Algebra 1

MAT-2001/CS-2250-1
Monsoon 2023

Kahaan Shah

November 28, 2023

Contents

Chapter 1

Introduction

Lecture 1

1.1 Integer, Groups and Abstraction

29 Aug. 10:10

1.1.1 Integers

We have $\mathbb{Z} = \{\cdots -3, -2, -1, 0, 1, 2, 3 \dots\}$. So integers is a non-empty set. We can add integer, subtract integers, multiply (not always divide). Other than division the other operations give an integer. These are called *binary operations*. Note that we can do multiplication and subtraction with addition as well. Some other things to note:

1. Addition is closed.
2. Addition is associative and commutative
3. 0 is an identity element
4. Every element has an additive inverse

Why isn't commutativity included?

We also have odd integers $= \{\cdots -5, -3, -1, 1, 3, 5 \dots\}$ and $2\mathbb{Z} = \{\dots 4, -2, 0, 2, 4 \dots\}$ (even integers). We can also consider $3\mathbb{Z}$ similarly.

1.1.2 Groups

Let us now try to abstract the above properties

Definition 1.1.1 (Group). A group is a non-empty set equipped with a binary operation $\circ_G$ satisfying the following properties:

1. **Closure:** If $a, b \in G$; then $a \circ_G b \in G$
2. **Associativity:** If $a, b, c \in G$; then $a \circ_G (b \circ_G c) = (a \circ_G b) \circ_G c$
3. **Identity:** $\exists$ a unique element $e \in G$ s.t. $\forall a \in G, a \circ_G e = e \circ_G a = a$
4. **Inverses:** Every element in $a \in G$ has an inverse $\overline{a} \in G$ s.t. $a \circ_G \overline{a} = e$ and also $\overline{a} \circ_G a = e$

Example. Examples of groups:

- $\mathbb{Z}, +$
- $\mathbb{R}, +$
- $\mathbb{R} \setminus \{0\}, \times$
- $\mathbb{R}^n, +$

- Trivial group: $G = \{e\}, e \circ_G e = e$
- $G = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix}; a, b, c, d \in \mathbb{Z}, +\}$. Then the additive inverse is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$. The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. This is written as $(M_2(\mathbb{Z}), +)$ and also holds for $(M_n(\mathbb{Z}), +)$.
- $2\mathbb{Z}, +$, we can also see this holds for $n\mathbb{Z}, +$. If $n = 0$ then we have the trivial group.

Definition 1.1.2 (Subgroup). A subgroup $(H, \circ_G)$ for a group $(G, \circ_G)$ is a non-empty subset of G that forms a group under $\circ_G$.

Example. G is a subgroup of itself

How to make a mathematician angry!

Remark. Every group other than the trivial group has at least 2 subgroups:

1. The group itself
2. The trivial group (take the identity of the group)

Example. Consider $\mathbb{Z}/n\mathbb{Z} \coloneqq \{$Set of remainders we obtain when dividing by $n \in \mathbb{N}\}$ $= \{\overline{0}, \overline{1}, \overline{2}, \dots \overline{n-1}\}$ where when $n = 5$ we have $\overline{0} = \{\dots, -25, -20, -15, -10, -5, 0, 5, 10, \dots\}$ and so on. So we can write $\mathbb{Z}_5 = \{\overline{0} \dots \overline{5}\}$. Now consider the operation $+_5$ for $\mathbb{Z}/5\mathbb{Z}$:

$+_5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Table 1.1: $+_5$ results

Lecture 2

31 Aug. 10:10

Example. Continuing from Table 1.1. We have law of addition defined as $\overline{a} +_5 \overline{b} = \overline{(a+b)}$. So $\overline{a_1} = \overline{a_2} \Leftrightarrow a_1 - a_2$ is divisible by 5. We also have $\overline{a} + \overline{0} = \overline{a}$. Each element also has an inverse: $\overline{0} = -\overline{0}$, $\overline{-1} = \overline{4}$ and so on.

Example. Fix a symbol a. With set $G \coloneqq \{1, a, a^2, a^3, a^4\}$. Let us define $\times_5$ as $a^{n_1} \times_5 a^{n_2} = a^{n_1+n_2}$ and $a^5 = 1$. Table for this looks the same as Table 1.1.

This and the previous group are isomorphic

.

Example. For $X^n - 1 = 0$ the roots are $\omega_n^1, \omega_n^2 \dots \omega_n^n (= 1)$ where $\omega_n = e^{\frac{2\pi i}{n}}$. Since $\omega_n^n = 1$ the multiplication of these numbers would be the same as the previous example for ω_5.

Chapter 2

Groups

2.1 Basic Properties

Definition 2.1.1 (Order). We say that group G has order n if the underlying set has cardinality n and we denote it by $|G|$. $|G|$ can also be ∞.

Example.

- $|\mathbb{Z}|n\mathbb{Z}| = 5$
- The examples above were **cyclic groups of order 5**.
- Similarly we can have cyclic groups of order n.

Definition 2.1.2 (Abelian Groups). A group G is called **abelian** (or also commutative) if the underlying group operation is commutative i.e. $\forall a, b \in G, a \circ_G b = b \circ_g a$.

Example. Consider the 2×2 matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{22} \end{bmatrix}$ then BA would be a 2×1 matrix. Consider the set $S = \{2 \times 2\}$ matrices. If B were also 2×2 then AB and BA are both 2×2 matrices. But $AB \neq BA$ in general. This multiplication is associative and we have $I = \begin{bmatrix} 1 & 0 \\ 0 & 1\mathbb{S} \end{bmatrix}$ since $AI = IA = A, \forall 2 \times 2$ matrices. There is also no inverse in general. We have $A^{-1} \coloneqq \frac{1}{\det(A)} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} = \frac{adj(A)}{\det(A)}$ and if A^{-1} exists then $AA^{-1} = A^{-1}A = I$. Now let us define $S \coloneqq \{2 \times 2\text{matrices with non-zero determinant}\}$. Since $\det(AB) = \det(A)\det(B) \Rightarrow AB \in S$. This set is called $GL_2(\mathbb{R}) \coloneqq \{A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}; a_{ij} \in \mathbb{R}, \det(A) \neq 0\}$. This group is non-abelian. We can say that all $GL_n(\mathbb{R})$ are groups over matrix multiplication.

Note. If G is a group and $a, b \in G$ then we use the notation $ab = a \circ_G b$. So under this associativity is $a(bc) = (ab)c$. Using induction we can show that associativity $\Rightarrow (a_1 \dots a_n) = (a_1 \dots a_i)(a_{i+1} \dots a_n) \forall i < n$.

Theorem 2.1.1. The identity element of a group is unique. If $e, e' \in G$ are identity elements then $e = e'$.

Theorem 2.1.2. The inverse of an element is unique. So $b'a = e = ab \Rightarrow b' = b$.

Remark. From this it follows that $(a_1 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$

Lecture 3

5 Sep. 10:10

Lemma 2.1.1 (Left inverse = right inverse)**.** Let G be a group and $a, b, b' \in G$ s.t. $ab = e = b'a$. Then $b = b'$.

Proof.

$$\begin{aligned} b &= eb \\ &= (b'a)b \\ &= b'(ab) && \text{(by associativity)} \\ b &= b' \end{aligned}$$

■

Theorem 2.1.3 (Cancellation Law)**.** If $ab, b, c \in G$ and if $ab = ac$ then $b = c$

Proof. If $ab = ac$ then by multiplying on the left $a^{-1}(ab) = a^{-1}(ac)$ so $b = c$. ■

Definition 2.1.3 (Conjugates)**.** In a group G two elements b and c are said to be **conjugates** if $\exists a \in G$ s.t. $aba^{-1} = c$.

2.2 Cyclic Groups

Definition 2.2.1 (Order of elements)**.** An element $g \in G$ is said to have order n if n is the least natural number such that $g \cdot g \cdot \dots \cdot g = e$.

Remark. Order of e is always 1

Example. Consider a cyclic group of order 5. $C_5 = \{1, a, a^2, a^3, a^4\}$. The order of a is 5 ($a \cdot a \cdot a \cdot a \cdot a = 1$). Order of a^2 is also 5. In fact all elements except 1 have order 5.

Example. Consider $G = (\mathbb{Z}, +)$. We know that $|Z| = \infty$. Order of 0 is 1. We say that the order of any other n is ∞.

Example. Cyclic group of order 6 (C_6). We see that order of a is 6, order of a^2 is 3, order of a^3 is 2, order of a^4 is 3 and order of a^5 is 6. Now considering the subgroups of C_6:

1. Trivial: $\{e\}$
2. C_6 itself
3. $H_1 = \{1(= a^{6k}), a^2, a^4\}$
4. $H_2 = \{1(= a^{6k}), a^3\}$

Definition 2.2.2 (Generated subgroups $\langle A \rangle$)**.** Let G be a group and let A be a subset of G. Then we denote by $\langle A \rangle$ to be the smallest subgroup that contains the set A. This is called the subgroup **generated** by A.

Remark. We measure size by inclusions, so if $H_1 \subset H_2$ then H_1 is smaller than H_2.

Example. Continuing from above $\langle 1 \rangle = \{1\}$. Similarly $\langle a \rangle = C_6$, $\langle a^2 \rangle = H_1$, $\langle a^3 \rangle = H_2$, $\langle a^4 \rangle = H_1$ and $\langle a_5 \rangle = C_6$.

Theorem 2.2.1. All subgroups of $(\mathbb{Z}, +)$ are of the form $(n\mathbb{Z}, +)$.

Example. Consider $G = (\mathbb{Z}, +)$. Recall that $n\mathbb{Z} \subset \mathbb{Z}, \forall n \in \mathbb{Z} \geq 1$. We have $\langle 0 \rangle =$ trivial group. We also have $\langle z \rangle = z\mathbb{Z}$.

Definition 2.2.3 (Generator Element). Let G be a group. We say that an element $g \in G$ generates the group or is a generator of the group if $\langle g \rangle = G$.

Example. We have a and a^5 as the generators of C_6.

Remark. C_p has no non-trivial subgroups $\forall p$ s.t. p is prime.

Theorem 2.2.2 (Generators of C_n). Number of generators $C_n = \phi(n)$ (where $\phi(n)$ is the cardinality of natural numbers $< n$ co-prime to n).

Lecture 4

7 Sep. 10:10

Definition 2.2.4 (Cyclic Group). A group C is called cyclic if it can be generated by a single element $c \in C$. This means $C = \langle c \rangle$.

Example. Note that these groups do not need to be of finite order. For example $(\mathbb{Z}, +)$ is an infinite cyclic group since $\langle 1 \rangle = \mathbb{Z}$. The group $C_2 = 1, -1$ is also cyclic since $\langle -1 \rangle = C_2$.

Corollary 2.2.1. Every subgroup of a cyclic group is also cyclic.

Remark. A group G will always have a generating set $\langle G \rangle = G$. If the generating set is a single element then the group is cyclic.

Definition 2.2.5 (Smallest Subgroup). Let $A \subset G$ be a subset of G. Then the group generated by the set A $\langle A \rangle$ is the smallest (under set inclusion) subgroup that contains the set A.

Proposition 2.2.1. Every cyclic group is abelian.

Proof. We have $C = \{\ldots, g^{-2}, g^{-1}e, g, g^2 \ldots\}$ and we can see that $g^a g^b = g^{a+b} = g^b g^a$. ■

But not every abelian group is cyclic.

