(1) = (1,1)
f(2) = f(1 + 1) = f(1) + f(1) = (1,1) + (1,1) = (2,2)
f(3) = (0,3)
f(4) = (1,0)
f(5) = (2,1)
f(6) = (0,2)
f(7) = (1,3)
f(8) = (2,0)
f(9) = (0,1)
f(10) = (1,2)
f(11) = (2,3)
f(0) = (0,0)
Hence, f is Injective and Surjective.
f(a+b) = f(a) + f(b)
f($[a]_{12} + [b]_{12}$) = f($[a+b]_{12}$) = ($[a+b]_3$,$[a+b]_4$) = ($[a]_3 + [b]_3, [a]_4 + [b]_4$) = ($[a]_3, [a]_4$)+($[b]_3, [b]_4$) = f($[a]_{12}$) + f($[b]_{12}$)
Hence, f is isomorphic.

Question: For $\mathbb{Z}_4$ and $\mathbb{Z}_2\ x\ \mathbb{Z}_2$, check if isomorphic.
Answer:
Cardinality is the same.
f(1) = (1,1) (identity maps to identity)
f(1 + 1) = (0,0)
f(0) = (0,0) = f(2).
f is not injective so no isomorphic.

Question: For $\mathbb{Z}_8$ and $\mathbb{Z}_2$ x $\mathbb{Z}_4$, check if isomorphic.
Answer:
Cardinality is the same.
f(1) = (1,1) f(1 + 1) = (0,2)
f(4) = (0,0) = f(0).
f is not injective so no isomorphic.

Trick: $\mathbb{Z}_{m*n} \cong \mathbb{Z}_m \ x \ \mathbb{Z}_n \iff$ greatest-common-divisor(n,m) = 1 (i.e. m and n are relatively prime).

Theorem 3.3.2. *Suppose R is a commutative ring and f:R→S is an isomorphism. Then, S is also a commutative ring.*

Proof. $\forall a, b \in R$, ab = ba. f(ab) = f(a)f(b). Also, f(ba) = f(b)f(a). So, f(ab) = f(ba). Hence, S is commutative. Furthermore, by surjective property for any c,d in S, we can always find two elements a and b such that f(a) = c and f(b) = d. For any two elements in S, show that cd = dc, i.e. show whether f(ab) = f(a)f(b) = f(b)f(a) = f(ba) where a≠b.
Since ab = ba, S is commutative. □

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\} \ncong \mathbb{R}^4 \text{ because } \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$$
is non-commutative and $\mathbb{R}^4$ is commutative.

Checking for isomorphism:
(1) Cardinality
(2) Both commutative
(3) Add several times until 0 is achieved.