2.3 Symmetric/Permutation Groups

Definition 2.3.1 (Symmetric Group). Consider a finite set Ω where $S_\Omega = \{$set of all bijections $\tau : \Omega \to \Omega\}$. For the set $\Omega_n = \{1 \ldots n\}$ we have $|S_n| = n!$. We can see that S_n is a non-abelian group over $\circ$. Here S_n is a symmetric group.

Definition 2.3.2 (Cyclic decomposition of elements of S_n). A cycle is a string of integers which represents an element of S_n which cyclically permutes the integers. We write this as $\tau = (a_1 \dots a_m), m \leq n$ which maps $a_1 \to a_2$, $a_2 \to a_3$ and so on until $a_m \to a_1$. We then have $a_{m+1} \to a_{m+1}$ up to $a_n \to a_n$.

Example. If $n = 13$ and we have $\sigma \in S_{13}$. Say we have $\sigma(1) = 12, \sigma(2) = 13, \sigma(3) = 3, \sigma(4) = 1, \sigma(5) = 11, \sigma(6) = 9, \sigma(7) = 5, \sigma(8) = 10, \sigma(9) = 6, \sigma(10) = 4, \sigma(11) = 7, \sigma(12) = 8, \sigma(13) = 2$. We can also write $\sigma = (1, 12, 8, 10, 4)(2, 13)(3)(5, 11, 7)(6, 9)$ which is the cyclic decomposition.

Example. Consider S_3 the set of all permutations of the set $\{1, 2, 3\}$. We have $|S_3| = 6$ and its elements are as follows:

1. $e = (1)(2)(3)$
2. $\tau_1 = (1, 2, 3)$
3. $\tau_2 = (2, 3)$
4. $\tau_3 = (1, 3)$
5. $\tau_4 = (2, 1)$
6. $\tau_5 = (1, 3, 2)$

For example we now have $\tau_3 \circ \tau_4 = (123) = \tau_1$ and $\tau_4 \circ \tau_3 = (132) \neq \tau_1$. So the group is not abelian.

Remark. The order of the group is equal to the LCM of the number of elements in each cycle of the cyclic decomposition of the group.

Lecture 5

2.4 Homomorphisms

12 Sep. 10:10

Definition 2.4.1 (Homomorphism). Let $(G_1, \circ_{G_1})$ and $(G_2, \circ_{G_2})$ be two groups. A homomorphism from G_1 to G_2 is a map $\varphi : G_1 \to G_2$ such that $\forall a, b \in G_1$ we have $\varphi(a \circ_{G_1} b) = \varphi(a) \circ_{G_2} \varphi(b)$.

Example. Consider $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ where $\varphi(a) = a + 5$. If φ is a homomorphism then $\varphi(a + b) = \varphi(a) + \varphi(b)$. But we have $a + b + 5 \neq a + b + 10$. So this is not a homomorphism.

Example. Consider $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ where $\varphi(a) = na$. Now φ is a homomorphism since $n(a + b) = na + nb$.

Example. Consider $\varphi : GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ where $\varphi(\mathbf{A}) = \det(\mathbf{A})$. This is a homomorphism since matrix multiplication preserves determinant multiplication ($\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B})$).

Example. Consider $\varphi : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \times)$ where $x \mapsto e^x$. This is a homomorphism since $e^{x+y} = e^x e^y$.

Example. Consider $\varphi : (\mathbb{R}, \times) \to (\mathbb{R}, +)$ where $x \mapsto \log(x)$. This is a homomorphism since $\log(xy) = \log(x) + \log(y)$.

Proposition 2.4.1. Let $\varphi : G_1 \to G_2$ be a group homomorphism then

1. If $a_1 \dots a_k \in G_1$ then $\varphi(a_1 \dots a_k) = \varphi(a_1) \dots \varphi(a_k)$.
2. $\varphi(e_{G_1}) = e_{G_2}$
3. $\varphi(a^{-1}) = \varphi(a)^{-1}$

Proof.

1. Follows from induction.
2. Proof by contradiction. Assume $\varphi(e_1) \neq e_2$ then $\varphi(e_1, a) = \varphi(e_1)\varphi(a)$ so $\varphi(a) = \varphi(e_1)\varphi(a)$. But $\varphi(e_1) \neq \varphi(e_2) \Rightarrow \varphi(a) \neq \varphi(a)$ which is a contradiction.
3. We have $\varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$. From part 2 we have $\varphi(e_1) = e_2 = \varphi(a)\varphi(a^{-1})$ therefore $\varphi(a^{-1}) = [\varphi(a)]^{-1}$

■

Definition 2.4.2 (Image of a homomorphism). $\operatorname{Im}\varphi = \{x \in G_2 | x = \varphi(a) \text{ for some } a \in G_1\} \subset G_2$

In modern notation $\subset \equiv \subseteq$

Proposition 2.4.2. If $x \in \operatorname{Im}(\varphi)$ then $x^{-1} \in \operatorname{Im}(\varphi)$

Proof. $\varphi(a^{-1}) = [\varphi(a)]^{-1} = x^{-1} \in \operatorname{Im}(\varphi)$ ■

Proposition 2.4.3. $\operatorname{Im}(\varphi) \subset G_2$ is a subgroup.

Definition 2.4.3 (Kernel of Homomorphism). $\ker\varphi = \{a \in G_1 | \varphi(a) = e_2\} \subset G_1$.

Proposition 2.4.4. $\ker\varphi$ is non-empty.

Proof. We always have $e_1 \in \ker\varphi$ ■

Proposition 2.4.5. Suppose $a \in \ker\varphi$ then $a^{-1} \in \varphi$.

Proof. Since $\varphi(a) = e_2$ and $\varphi(a^{-1}) = \varphi(a)^{-1} = e_2^{-1} = e_2$ we have $a^{-1} \in \ker\varphi$ ■

Example. Consider the earlier homomorphism for $GL_2(\mathbb{R})$ where $\mathbf{A} \mapsto \det(\mathbf{A})$. We have $\ker\varphi = \{\mathbf{A} | \det(\mathbf{A}) = 1\}$.

Proposition 2.4.6. $\ker\varphi \subset G_1$ is a subgroup.

Definition 2.4.4 (Left coset). Suppose $H \subset G$ is a subgroup and $a \in G$ then $\{ah_1, ah_2, ah_2\}, h_1, h_2, h_3, \dots \in H$ is called a left coset and denoted by $aH := \{g \in G | g = ah \text{ for some } h \in H\}$.

Proposition 2.4.7. The following are equivalent:

1. If $\varphi(a) = \varphi(b)$ for some $a, b \in G_1$
2. $a^{-1}b \in \ker\varphi$

3. a is in the coset b $\ker\varphi$

4. The cosets $b\ker\varphi = a\ker\varphi$

Proof. Suppose $\varphi(a) = \varphi(b)$. Then we have $\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = [\varphi(a)]^{-1}\varphi(b) = \varphi(b)^{-1}\varphi(b) = e_2$. Therefore we have $1 \Rightarrow 2$.

If $\varphi(a^{-1}b) \in \ker\varphi$ then $\varphi(a^{-1}b) = e_2$, so $\varphi(a^{-1})\varphi(b) = e_2$ and $[\varphi(a)]^{-1}b = e_2$ therefore $\varphi(b) = \varphi(a)$. Therefore $2 \Rightarrow 1$. ■

Remark. φ is one to one (as a map) if $\varphi(a) = \phi(b) \Rightarrow a = b$. We have shown that if φ is a group homomorphism then $\varphi(a) = \varphi(b) \Leftrightarrow a^{-1}b \in \ker\varphi$.

Corollary 2.4.1. A group homomorphism is injective if and only if $\ker\varphi = \{e_1\}$

Lecture 6

14 Sep. 10:10

Definition 2.4.5 (Conjugate). If $a, g \in G$ then the element gag^{-1} is called the conjugate of a by g

Definition 2.4.6 (Normal Subgroup). A subgroup $N \subset G$ is called a normal subgroup if $\forall a \in N$ and $\forall g \in G$ the conjugate $gag^{-1} \in N$. We write this as $N \trianglelefteq G$

Proposition 2.4.8. If $\varphi : G \to G'$ then $\ker\varphi \trianglelefteq G$ is a normal subgroup of G.

Proof. Let $a \in \ker\varphi \subset G$. Let $g \in G$ be any element. To check that $gag^{-1} \in \ker\varphi$ lets compute $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g)e'\varphi(g)^{-1} = e'$, therefore $gag^{-1} \in \ker\varphi$ and $\ker\varphi \trianglelefteq G$. ■

Proposition 2.4.9. If G is an abelian group then any subgroup H is normal in G.

Proof. If G is abelian then $\forall a \in H, \forall g \in G$ we have $gag^{-1} = gg^{-1}a = a \in H$, therefore $H \trianglelefteq G$. ■

Definition 2.4.7 (Centre of a group). The centre of a group $Z(G)$ is the set of elements of G that commute with every element in $G\ldots$. So $Z(G) = \{z \in G | zx = xz, \forall x \in G\}$.

Example. Consider $GL_2(\mathbb{R})$ and $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ and $B \in GL_2(\mathbb{R})$ then $AB = BA, \forall B \in GL_2(\mathbb{R})$.

Remark. We always have $e \in Z(G)$.

Remark. If $z \in Z(G)$ then $z^{-1} \in Z(G)$ (multiply on left and right by z^{-1}).

Proposition 2.4.10. if $z_1, z_2 \in Z(G)$ then $zz^{-1} \in G$. This also shows that $Z(G)$ is a subgroup of G. In fact $Z(G) \trianglelefteq G$. $Z(G)$ is an abelian subgroup.

Definition 2.4.8 (Isomorphism). A homomorphism $\varphi : G \to G'$ is called an isomorphism if φ is a bijection. Written as $G \cong G'$

Remark. If φ is an isomorphism we have $\ker\varphi = \{e_1\}$ and $\operatorname{Im}\varphi = G'$.

Lemma 2.4.1. $\varphi : G \to G'$ is an isomorphism if and only if $\varphi^{-1} : G' \to G$ is also an isomorphism.

Definition 2.4.9 (Automorphism). An isomorphism $\phi : G \to G$ from the group to itself is called an automorphism.

Example. The identity map is an automorphism.

Example. The map $\varphi_a : G \to G, \forall a \in G$ where $\varphi_a(g) = aga^{-1}$ is an automorphism.

Example. Consider the map $G \to G$ where $g \mapsto e$. This is not an automorphism since it is a bijection.

Example. Consider $\varphi : G \to G$ where $\varphi(g) = g^{-1}$. This map is a bijection since every element has a unique inverse. However it is not a homomorphism since $\varphi(g_1g_2) = g_2^{-1}g_1^{-1} = \varphi(g_2)\varphi(g_1)$. However if G is abelian then it is an automorphism.

Definition 2.4.10 (Left cosets). Let G be a group and $H \subset G$. Fix an element $a \in G$, the left coset of H in G with regards to a is the set $aH := \{ah | \forall h \in H\}$

Lecture 7

19 Sep. 10:10

Proof. Continuing the proof of Proposition 2.4.7.

We have $a^{-1}b \in \ker\varphi \Rightarrow a^{-1}b = k$ such that $k \in \ker;\varphi$. Therefore $b^{-1}a = k^{-1}$. So $a = bk^{-1}$ therefore $a \in b\ker;\varphi$. So we have $2 \Rightarrow 3$.

If $a \in b\ker\varphi$ then $a\ker\varphi \subset b\ker\varphi$ since we have $a = bk^{-1}$ therefore $ak_1 = b(k^{-1}k_1)$. Similarly we can show that $b\ker\varphi \subset a\ker\varphi$ therefore $a\ker\varphi = b\ker\varphi$ and $3 \Rightarrow 4$.

If we have $a\ker\varphi = b\ker\varphi$ then $\ker\varphi = a^{-1}b\ker\varphi$. Since $\forall k_i \in \ker\varphi a^{-1}bk_i = k_j$ for some $k_j \in \ker\varphi$ then $a^{-1}b = k_jk_i^{-1} \in \ker\varphi$. Therefore $4 \Rightarrow 2$.

■

2.5 Equivalence relations and equivalence classes

Definition 2.5.1 (Equivalence Relation). Let S be a non-empty set. And equivalence relation on a st S is a relation that holds between certain pairs of elements of S. We usually denote this by $a \sim b$. An equivalence relation is required to be:

- **Transitive:** If $a \sim b$ and $b \sim c$ then $a \sim c$.
- **Symmetric:** $a \sim b \Rightarrow b \sim a$.
- **Reflexive:** $a \sim a$

Example. Consider the sets of odd numbers and even numbers. If $a, b \in \{\text{Odd Numbers}\}$ then $2|a-b$. So we can say $a \sim b$ if $2|a-b$ is an equivalence relation.

Example. Consider the set of all triangles. $\Delta_1 \sim \Delta_2$ if Δ_1 and Δ_2 are congruent. This is an equivalence relation.

Example. Consider group G. Let us define a relationship on the elements of the group as follows: $a \sim b$ if a is a conjugate of b i.e. $b = gag^{-1}$ for some $g \in G$. Checkig the axioms:

- $a \sim a$ since $a = eae^{-1}$.
- $a \sim b \Rightarrow b = gag^{-1} \Rightarrow a = g^{-1}bg = a \Rightarrow b \sim a$.
- If $a \sim b$ and $b \sim c$ then $c = (g_2g_1)a(g_2g_1)^{-1}$ so $a \sim c$.

Definition 2.5.2 (Equivalence Class). Consider set S with equivalence relation $\sim$. $\forall a \in S$ I have an equivalence class $C_a \coloneqq \{b | b \in S, a \sim b\}$

Remark. $a \in C_a$ so $C_a \neq \phi$

Lemma 2.5.1. Given a equivalence relation $\sim$ on a set S, the equivalence classes partition the set S. Suppose $C_a \cap C_b \neq \phi$ then $C_a = C_b$.

Proof. Let $d \in C_a \cap C_b$. We have $d \in C_a \Rightarrow a \sim d$. But we also have $d \in C_b \Rightarrow b \sim d \Rightarrow a \sim b$ by transitivity. So $b \in C_a$. Therefore $C_b \subset C_a$ by repeated application of transitivity. Simlarly $Ca \subset C_b$ so we have $C_a = C_b$. ■

Example. We have the sets $C_0 \dots C_4$ where $C_i \coloneqq \{b \in \mathbb{Z} | b \equiv i \mod 5\}$.

Lecture 8

Suppose S is a set and $\sim$ is an equivalence relation. Then recall that the equivalence classes for this relation C_a partition the set S. Let us now build a new set defined $\overline{S} \coloneqq \{C_{a_1}, C_{a_2} \dots\}$ such that C_{a_i} are distinct. We will now denote C_a by $\overline{a}$. So now set $\overline{S} = \{\overline{a}_1, \overline{a}_2 \dots\}$. 21 Sep. 10:10

Definition 2.5.3 (Projection). The projection $\Pi : S \to \overline{S}$ such that $a \mapsto \overline{a}$.

Example. $S = (\mathbb{Z}, +)$ with $\sim$ odd or even $(a - b \mod 2 = 0)$. So we have $\overline{S} = \{\overline{0}, \overline{1}\}$.

Consider G a group and $H \subset G$ a subgroup.

Lemma 2.5.2. Cosets give an equivalence relation.

Proof. We define a relation on the set of elements of the group G as follows. $a \sim b$ if $b = ah$ for some $h \in H$ (same as saying $b \in aH$). It is reflexive since $a = ae$. Symmetric by multiplying with inverse and transitive from Proposition 2.4.7 part 3 and 4. ■

Remark. The set of distinct left cosets will be the equivalence classes.

Example. Let $G = (\mathbb{Z}, +)$ and $H = 5\mathbb{Z}$. The left cosets of this are of the form $a + 5\mathbb{Z}$ where $0 \leq a \leq 4$. We have the equivalence relation $a \sim b$ if $b = a + 5\mathbb{Z} \Leftrightarrow b - a \in 5\mathbb{Z}$.

Corollary 2.5.1. The distinct left cosets of a subgroup H of a group G partition the group.

Proof. Distinct left cosets are equivalence classes. ■

Proposition 2.5.1. The following are equivalent:

1. $b = ah$ for some $h \in H$
2. $a^{-1}b \in H$
3. $b \in aH$ (left coset)
4. The left cosets aH and bH are equal

Remark. If we set $H = \{e\}$ then the set of left cosets is a bijection with G.

Lemma 2.5.3. All distinct left cosets aH have the same order.

Proof. We can define a bijection between aH and H, since we cn take $ah_i \mapsto h_i$. ■

Corollary 2.5.2. All left cosets have the same cardinality as the subgroup H itself.

Definition 2.5.4 (Index)**.** The number of distinct left cosets of a subgroup H is called the index of H in G written as $[G : H]$.

Lemma 2.5.4. $|G| = [G : H]|H|$.

Proof. So we have $G = \sqcup_{a \in G} aH$ and $|G| = \sum_{a \in G} |aH| = \sum_{a \in G} |H|$ (all of this is up to distinct cosets). ■

Corollary 2.5.3 (Lagrange's Theorem)**.** If $H \subset G$ then $|H| \mid |G|$

Corollary 2.5.4. Every group of prime order have no proper subgroups (only have trivial subgroup and the group itself).

Corollary 2.5.5. $O(a) \mid |G| \forall a \in G$.

Proof. Let G be any finite group and $a \in G; a \neq e$. We have $\langle a \rangle = \{e, a, a^2, \ldots, a^{O(a)-1}\}$. We have $|\langle a \rangle| = O(a)$. ■

Theorem 2.5.1. If $|G|$ is prime then G is a cyclic group and each non-trivial element is a generator. So if $O(G) = p \Rightarrow G \cong C_p$ where $O(a) = p, \forall a \in G \neq e$.

Lecture 9

2.6 Right Cosets

26 Sep. 10:10

Definition 2.6.1 (Right Coset)**.** Let G be a group and H be a subgroup then the right cosets of H in G are defined as $Hg = \{hg | h \in H\} \forall g \in G$.

Remark. Similar to left cosets, right cosets also give an equivalence relation on the group G via the relation $a \sim b$ if $b = ha$ for some $h \in H$.

Proposition 2.6.1. Let H be subgroup of G then the following are equivalent:

1. $H \trianglelefteq G$, i.e. $\forall h \in H$, $\forall g \in G$, $ghg^{-1} \in H$.
2. $\forall g \in G$, $gHg^{-1} = H$
3. $\forall g \in G$, $gH = Hg$
4. Every left coset of H in G is a right coset (Every $kH = Hl$ for some $k, l \in G$).

Proof. Since $H \trianglelefteq G$ we know that $ghg^{-1} \in H \forall h \in H$. So we have $gHg^{-1} \subset H$. This is true $\forall g \in G$ and therefore true for g^{-1}. By multiplying on left and right we get $H \subset gHg^{-1}$. Therefore $H = gHg^{-1}$ and $1 \Rightarrow 2$.

Since every element $ghg^{-1} \in H \forall h \in H, \forall g \in G$ so by definition $H \trianglelefteq G$. So $2 \Rightarrow 1$

We have $gHg^{-1} = H$ If we multiply on the right we get $gHg^{-1}g = Hg$ so $gH = Hg$. So $2 \Rightarrow 3$.

We have $gH = Hg$. So multiplying on the right by g^{-1} we get $gHg^{-1} = H$ so $3 \Rightarrow 2$.

We have $gH = Hg$, so obviously every left coset is a right coset so $3 \Rightarrow 4$.

$G = \sqcup_{k \in H} kH = \sqcup_{l \in H} Hl$. Every kH intersects trivially with a right coset Hl or it equals a right coset Hl. Now consider $kH \cap Hk$. Since $k \in kH$ and $k \in Hk$ the intersection is not trivial and $kH = Hk$. So we have $4 \Rightarrow 3$. ■

Remark. The main upshot is that if $H \trianglelefteq G$ then $gH = Hg$.

2.7 Quotient Groups

Proposition 2.7.1. If $H \subset G$ and $g \in G$ then gHg^{-1} is also a subgroup of G.

Theorem 2.7.1 (Unique Subgroup). If $H \subset G$ is a unique subgroup of order r then $H \trianglelefteq G$

Proof. We know that $|H| = |gHg^{-1}|$. But H is the unique subgroup so $H = gHg^{-1} \Rightarrow H \trianglelefteq G$ ■

Lecture 10

28 Sep. 10:10

Example. Consider S_3 which has order 6. Let $H = \{e, (1,2)\}$. We can check that H is not normal since we have $g = (1,2,3)$ since we have $(1,2,3) \circ (1,2) \circ (1,2,3) = (13) \notin H$. So H is not normal but gHg^{-1} is still a subgroup.

Theorem 2.7.2 (Index and normal subgroups). Let $H \subset G$ be a subgroup of index 2. Then H is necessarily normal.

Proof. If H has index 2 then the distinct cosets are of the form H and gH for some $g \notin H$. Let $h \in H$ and $g \notin H$ then $hg^{-1} \notin H$. Therefore $ghg^{-1} \notin gH$. So $ghg^{-1} \in H$ and H is normal. Note that $\forall g \notin H$, $g \in gH$. ■

Remark. We have $|S_n| = n!$ so S_n always has an index 2 subgroup called the alternating group $|A_n| = \frac{n!}{2}$ (by Lagrange's theorem).

Fix a group G and $N \trianglelefteq G$. We shall see that the set of left cosets of N in G can be given a group structure. We have notation $\overline{G} = G/N = \{\text{set of left cosets on } N \text{ in } G\ \}$. We also have $\overline{a} = aN$ which are the left cosets. There exists a projection map $\pi : G \to \overline{G} = G/N$. So we have $\pi(a) = \overline{a} = aN$. If $AandB$ are subsets of G then $AB \subset G$ where $AB = \{x \in G | x = ab, a \in A, b \in B\}$. This is called the product set of A and B, it is not the cartesian product.

Lemma 2.7.1. Let aN and bN be any 2 left cosets. Then the product set $aNbN$ is also a left coset and $aNbN = abN$.

Proof. We have $aNbN = \{x = G | x = an_1bn_2, n_1 \in N, n_2 \in N\}$. Since $N \trianglelefteq G$ we know that every left coset is also a right coset and both are equal. So $n_1b \in Nb = bN$. If $n_1b \in N$ then $\exists n_3 \in N$ such that $n_1b = bn_3$. So we have $an_1bn_2 = abn_3n_2 = abn_4$ for some $n_4 \in N$. So $aNbN = abN$. ■

Theorem 2.7.3 (Operations on $\overline{G}$)**.** There is a binary operation on the set of left cosets of G that makes $\overline{G}$ into a group and π is a surjective group homomorphism such that $\ker \pi = N$.

Proof. We have $\overline{G} = \{N, a_1N, a_2N, \dots\} = \overline{a_1}, \overline{a_2}, \overline{a_3} \dots$. Define a binary operation on G as follows: $\times : \overline{G} \times \overline{G} \to \overline{G}$. We define $\overline{a_i} \times \overline{a_j} = \overline{a_ia_j}$ since $a_iNa_jN = a_ia_jN$ from the lemma. Identity in G/N is $\overline{e} = N$. Inverse of any $\overline{a_i} \in G/N$ is $\overline{(a_i^{-1})} = a_i^{-1}N$. It is closed since all $\overline{a_ia_j}$ are some left coset. Since $\pi(ab) = \overline{ab} = abN = aNbN = \pi(a)\pi(b)$ we see that π is a group homomorphism. Since every $\overline{a}$ has a pre-image a mapped by π to $\overline{a}$. The kernel is given by the set of a such that $\pi(a) = \overline{e} = N$. So $a \in N$ and N is the kernel. ■

Remark. Suppose $\pi(a) = \overline{a} = \pi(b)$ then $aN = bN \Leftrightarrow b^{-1}a \in N \Leftrightarrow a^{-1}b \in N$.

Theorem 2.7.4 (First Isomorphism theorem)**.** Let $\phi : G \to G'$ be a group homomorphism. Then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi$ which is isomorphic to $\text{Im}(\varphi) \subset G'$. So $\overline{\varphi} : G/\ker \varphi \to G'$ where $\overline{\varphi}(\overline{a}) = \varphi(a)$ is injective.

Proof. We have $\varphi = \overline{\varphi} \circ \pi$ where $\pi : G \to G/\ker \phi$. So $\varphi(a) = \overline{\varphi}\pi(a) = \overline{\varphi}(a)$. We can see that $\overline{\varphi}(\overline{a}) = e'$ gives the kernel, so the kernel is $\overline{e}$ and it is injective. ■

Lecture 11

3 Oct. 10:10

Exercise. Show that if G has only one element of order 2 then this element is in $Z(G)$.

Answer. Let $x \in G$ be order 2 so $x^2 = e$. For any element $g \in G$. We have gxg^{-1} has order 2. So $gxg^{-1} = x$ or $gxg^{-1} = e$. But if $gxg^{-1} = e$ then $x = e$ which is a contradiction so $gxg^{-1} = x$. So $x \in Z(G)$. ⊛

Exercise. Let G be a finite subgroup and H, K be subgroup of relatively prime order. Then $H \cap K = \{e\}$.

Answer. From lagranges theorem we know that $|H \cap K| | |H|$ and $|H \cap K| | K$. Since they are relatively prime we have $|H \cap K| = 1$ and so it is the trivial subgroup. ⊛

Exercise. $G = S_3$ and $H = \{e, (1, 2)\}$. How many distinct left cosets are there?

Answer. By lagrange's theorem we have $[G : H] = \frac{|G|}{|H|} = 3$. ⊛

Chapter 3

Rings

Lecture 12

3.1 Introduction to Rings

17 Oct. 10:10

Definition 3.1.1 (Ring). A ring R is a set with two laws of composition $+$ and $\times$, called addition and multiplication that satisfies these axioms:

1. With respect to addition R is an abelian group which we denote by R^+ and its identity is denoted by 0 (additive identity)
2. Multiplication is associative and the multiplicative identity is denoted by 1.
3. Distributive law: $(a+b)\times c = a\times c + b\times c$

Definition 3.1.2 (Commutative Ring). If $\times$ is commutative then we say R is a commutative ring. Else R is a non-commutative ring.

Example.
1. Ring of integers: $(\mathbb{Z}, +, \times)$
2. Set of $n\times n$ matrices with integer entries: $(M_n(\mathbb{Z}, +, \times)$
3. Quotient groups: $\mathbb{Z}/n\mathbb{Z}$ with addition and multiplication on the $\bar{i}$
4. Polynomial rings are denoted by $\mathbb{Z}[x] \coloneqq \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | a_0, \ldots, a_n\mathbb{Z}\}$. They are a group under addition and associative under multiplication.
5. Consider the set of gaussian integers $\mathbb{Z}[\iota] \coloneqq \{a + bi | a, c \in \mathbb{Z}\}$. Group under addition and associative under multiplication.
6. Suppose R is a ring. We have $R[x] = \{a_0 + a_1x + \cdots + a_nx^n | a_0, \ldots a_n \in R\}$ which is also commutative.

Definition 3.1.3 (Monic polynomial). A polynomial $p(x) = a_o + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$ is called monic if $a_n = 1$

Proposition 3.1.1. Let R be a ring and $f(x)$ be a monic polynomial and $g(x)$ be any polynomial. Both $f(x)$ and $g(x)$ are in $R[x]$. Then $\exists! q(x), r(X) \in R[x]$ such that $g(x) = f(x)q(x) + r(x)$ such that $\deg(r(x)) < \deg(f(x))$

3.2 Ring homomorphisms and Ideals

Definition 3.2.1 (Ring Homomorphism). A ring homomorphism is a map from $R \to R'$ such that

1. $\varphi(a+b) = \varphi(a) + \varphi(b) \forall a, b \in R$
2. $\varphi(a \times b) = \varphi(a) \times \varphi(b)$
3. $\varphi(1) = 1$

Remark. $\varphi(0) = 0$ follows from 1 (group homomorphism).

Definition 3.2.2 (Ring ismorphism). A bijective ring homomorphism is called a ring isomorphism.

Example. $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ where $a \mapsto \overline{a}$.

Example. $\mathbb{S} \to M_2(\mathbb{Z})$ where $a \mapsto \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$

Lecture 13

19 Oct. 10:10

Proposition 3.2.1. Let R be a ring then $\exists$ unique ring homomorphism $\varphi : \mathbb{Z} \to R$ such that $\forall n \geq 0, \varphi(n) = 1_R + \cdots + 1_r$ and $\varphi(-n) = -\varphi(n)$

Proof. To show that φ is a ring homomorphism the addition is obvious, and for multiplication we see that $\varphi(ab) = 1_R + \cdots + 1_R = (1_R + \cdots + 1_R) \times (1_R + \cdots + 1_R) = \varphi(a)\varphi(b)$ (by distributive law).

For uniqueness let φ' be another ring homomorphism. We know that $\varphi(1) = 1$ so the same relations follow. ■

Definition 3.2.3 (Kernel of a homomorphism). Let $\varphi : R \to R'$. Then $\ker \varphi = \{S \in R | \varphi(S) = 0\} \subset R$. (Same as a group homomorphism)

Remark. Suppose $s \in \ker \varphi$ and $r \in R$ then $\varphi(rs) = 0$. If $s_1, s_2 \in \ker \varphi$ then $s_1 + s_2 \in \ker \varphi$

Definition 3.2.4 (Ideal). And ideal I of a ring R is a non-empty subset of R such that

1. I is closed under addition ($0 \in I$)
2. If $s \in I$ and $r \in R$ then the product $r \times s \in I$

Remark. Kernel of a ring homomorphism is an ideal

Definition 3.2.5 (Principal Ideals). Let R be a ring and $a \in R$. Then the set $(a) = aR := \{ar | \forall r \in R\}$. So $(ar_1 + ar_2) = a(r_1 + r_2) \in a(R)$ and $r_1 \in R, ar_2 \in (a)$ then $r_1 ar_2 = ar_1 r_2 \in aR$.

Example.

Definition 3.2.6 (Units of a ring). $R^\times := \{a \in R | \exists a, b \in R, ab = 1\}$

Example. 1. $\mathbb{Z}^\times = \{\pm 1\}$

2. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$
3. $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$
4. $\mathbb{R}^\times = \mathbb{R} - \{0\}$

Definition 3.2.7 (Field). A field F is a ring where $F^\times = F - \{0\}$

Remark. $F^\times$ form an abelian group under multiplication

Example. $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{0\}$

Proposition 3.2.2. 1. The only ideals of field are (0) and R

2. A ring that has exactly 2 ideals is a field

Proof. Let I be an ideal of the field F. $I = (0)$ or contains a non-zero element a. But if $a \in I$ then $a^{-1} \times a \in I \Rightarrow 1 \in I$. But if $1 \in I$ then $r \in I \forall r \in R \Rightarrow I = R = (1)$.

Let $a \neq 0 \in R$. Then $0 \subsetneq (a) \subset R \Rightarrow (a) = R \Rightarrow 1 \in (a) \Rightarrow 1 = ar$ for some r. So $r = a^{-1}$. ■

Lecture 14

22 Oct. 10:10

Definition 3.2.8 (Zero divisor). Let R be a ring. Let $a, b \in R$ such that $a, b \neq 0$ but the product $ab = 0$. In this case a, b are zero divisors.

Example. Let $\mathbb{Z}/6\mathbb{Z}$. Then $\overline{2} \times \overline{3} = \overline{0}$ so they are 0 divisors.

Definition 3.2.9 (Integral Domain). A ring R is called an integral domain if there are no zero divisors in R.

Example. $\mathbb{Z}$ is an integral domain. $\mathbb{Z}/p\mathbb{Z}$ for a prime p is an integral domain. $\mathbb{Z}[x]$ is an integral domain.

Lemma 3.2.1. Every field F is an integral domain.

Proof. By contradiction. Assume F is not an integral domain. So by definition there are 0 divisors in the field F. But $a \neq 0 \Rightarrow a^{-1} \in F$ such that $a^{-1}a = 1$. But then $aa^{-1}b = 0 \Rightarrow b = 0$ which is a contradiction. So F is an integral domain. ■

3.3 Prime and Maximal Ideals

Definition 3.3.1 (Prime Ideal). An idea $I \in R$ is called a prime ideal if $I \neq 0$ nor $I = R$ and for $a, b \in R$ such that $ab \in I$ then $a \in I$ or $b \in I$

Example. $R = \mathbb{Z}$ then $p\mathbb{Z}$ is a prime ideal. But $6\mathbb{Z}$ is not an ideal.

Definition 3.3.2 (Maximal Ideal). And ideal $I \subset R$ is called maximal if $I \neq 0$ or $I \neq R$ and $\exists$ no other ideal $J \neq R$ such that $I \subset J$.

Example. $p\mathbb{Z}$ is a maximal ideal.

3.4 Quotient Rings

Definition 3.4.1 (Quotient rings). Let R be a ring and $I \in R$ any ideal. Then we know that R^+ is an abelian group, and the ideal $I \subset R^+$ is a normal additive subgroup. So by group theory we know we can form the quotient R/I. This also has the structure of a ring. So we have $\overline{R} = R/I = \{a + I | a \in R\}$

Theorem 3.4.1 (Quotient rings). $I \subset R$ is an ideal of a ring R. Then $\exists!$ ring structure on $\overline{R} = R/I$ the set of additive cosets of I in R such that the map $\pi : R \to R/I$ is $a \mapsto a + I = \overline{a}$ is a ring homomorphism with $\ker \pi = I$. Here π is called the canonical map.

Proof. We already have an additive group structure on $\overline{R} = .R/I$. We need to define a multiplication on the set of additive cosets. $\overline{a} \times \overline{b} = ab + I$. We have $\overline{a} \times \overline{b} = (a + I)(b + I)$. We have $\pi(a) = I \Leftrightarrow a \in I$ so $\ker \pi = I$. ■

Remark. In $\overline{R} = R/I$ we have $0_{\overline{R}} = I$ and $1_{\overline{R}} = 1 + R$. We also have $-\overline{a} = \overline{-a}$

Example. Let $R = \mathbb{Z}$, $I = n\mathbb{Z}$ for $n \in \mathbb{Z}$. Then $\overline{R} = \mathbb{Z} = n\mathbb{Z}$

Theorem 3.4.2 (First isomorphism theorem for rings). Let $f : R \to R'$ be a surjective ring hommorphism with $\ker(f) = I \in R$. Then $\exists$ isomorphism $\overline{f} : R/I \to R'$

Theorem 3.4.3 (Correspondence theorem). Let $\varphi : R \to R'$ be a surjective ring homomorphism. Then there is a bijective correspondence between the set of ideals of R' and the set of ideals of R that contain $K = \ker \varphi$.

Proof was done in lecture 15

Proof. Let I be an ideal of R that contains K. It is enough to show that $\varphi(I)$ is closed under products. Let $r' \in R'$ and $i' \in \varphi(I)$. We want to show that $r'i' \in \varphi(I)$. Now $i' \in \varphi(I) \Rightarrow \exists i \in$ such that $\varphi(i) = i'$. Similarly $r' \in R' \Rightarrow \exists r \in R$ such that $\varphi(r) = r'$. Note that $ri \in I$ since I is an ideal, so $r'i' = \varphi(ri) \in \varphi(I)$. So $\varphi(I)$ is an ideal of R'.

We have J an ideal of R'. We want to show that $\varphi^{-1}(J) \subset R$ that contains K. Suppose $a \in R$ and $\varphi(a) = \widetilde{a} \in J$. Then $a \in \varphi^{-1}(J) \subset R$. Let $r \in R$ and $a \in \varphi^{-1}(J)$ then $\varphi(ra) = \varphi(r)\varphi(a) = \widetilde{r}\widetilde{a} \in J \Rightarrow ra \in \varphi^{-1}(J)$ so it is an ideal. Since $0 \in J \Rightarrow \varphi^{-1}(0) \subset \varphi^{-1}(J) \Rightarrow K \subset \varphi(J)$.

Suppose $\varphi(I) = J$ and $\varphi^{-1}(J) = I$. Consider $\pi \circ \varphi(r) \coloneqq \varphi(r) + J$. So this is $R \to R'/J$. We see that $\ker \pi \circ \varphi = \{r \in R | \varphi(r) = 0 + J\} = I$. So we have $R/I \cong R'/J$ ■

Corollary 3.4.1. Let $\varphi : R \to F$ be a surjective ring homomorphism to a field F. Then $\ker \varphi$ is a maximal ideal.

Lecture 15

31 Oct. 10:10

Proposition 3.4.1. Let $P \subset R$ be an ideal in a ring R. Then P is prime $\Leftrightarrow$ R/P is an integral domain.

Proof. Suppose R/P is an integral domain. Then $\overline{a} \times \overline{b} = 0 \Rightarrow \overline{a} = 0$ or $\overline{b} = 0$. But $\overline{ab} = 0 \Rightarrow ab \in P \Rightarrow a \in P$ or $b \in P$ therefore P is prime.

Suppose P is a prime ideal. Assume R/P is not an integral domain. So $\exists \overline{a}, \overline{b} \in R/P; a, b \neq 0; \overline{ab} = 0$. But $\overline{ab} = 0 \Rightarrow ab \in P$. But P is a prime ideal so $a \in P$ or $b \in P$ so either $\overline{a} = 0 or \overline{b} = 0$ which is a contradiction. ■

Proposition 3.4.2. Let M be an ideal in R. Then M is a maximal ideal $\Leftrightarrow$ R/M is a field.

Proof. R/M is a field $\Leftrightarrow$ the set of ideals of $R/M = \{0, R/M\}$. By the correspondence theorem we have a bijection between the set of ideals of R that contain M and the set of ideal of R/M. We have $\pi^{-1}(R/M) = R$. So there is only one ideal of R that contains M which is R itself, so M is a maximal ideal. ■

Corollary 3.4.2. Every maximal ideal in a ring R is prime.

Proof. Let M be a maximal ideal. So we know that R/M is a field. But since every field is an integral domain, R/M is an integral domain. So M is a prime ideal. ■

3.5 Product Rings

Definition 3.5.1 (Product Rings). Let R and R' be any two rings. Then we can give a ring structure on the cartesian product $R \times R' = \{(r, r') | r \in R; r' \in R'\}$. Here $(r_1, r_1') + (r_2, r_2') = (r_1 + r_2, r_1' + r_2')$. Similarly $(r_1, r_1') \times (r_2, r_2') = (r_1 \times_R r_2, r_1' \times_{R'} r_2')$. So we have $(1_R, 1_{R'})$ and $(0_R, 0_{r'})$ as the multiplicative and additive identities.

Remark. False theorem: if R and R' are integral domains then $R \times R'$ is an integral domain is a false statement. Consider $(1, 0) \times (0, 1) = 0$ so they are 0 divisors and thus it is not an integral domain.

Lecture 16

3.6 Chinese Remainder Theorem

2 Nov. 10:10

Remark. Given ideals I and J we can write their sum as $I + J := \{r_i + r_j | r_i \in I; r_j \in J\}$ which is a ring in R.

Definition 3.6.1 (Co-Maximal). I and J are said to be co-maximal (co-prime) if $I + J = R$

Example. Recall that Bezout's Lemma states that if $m, n \in \mathbb{Z}$ then $\exists a, b\mathbb{Z}$ such that $\gcd(m, n) = am + bn$. If $\gcd(m, n) = 1$ $m\mathbb{Z} + n\mathbb{Z} = \{am + bn | a, b \in \mathbb{Z}\}$. Bezout's theorem gives us that $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z} = \mathbb{Z}$.

Theorem 3.6.1 (CRT). Let R be a ring and let $A_1, A_2, \ldots, A_k$ be pairwise co-maximal ideals $(A_i + A_j = R, \forall i, j)$ then $R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k$.

Proof. Let us define a map $crt : R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k$ so $r \mapsto (r+A_1, r+A_2, \ldots, r+A_k)$. Then we have $\ker(crt) = \{r \in R | crt(r) = (r + A_1, r + A_2, \ldots, r + A_k) = (0, 0, \ldots, 0)\}$. We have this when $r \in A_1, r \in A_2 \ldots r \in A_k$. So $r \in A_2 \cap A_2 \cap \cdots \cap A_k$.

By the first isomorphism theorem $R/A_1 \cap \cdots \cap R/A_k \hookrightarrow R/A_1 \times \cdots \times R/A_k$. One can also show that crt is surjective, and then by the isomorphism theorem we know that they are isomorphic. ■

This part isn't done yet

Example. Applications:

- Consider $R = \mathbb{Z}$. Two ideals (m) and (m) are co-maximal when $\gcd(m, n) = 1$. By CRT we know that $\mathbb{Z}/m\mathbb{Z} \cap n\mathbb{Z} \cong \mathbb{Z}/m \times \mathbb{Z}/n$. We know that $m\mathbb{Z} \cap n\mathbb{Z} = \{t \in \mathbb{Z} | mn \mid t\}$
- Suppose $n = p_1^{e_1} \ldots p_k^{e_k}$ (prime factorization). We know that $p_i^{e_i}$ and $p_j^{e_j}$ are co-maximal. We know that $(p_1^{e_1}) \cap \cdots \cap (p_k^{e_k}) = n$. So by CRT $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_k^{e_k}$.

Remark. We see that $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$. So $|(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m)^\times| \cdot |(\mathbb{Z}/n)^\times|$ which is the same as $\varphi(mn) = \varphi(m)\varphi(n)$ where φ is euler's totient function given by $\varphi(k) = |\{1 \leq l \leq k | gcd(l, k) = 1\}|$.

3.7 RSA Cryptography

Theorem 3.7.1 (Euler's Generalisation). Let $n \in N$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. So consider $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. So $\overline{a}^{\varphi(n)} \equiv 1 \mod n$. If n is prime then $\varphi(n) = n - 1$. So $\overline{a}^{p-1} \equiv 1 \mod p$.

Choose two very large primes p and q. Now $n = pq$. We know that $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$. Given a sufficiently large n it is difficult to factorise into it's prime factors, and so we cannot computer $\varphi(n)$ just by knowing n.

3.7.1 RSA Key

1. Generate two large primes p, q and $n = pq$.
2. $\varphi(n) = (p - 1)(q - 1)$
3. Randomly choose $e \in \{1, \ldots, \varphi(n) - 1\}$ such that $\gcd(e, \varphi(n) = 1)$. So we know that $e \in (\mathbb{Z}/\varphi(n))^\times \Rightarrow \exists d \in (\mathbb{Z}/\varphi(n))\times, ed = 1 \mod \varphi(n)$.
4. Find d such that $ed \equiv 1 \mod \varphi(n)$.
5. The public key are the numbers n and e
6. The private key is n and d.

3.7.2 RSA Encryption

The input is a number M that is coprime to n (required by Euler). So we have $V \coloneqq M^e \mod n$ where V is the ciphertext.

3.7.3 RSA Decryption

We compute $\overline{M} = V^d \mod n$ where $\overline{M}$ is the plaintext. We see that $\overline{M} = V^d \mod n = M^{ed} \mod n = M(M^{k\varphi(n)}) \mod n = M \mod n$. This is because $ed \equiv 1 \mod \varphi(n)$ so $ed = 1 + k\varphi(n)$

Lecture 17

3.8 Irreducible polynomials and Eisenstien's criteria

4 Nov. 10:10

Definition 3.8.1 (Reducible ELements). Let F be a field. We say that a non-constant polynomial $f(x) \in F[x]$ is reducible over F if we can factor this polynomial $f(x)$ as a product of $g(x), h(x) \in F[x]$ such that $\deg(g(x)), \deg(h(x)) < \deg(f(x))$. We say that a non-constant polynomial is reducible if it is not reducible.

Example. Let $F = \mathbb{Q}$ and $f(X) = x^2 - 2 \in \mathbb{Q}[x]$. Note that $f(x)$ has no roots over $\mathbb{Q}$. Assume that $f(x)$ is reducible over the rational numbers. So there exist $g(x), h(x) \in \mathbb{Q}[x]$ and $\deg(g(x)), \deg(h(x)) < \deg(f(x)) = 2$. So $\deg(g(x)) = \deg(h(x)) = 1$. But this is irreducible since there are no rational roots and $g(x)$, $h(x) \in Q[x]$ and cannot produce irrational roots.

Example. $F = \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$. Let $f(x) = x^3 + \overline{3}x + 2 \in \mathbb{F}_5[x]$. Suppose $f(x)$ is reducible. We know $\deg(g(x)) = 1, 2$ and similarly 2 or 1 for $h(x)$. So upto reordering we can assume that $\deg(g(x)) = 1$ and $\deg(h(x)) = 2$. So we have $g(x) = \overline{a}x + \overline{b} \Rightarrow x = -\overline{b}\overline{a}^{-1}$ is a root of $g(x)$ and this exists in $\mathbb{F}_5$. This is a root of $g(x)$ and hence also a root of $f(x)$. We can check if $f(x)$ has a root in this field by hand. By evaluating we see that $f(X)$ has no roots.

Theorem 3.8.1 (Roots). Let $f(x) \in F[x]$ be of degree two or three. Then $f(X)$ is irreducible if and only if it has no roots.

Proof. If $f(x)$ has a root α then $f(x) = (x - \alpha)h(x)$ where $h(x) \in F[x]$. ■

Theorem 3.8.2 (Gauss' Theorem). Let $f(x) \in \mathbb{Z}[x]$. Then we can factor $f(x)$ into two polynomials of degrees r and s in $\mathbb{Z}[x]$ if and only if we can factor $f(x)$ into two polynomials of the same degrees r and s in $\mathbb{Q}[x]$.

Corollary 3.8.1. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in Z[x]$ where $a_0 \neq 0$. Suppose $f(x)$ has a root in $Q[x]$ then it also has a root $m \in \mathbb{Z}$ and m divides a_0.

Proof. Suppose $\alpha \in \mathbb{Q}$ is a root of $f(x)$. This means $f(x)$ is reducible over $Q[x]$. So by Gauss' theorem, so there exists a factor of $f(x)$ of degree one over $\mathbb{Z}$. We will denote this linear factor as $ax + b$ for some $a, b \in \mathbb{Z}$. In particular we can write $f(x) = (ax + b)g(x)$ where $\deg(g(x)) = \deg(f(x)) - 1$. We know that the coefficient of x^n is divisible by a so $a = \pm 1$. So upto replacing $g(x)$ by $-g(x)$ we can assume $a = 1$. $f(x) = (x + b)g(x)$. So $-b$ is a root of $f(x)$ and $b \in \mathbb{Z}$. The constant term of $f(x)$ is a_0 and $(x + b)g(x)$ id divisible by $-b$. ■

Example. $f(x) = x^{3-1}$. We know that $m = \pm 1$ or $m = \pm 2$ so there is no root over $\mathbb{Z}$ which means there is no root over $\mathbb{Q}$.

Theorem 3.8.3 (Eisenstien's criteria). Let $f(x) = a_n a^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. Suppose there is a prime number p that divides $a_0 \ldots a_{n-1}$ and does not divide a_n and p^2 does not divide a_0. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose $f(x)$ is reducible over $\mathbb{Q}[x]$. So $f(x) = g(x)h(x)$. So by Gauss' theorem $f(x) = \widetilde{g}(x)\widetilde{h}(x)$ for some $\widetilde{g}, \widetilde{h} \in \mathbb{Z}[x]$. We can reduce the co-efficients modulo p. The factorisation still holds. So we have $\overline{f}(x) = \overline{a}_n x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_0 \in \mathbb{Z}/p\mathbb{Z}$. So $\overline{f}(x) = \overline{a}_n x^n$. So in particular $\overline{f}(x) = \overline{g}(x)\overline{h}(x) = \overline{a}_n x^n$ The constant term of $\overline{f}(x) = 0$. But the constant term of $f(x) = a_0$ can be written as the product of the constant terms of $\widetilde{g}$ and $\widetilde{h}$ so $a_0 = b_0 c_0$. Similarly for $\overline{f}(x)$. So $0 = \overline{b_0} \times \overline{c_0}$ in $\mathbb{Z}/p\mathbb{Z}$ which is an integral domain. So $\overline{b_0} = 0 = \overline{c_0}$. So $a_0 = b_0 c_0$ then p^2 divides a_0 which is a contradiction. ■

Corollary 3.8.2. $x^n + p$ is irreducible $\forall n \in N$ and all primes p.

Lecture 18

Revision of Appendix B 7 Nov. 10:10

Chapter 4

Group Actions

Lecture 19

9 Nov. 10:10

Let S be the set of column vectors $S = \{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} ; x_i \in \mathbb{R}\}$ and $A \in GL_n(\mathbb{R})$ and $\det A \neq 0$. Now, we can multiply $As = \begin{bmatrix} \sum_{i=1}^n a_{1i}S_i \\ \sum_{i=1}^n a_{2i}S_i \\ \vdots \\ \sum_{i=1}^n a_{ni}S_i \end{bmatrix} \in S$ for $s \in S$. Here the group $GL_n(\mathbb{R})$ "acts" on the set S.

Definition 4.0.1 (Group Action). Let G be a group and S be a set. A group action of G on the set S is a map $\phi : G \times S \to S$, $(g, s) \mapsto g \cdot s \in S$ such that:

1. $e \cdot s = s, \forall s \in S$
2. $(g', g \cdot s) \mapsto g' \cdot (g \cdot s) = (g'g)s, \forall s \in S, \forall g, g' \in G$ (associative law).
3.

Example. So the relation of $GL_n(\mathbb{R})$ on S defined above is a group action. The identity matrix $I_{n\times n}$ always gives $Is = s$ and matrix multiplication is associative.

Example. Let $G = S_n$. And $S = \{1, 2, 3 \dots n\}$. So now for $G \times S \to S$ consider $\forall \sigma \in S_n, k \in S, (\sigma, k) \mapsto \sigma(k)$.

Example. G is a group and $S = G$. For $G \times G \to G$ we have $(g, h)1 > g \cdot h = gh \in G$.

Example. Suppose $H \subset G$ is a subgroup of G. Let G/H be the set of left cosets of H in G, $G/H = \{[H], [g_1H, g_2H \dots]\}$. We can define a group action on the set of left cosets as follows: $\phi : G \times G/H \to G/H$ where $(g, [g_iH]) \mapsto ([gg_iH])$.

Example. Conjugacy action. G is a group. We define an action $\phi : G\times G \to G$ where $(g, h) \mapsto ghg^{-1}$.

4.1 Orbit and Stabilizer

Definition 4.1.1 (Orbit). Let G be a group acting on set S. Then for every element in $s \in S$ we have $Orb(S) = \mathcal{O}_s = \{s' \in S | s' = g \cdot s \text{ for some } g \in G\}$

Proposition 4.1.1. Let us define a relation on S as follows $S_1 \sim S_2$ if $\exists g \in G, s_2 = g \cdot s$. This relation is an equivalence relation and the equivalence classes are the orbits. So the orbits partition the set S.

Proof. We have $s_1 \sim s_1$ since $e \cdot s_1 = s_1$. If $s_1 \sim s_2$ then $s_2 = g \cdot s_1$ for some $g \in G$. But then $g^{-1} \in G$ so $g^{-1}s_2 = s_1$ and $s_2 \sim s_1$. We can also show that transitivity holds. ■

Definition 4.1.2 (Transitive group actions). If $Orb(s) = S, \forall s \in S$ then the group action is called transitive.

Example. In the example above with symmetric groups we have $Orb(k) = S$ since there exists some permutation that takes k to each of the elements in the set. So this is a transitive group action.

Definition 4.1.3 (Stabilizer). Let G be a group acting on set S. The stabilizer of an element $s \in S$ is the set of group elements that leaves s fixed. This is given by $G_s = \{g \in G | g \cdot s = s\}$. The identity is always in the stabilizer.

Corollary 4.1.1. if $g \in G_s$ and $h \in G_s$ then $h^{-1} \in G_s$. So $gh^{-1} \in S$. This shows that G_s is a subgroup of $G, \forall s \in S$.

Remark. So group actions can give us equivalence relations and subgroups on the group G.

Exercise. Prove or disprove that G_s is a normal subgroup of G.

Proof. Let $h \in G_s$. If $G_s \trianglelefteq G$ then $ghg^{-1} \in G_s, \forall g \in G$. So then $ghg^{-1} \cdot s = s$. This is the same as $gh \cdot (g^{-1} \cdot s)$ by associativity. Since $h \in G_s$ need not always stabilise $g^{-1} \cdot s$. ■

Lecture 20

4.2 Orbit Stabilizer Theorem

14 Nov. 10:10

Proposition 4.2.1. Let S be a set on which a group G acts. Let $s \in S$ and $G_s = \{g \in G | g \cdot s = s\}$ is the stabilizer. If $a, b \in G$ then $a \cdot s = b \cdot s \Leftrightarrow a^{-1}b \in G_s$. Equivalent to saying $b \in aG_s$. Suppose $a \cdot s = s'$. Then $G_{s'} = aG_sa^{-1}$. This happens whenever $s' \in Orb(s)$.

Proof. If $a \cdot s = b \cdot s \Leftrightarrow a^{-1}b \cdot s = s \Leftrightarrow a^{-1}b \in G_s \Leftrightarrow b \in aG_s$. Suppose $g \in aG_sa^{-1}$. Now consider $g \cdot s' = g \cdot (a \cdot s) = aha^{-1} \cdot (a \cdot s) = ah \cdot s = a \cdot s = s'$. So $aG_sa^{-1} \subset G_{s'}$. Let $h' \in G_{s'}$ and let $g' = a^{-1}h'a$. We know $a \cdot s = s' \Rightarrow s = a^{-1} \cdot s'$. Now consider $g' \cdot s = a^{-1}h'a \cdot (a^{-1} \cdot s') = a^{-1}h' \cdot s' = a^{-1} \cdot s' = s$. So $a^{-1}G_{s'}a \subset G_s$. So $aG_sa^{-1} = G_{s'}$. ■

Theorem 4.2.1 (Orbit-Stabilizer Theorem). let S be a set on which a group G acts and let $s \in S$. Let G_s and $Orb(s)$ be its stabilizer and orbit respectively. There is a bijective map $\epsilon : G/G_s \to Orb(s)$ where $[aG_s] \mapsto a \cdot s$. This map ϵ is compatible with group operations so $\epsilon(g \cdot [c]) = g \cdot \epsilon([c])$.

Proof. We know that G/G_s is the set of left cosets of G_s. Suppose $aG_s = bG_s$ for distinct elements $a, b \in G$ then we have to show that $a \cdot s = b \cdot s$. We see that $aG_s = bG_s \Leftrightarrow a^{-1}b \in G_s \Leftrightarrow a^{-1}b \cdot s = s \Leftrightarrow a \cdot s = b \cdot s$. Which shows the the map is well defined and injective. ■

Proposition 4.2.2 (Counting Formula). Let S be a finite set on which the group G acts. And let G_s and $Orb(s)$ be the stabilizer and orbit of an element $s \in S$. Then $|G| = |G_s||Orb(s)|$.

Proof. By the orbit stabilizer theorem we know that the set of left cosets G/G_s is in bijection with $Orb(s)$ $\forall s \in S$. If two sets are in bijection they have the same cardinality. But by Lagrange's theorem we know that $|G/G_s| = [G : G_s]$. So we have $|G/G_s| = |G|/|G_s|$. So we have $|G| = |G_s||Orb(s)|$. ■

Corollary 4.2.1. We know that $|S| = \sum_{i=1}^{k} |Orb(s_i)| = \sum_{i=1}^{k} [G : G_{s_i}] = |G| \sum_{i=1}^{k} \frac{1}{|G_{s_i}|}$

4.3 Class Equation

Let G be a group which acts on itself via conjugation. So we have $G \times G \to G$ where $(g, h) \mapsto ghg^{-1}$. This is a well defined group action.

Lemma 4.3.1. For all $x \in G$ we have $Orb(x) = x \Leftrightarrow x \in Z(G)$.

Proof. $Orb(x) \Leftrightarrow gxg^{-1} = x \forall g \in G \Leftrightarrow gx = xg \forall g \in G \Leftrightarrow x \in Z(G)$. ■

$\forall x \in G$ the orbits $Orb(x)$ are called the conjugacy classes associated to the elements x and the stabilizers G_x are called the centralizers. So we have $Orb(x) = \{gxg^{-1} | g \in G\}$ and $G_x = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$. So in the conjugation action fixing x translates to commuting with x.

We have $|G| = \sum_{i=1}^{k} |C_{x_i}|$ where C_{x_i} are distinct conjugacy classes. By the lemma we have $|C_{x_i}| = 1, \forall x_i \in Z(G)$. So we have $|G| = 1+1+\cdots+1+\sum_{i=1}^{k} |C_{x_i}| = |Z(G)+| \sum_{i=1}^{k'} |C_{x_i}| = |Z(G)| + \sum_{i=1}^{k'} |[G : G_{x_i}]|$ where G_{x_i} is the centralizer. This is the class equation.

4.4 Cayley's Theorem

Let G be a group and let $g \in G$. Then the map $m_g : G \to G$ where $x \mapsto g \cdot x$ is a bijection. In particular m_g is a permutation of the elements of G. So $m_g \in S_{|G|}$. In particular if $|G| = n$ then $m_g \in S_n$.

Theorem 4.4.1 (Cayley's Theorem). The map $\phi : G \to S_{|G|}$ where $g \mapsto m_g$ is an injective group homomorphism. So every group G is isomorphic to a subgroup of a symmetric group.

Proof. We see it is a homomorphism since $g_1 g_2 \mapsto m_{g_1 g_2} = m_{g_1} \circ m_{g_2}$ (check using associativity). To show ϕ is injective we use its kernel. We know $\ker \phi = \{g \in G | m_g = id\}$. So we have $m_g = id \Leftrightarrow gx = x, \forall x \in G \Leftrightarrow g = e$. So $\ker \phi = e$. So we have $G \hookrightarrow S_{|G|}$. ■

Lecture 21

16 Nov. 10:10

4.5 Sylow Theorems

Suppose that a group G acts on a set S, and yet $U \subset S$ of order r. Then, $\forall g \in G$, we have $gU = \{g \cdot u | u \in U\} \subset S$ is another subset of order r. This way we can define an action of G on the set of subset of S of a given order r. So we have an action $G \times S \to S$ where $(g, s) \mapsto g \cdot s$. We now have an action $G \times S'_r \to S'_r$ where $(g, U) \mapsto gU$ as defined above where S'_r is the set of subsets of order r of S.

Definition 4.5.1 ($p-$groups). Let p be a prime number. A finite group G is called a $p-$group if the order of the group is a power of p ($|G| = p^k, k \geq 1$).

Definition 4.5.2 (Sylow-p-subgroup). Let G be a finite group of order n and let p be a prime that divides n. So we have $n = p^e m$ where $p \nmid m$. Subgroups of G of order p^e are called sylow-p-

subgroups.

Lemma 4.5.1. Let U be a subset of the group G. Note that G acts on the subsets of G of a fixed order r. Then the order of the stabilizer denoted as $Stab([U])$ divides $|U| = r$ and $|G|$.

Proof. Let $H = Stab([U]) \subset G$. So $hU = U, \forall h \in H$. So $\forall u \in U$ and $\forall h \in H$ we have $hu \in U$. So the right coset $Hu \subset U$. So U is partitioned into right cosets Hu. So $U = \sqcup_{i=1}^{k} Hu_i$. We have already seen that $|Uu_i| = |H|$. So we know $|U| = k|H|$. We also know that $H \subset G$ so by lagrange's theorem $|H|$ divides $|G|$. ■

Lemma 4.5.2. Let $n = p^e m$ where $e \geq 1$ and $p \nmid m$. The number of subsets of order p^e in a set of order n, say N is not divisible by p.

Proof. Proof uses the fact that $N = \binom{n}{p^e}$ ■

Let G be a finite group whose order is divisible by a prime p.

Theorem 4.5.1 (First Sylow Theorem). G contains a sylow-p-subgroup.

Proof. We have $|G| = p^e m$. Let S'_{p^e} be the set of all subsets of G of order p^e. G acts on this set by left multiplication so by disjoint union we have $S'_{p^e} = \sqcup_{orb(s')} orb(s')$. So $N = |S'_{p^e}| = \sum_{orb(s')} orb(s')$. By lemma 2 above we have $p \nmid N \Rightarrow \exists$ some orbit $orb([U])$ such that $p \nmid |orb([U])|$. So let $H = Stab([U]) \subset G$. By lemma 1 above we know that $|H|$ divides $|U| = p^e$. So $|H|$ is a power of p. By orbit stabilizer theorem we know that $|G| = |Orb([U])| \cdot |Stab([U])|$. So we know that $p^e m = |Orb([U])||H|$. Since $p \nmid |Orb([U])|$ we have $|H| = p^e$ and $|Orb([U])| = m$. So we see that H is sylow-p-subgroup. ■

Corollary 4.5.1 (Cauchy's Theorem). Let G be a finite group whose order is divisible by a prime p. Then G contains a subgroup H of order p.

Proof. By sylow's thorems there exists a sylow-p-subgroup K of order p^e. This implies that $\exists x \in K$ such that $x \neq e$. Recall that $O(x) \mid |K| = p^e \Rightarrow O(x) = p^\alpha$ for some $\alpha \leq e$. Then $x^{p^{\alpha-1}}$ has order p. So the cyclic group $H = \langle x^{p^{\alpha-1}} \rangle$ is a cyclic subgroup of order G with order p. ■

Theorem 4.5.2 (Fixed point theorem). Let K be a p-group and S be a finite set on which K acts. If $p \nmid |S|$ then $\exists$ a fixed point for the action of K on S, i.e. there is an $s \in S$ such that $Stab(s) = K$.

Proof. $S = Orb(1) \sqcup Orb(2) \sqcup \cdots \sqcup Orb(n)$. So we have $|S| = \sum_{i=1}^{n} |\mathcal{O}_i|$. By the orbit stabilizer theorem we have $|K| = |\mathcal{O}_i||Stab(s_i)|$. Since K is a $p-$group all the stabilizers are also $p-$groups. So $p \mid \mathcal{O}_i$ unless $Stab(s_i) = K$ in which case $\mathcal{O}_i = 1$. So $p \mid \sum_{i=1}^{n} \mathcal{O}_i$ unless $Stab(s_i) = K$. But $p \nmid |S|$ so there is at least one s_i such that $Stab(s_i) = K$. ■

Definition 4.5.3 (Normalizer). For the conjugate group action $g([H]) = gHg^{-1}$, the stabilizer $Stab([h]) = \{g \in G | gHg^{-1} = H\}$ is called the normalizer $N(H)$.

Theorem 4.5.3 (Second Sylow Theorem). The sylow-p-subgroups are conjugates. Every subgroup of G that is a p-group is contained in a sylow-p-subgroup.

Proof. Given a sylow-p-subgroup H and a p-group $K \subset G$ we will show that K is contained in some conjugate subgroup H' of H. When K itself is a sylow-p-subbgroup then $K = H'$.

Let C be the set of left cosets of H in G so $|C| = [G : H] = m$. So $p \nmid |C|$. Now G acts on C where $g, [aH] \mapsto [gaH] = g \cdot [aH]$. This is a transitive action. Lets denote the coset $[H]$ with c. We have $Stab_G(c) = \{g \in G | g[H] = [H], [gH] = [H]\} = H \subset G$. Now consider the same action of K on C (called restricting the action of G on C to K). Since K is a p-group and $p \nmid |C|$, by the fixed point theorem there exists some element $c' \in C$ such that $Stab_K(c') = k \in K | k \cdot c' = c' = K$.

Let $Stab(c') = \{g \in G | g \cdot c' = c'\}$ be the stabilizer of c' for the action of G. So in particular $K \subset Stab_G(c')$. The action of G on C is transitive so there exists some element $g \in G$ such that $c' = g \cdot c$. So now $Stab_G(c') = gStab_G(c)g^{-1}$ (from Proposition 4.2.1). So $K \subset Stab_G(c') = gStab_G(c)g^{-1}$. So $K \subset g[H]g^{-1}$. Since $|H| = p^e$ we know $|gHg^{-1}| = p^e$, so H' is a sylow-p-subgroup. ■

Corollary 4.5.2. If a finite group G has only one sylow-p-subgroup then that subgroup is normal.

Proof. Proof by contradiction. Let $K \subset G$ be the unique sylow-p-subgroup of G and assume it is not normal. This means that $gKg^{-1} \neq K$. But then gKg^{-1} is also a sylow-p-subgroup different from K which is a contradiction by second Sylow thoerem. ■

Theorem 4.5.4 (Third Sylow Theorem)**.** Let s denote the number of sylow-p-subgroups of G. Then s divides m and $s \equiv 1 \mod p$.

Proof. Let S be the set of sylow-p-subgroups of G. We can define an action on $G \times S \to S$ where $g, [H_i] \mapsto g \cdot [H_i] = gH_ig^{-1}$. This action is transitive by the second sylow theorem. We have $Stab([H_i]) = N(H_i)$. We also have $S = \mathcal{O}_{H_i} \Rightarrow s = |\mathcal{O}_{H_i}| = \frac{|G|}{|N(H_i)|} = [G : N(H_i)]$. But $H_i \subset N(H_i)$ so $|H_i| \mid |N(H_i)|$. So $\frac{|G|}{N(H_i)} \mid \frac{|G|}{H_i}$. So $s \mid m$.

Restricting H_1 on S. So we have $H_1 \times S \to S$ where $h, [H_i] \mapsto [hH_ih^{-1}]$. This action need not be transitive. So in particular we have $S = \mathcal{O}_{[H_1]} \sqcup \cdots \sqcup \mathcal{O}_r$. We know that $|\mathcal{O}_{[H_1]}| = 1$. Also $\mathcal{O}_{s_i} = \frac{|H_i|}{|Stab(s_i)|}$. So we have $p \mid |\mathcal{O}_{s_i}|$ for $i \geq 1$. So $s = |\mathcal{O}_{[H_1]}| + \sum_{i=2}^{r} |\mathcal{O}_{s_i}| = 1 + \sum_{i=2}^{r} |\mathcal{O}_{s_i}|$. So we have $s \equiv 1 \mod p$. ■

Lecture 22

See proofs of second and third Sylow theorem above. 21 Nov. 10:10

Chapter 5

Alternating Groups

Lecture 23

23 Nov. 10:10

Let S_n be the symmetric group, i.e. the group of permutations of $\{1 \dots n\}$. Then S_n acts on $\mathbb{Z}[x_1 \dots x_n]$ (set of polynomials in variables $x_1 \dots x_n$ defined over $\mathbb{Z}$). $S_n \times \mathbb{Z}[x_1, \dots x_n] \to \mathbb{Z}[x_1, \dots, x_n]$ where $(\tau, Q(x_1, \dots x_n)) \mapsto Q(X_{\tau(1),\dots,X_{\tau(n)}})$.

Now consider $P(X_1 \dots X_n) = \Pi_{i<j}(X_j - X_i)$. So S_3 acts on $P(X_1, X_2, X_3) = (X_3 - X_2)(X_3 - X_1)(X_2 - X_1)$. Consider $\sigma = (1, 2)$. So we have $\sigma \cdot P(X_1, X_2, X_3) = (X_{\sigma(3)} - X_{\sigma(2)})(X_{\sigma(3)} - X_{\sigma(2)})(X_{\sigma(2)} - X_{\sigma(1)}) = (X_3 - X_1)(X_3 - X_2)(X_1 - X_2) = -P(X_1, X_2, X_3)$. Now consider $\tau = (1, 2, 3)$. So we have $\tau \cdot P(X_1, X_2, X_2) = P(X_1 - X_3)(X_1 - X_2)(X_3 - X_2) = P(X_1, X_2, X_3)$.

Now consider $(i, j) \cdot P(X_1, \dots X_n)$. This is also $\pm P(X_1, \dots X_n)$. So we have $\mathcal{O}_P = \{P(X_1, \dots X_n), -P(X_1, \dots X_n)\}$. By the orbit stabilizer theorem we know $|\mathcal{O}_P||Stab(P)| = |S_n|$. So we have $Stab(P) \subset S_n$ is a subgroup of order $\frac{n!}{2}$. So the stabilizer $Stab(P)$ is called an alternating group or A_n where $[S_n : A_n] = 2$. In particular we have $A_n \trianglelefteq S_n$ is a normal subgroup. The two left cosets are $[A_n]; [\sigma A_n]$ where $\sigma P = -P$.

Now consider element $(a_1, \dots, a_k) \in S_n$ which is a cycle of length k. You can write this as a composition of transpositions $(a_1, a_2)(a_1, a_3) \dots (a_1, a_k)$ and hence every element of S_n can also be written as product of transpositions.

Definition 5.0.1 (Even cycles). A cycle $(a_1 \dots a_k)$ of a group is called even if it can be written if it can be written as the product of an even number of transpositions.

Remark. A cycle of odd length is even. So we can define $A_n = \{\sigma \in S_n | \sigma \text{is even}\}$.

Recall that a group G is called simple if the only normal subgroups of G are G and $\{e\}$. For example $\mathbb{Z}/p\mathbb{Z}$ are simple groups. We see that $\forall n \geq 5, A_n$ is a simple subgroup. A_3 is also simple. The classification of finite simple groups has been completed.

Theorem 5.0.1 (Alternating and simple groups). A_n is simple for $n \geq 5$.

Proof. **Step 1:** A_n is generated by 3-cycles. In fact A_n is generated by $(1,2,k)$. A_n is the group of even permutations. In particular every element is a product of transpositions of the form $(a,b)(c,d)$ or $(a,b)(a,c)$. We have $(a,b)(c,d) = (a,c,d)(a,c,b)$ and $(a,b)(a,c) = (a,b,c)$. So A_n is generated by 3-cycles. We have $(1,a,2) = (1,2,a)^{-1}$ and $(1,a,b) = (1,2,b)(1,2,a)^{-1}and(2,a,b) = (1,2,b)^{-1}(1,2,a)$. So we have $(a,b,c) = (1,2,a)^{-1}(1,2,c)$ $(1,2,b)^{-1}(1,2,a)$. So we have shown that A_n is generated by $(1,2,k)$ cycles.

Step 2: If $H \trianglelefteq A_n$ and H contains a 3 cycle then $H = A_n$ where $(A_1, a_2, a_3) \in H$. So without loss of generality we can assume that $(1,2,3) \in H$. We have $(1,2,k) = (1,2)(3,k)(1,2,3)^{-1}((1,2)(3,k))^{-1}, \forall k \geq 3$. Since this is a normal subgroup we know that $(1,2,k) \in H$. No we have $\langle (1,2,3), (1,2,4)\dots\rangle \subset H \Rightarrow A_n \subset H \Rightarrow A_n = H$.

Step 3: Now we want to show that every normal subgroup of A_n contains a 3 cycles. Assume that $H \trianglelefteq A_n$ and $H \neq \{e\}$. Let $x \neq e \in H$. Suppose the order of x is lm where l is prime. Then $ord(x^m) = l$. Replacing x by x^m we may assume that the order of x is a prime l. If $l \geq 5$ then $x = (1,2,3\dots l)y$ where y is some other l cycles since it is the product of l cycles. Take $g = (4,3,2)$. If $H \trianglelefteq A_n$ then $gxg^{-1}x^{-1} \in H$. So we get this as $(4,3,2)[(1,2,\dots l)y](2,3,4)[y^{-1}(l,l-1,\dots 3,2,1)]$ which is the three cycle $(2,4,5)$. So by step 2 we have $H = A_n$.

Now consider when $l = 3$ If x is a 3 cycle we are done. So assume there are at least 2 three cycles $x = (1,2,3)(4,5,6)y$. Take $g = (4,3,2)$ then the commutator $gxg^{-1}x^{-1} \in H$ and it is given by $(1,5,2,4,3)$. And this is back to case 1. Lastly, consider if $l = 2$. So x is an even element, i.e. it is the produt of an even number of transpositions. If $x = (1,2)(3,4)(5)y$. Or it is of the form $x = (1,2)(3,4)(5,6)y$. In each case we can choose $g = (5,3,1)$ to get a 5 cycle or 3 cycle respectively and so we see it has a 3 cycle. ■

Lecture 24

See proof for theorem above. 28 Nov. 10:10

Appendix

Appendix A

DS Notes

DS 1

30 Aug. 13:30

Exercise. Lets S^* be the group of all non-zero 2×2 matrices under multiplication with real entries. Does $(S^*, \cdot)$ forms a group?

Answer. No, every matrix does not have an inverse. ⊛

At least one entry is non-zero

Exercise. Let $G = (\mathbb{Z}, +)$. Prove $H = (n\mathbb{Z}, +)$ is a subgroup of G where $n \in \mathbb{N}$.

Answer. We have $H = \{na | a \in \mathbb{Z}\}$. Now proving each property:

1. **Closure:** Take any 2 elements na and nb from H where $a, b \in \mathbb{Z}$. We can see that $na + nb = n(a + b)$ where $a + b \in \mathbb{Z}$ from G.
2. **Associativity:** Let $na, nb, nc \in H$. We can see that $(na + nb) + nc = na + nb + nc + na + (nb + nc)$. This follows from associativity of G.
3. **Identity:** We know that $0 \in H$ and $na + 0 = na$ so 0 is the identity. .
4. **Inverse:** For any arbitrary element $na \in H$, we claim that $-na$ is the inverse. We can see this since $na + (-na) = (n - n)a = 0a = 0$.

⊛

The identity of subgroup is inherited from the group

Exercise. Give example of a infinite group that has non-trivial finite subgroup.

Answer. For example $G = (R \setminus \{0\}, \cdot)$ Then we have $H = (1, -1, \cdot)$. ⊛

DS 2

6 Sep. 16:40

Exercise. Prove that every cyclic group is abelian. Give an example to show that the converse of the above statement is not true in general.

Proof. Let $G = \langle g \rangle$ be a cyclic group. We want to show that $ab = ba, \forall a, b \in G$. As G is cyclic we can write $a = g^{n_1}, = b = g^{n_2}$ for some $n_1, n_2 \in \mathbb{N}$. Now $ab = g^{n_1} g^{n_2} = g^{n_1 + n_2} = g^{n_2 + n_1} = g^{n_2} g^{n_1} = ba$. ■

Answer. We see that $G = (\mathbb{R}^2, +)$ is abelson but not cyclic. ⊛

$(\mathbb{Z}^+, +)$ is an infinite cyclic group

Exercise. Let $G = GL_2(\mathbb{R} = \{A \in M_{2\times 2}(\mathbb{R}) : \det(A) \neq 0\})$ and $H = SL_2(\mathbb{R} = \{A \in M_{2\times 2}(\mathbb{R}) : \det(A) = 1\})$. Prove that $\forall g \in$ and $\forall h \in H$, $ghg^{-1} \in H$.

Proof. Since matrix multiplication preserves the determinant we have:

$$\begin{aligned}\det\left(ghg^{-1}\right) &= \det(gh)\det\left(g^{-1}\right)\\ &= \det\left(gg^{-1}\right)\det(h)\\ &= 1 \cdot 1\\ &= 1\end{aligned}$$

■

Exercise. Prove that for any abelson group G, $(ab)^n = a^n b^n$ where $a, b \in G$ and $n \in \mathbb{N}$

Proof. Base case ($n = 1$): Trivially true
Assumption: Assume the statement holds for $n = k$
When $n = k + 1$:

$$\begin{aligned}(ab)^{k+1} &= (ab)^k(ab)\\ &= a^k b^k ab\\ &= a^k b^k (ba) && \text{(Using associativity and abelian)}\\ &= a^{k+1}b^{k+1}\end{aligned}$$

■

Exercise. Let G be a group such that $x^2 = e, \forall x \neq 0$. Prove that for any such element x we have $x = x^{-1}$ and G is abelian.

Proof. We see that $x^2 = e$ so:

$$\begin{aligned}xx &= e\\ xx &= xx^{-1}\\ x^{-1}xx &= x^{-1}xx^{-1}\\ ex &= ex^{-1}\\ x &= x^{-1}\end{aligned}$$

From this remark we can show that:

$$\begin{aligned}xy &= (xy)^{-1}\\ &= y^{-1}x^{-1}\\ &= yx\end{aligned}$$

■

Exercise. Let $h \in G$ be an arbitrary element and $f : G \to G$ defined by $f(h) = ghg^{-1} \forall g \in G$. Prove that f is a bijection.

Proof. For injectivity have:

$$\begin{aligned} f(h_1) &= f(h_2) \\ gh_1g^{-1} &= gh_2g^{-1} \\ g^{-1}gh_1g^{-1}g &= g^{-1}gh_2gg^{-1} \\ h_1 &= h2 \end{aligned}$$

For surjectivity if $k \in G$, we want to find some $h \in G$ s.t. $f(h) = k$.

$$\begin{aligned} f(h) &= k \\ ghg^{-1} &= k \\ g^{-1}ghgg^{-1} &= g^{-1}kg \\ h &= g^{-1}kg \end{aligned}$$

■

DS 4

20 Sep. 16:40

Definition A.0.1 (Centre of a group). $Z(G) \coloneqq \{g \in G | xg = gx \forall x \in G\}$

Lemma A.0.1. $Z(G) \subset G$

Proof. We have identity since $ex = xe = x$. And so on. ■

Lemma A.0.2. $Z(G)$ is a normal subgroup of G. ($Z(G) \trianglelefteq G$)

Proof. Let $a \in Z(G)$, then we have $gag^{-1} = agg^{-1} = a \in Z(G)$. ■

Lemma A.0.3. $Z(G)$ is abelian.

Proof. This is obvious from the definition. ■

Lemma A.0.4. $Z(G) = G \Leftrightarrow G$ is abelian.

Proof. Again obvious from the definition. ■

Exercise. Find all possible homomorphisms between $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_6, +)$.

Remark. Let $\varphi : G \to G'$ be a homomoprhosm and $a \in G$ s.t. $\varphi(a)$ is also finite and moreover $O(\varphi(a)) \mid O(a)$. If φ is an isomorphism then $O(\varphi(a)) = O(a)$.

DS 5

27 Sep. 16:4

Exercise. Find all left cosets of C_2 in C_6.

Answer. We have $C_2 = \{e, g_3\} \subset C_6$. Now checking by multiplying with e, g, g^2 we get all left cosets as $\{e, g^2\}, \{g, g^4\}, \{g^2, g^5\}$. ⊛

Theorem A.0.1 (Abelian and Normal subgroups). Every subgroup of abelian group is normal.

Proof. Since G is abelian all $ghg^{-1} = hgg^{-1} = h$ so any subgroup $H = gHg^{-1}$ and it is a normal subgroup. ■

DS 9

8 Nov. 16:40

Exercise. $G = \mathbb{Q}/\mathbb{Z} = \{x + \mathbb{Z}; x = \frac{p}{q}\}$. Show that order of G is infinite and show that order of every element of G is finite.

Answer. Let $O(G) = m > 0$. Then by langranges's theorem $m(x + \mathbb{Z}) = \mathbb{Z} \Rightarrow mx + \mathbb{Z} = \mathbb{Z} \Rightarrow mx \in \mathbb{Z}$. Let us take $x = \frac{1}{2m}$ then $mx = \frac{m}{2m} \notin \mathbb{Z}$. This is a contradiction so order of G is infinite. Now let $x + \mathbb{Z} = \frac{p}{q} + \mathbb{Z}$. Then $q(\frac{p}{q} + \mathbb{Z}) = p + \mathbb{Z} = \mathbb{Z}$. S order of $x \leq q < \infty$. ⊛

Exercise. Show that $C[0,1]$ is not an integral domain where $C[0,1] = \{f : [0,1] \to \mathbb{R} | f \text{ cont.}\}$.

Answer. Let $f(x) = \frac{1}{2} - x$ for $0 \leq x \leq \frac{1}{2}$ and 0 otherwise. Let $g(x) = 0$ for $0 \leq x \leq \frac{1}{2}$ and $\frac{1}{2}$ otherwise. Both functions are continious. But we see that $f(x) \cdot g(x) = 0$ and so they are 0 divisors. ⊛

Exercise. Let F be a field and consider $R = F[x, y]$. Show that the ideal $\langle x, y\rangle$ in R is not principal.

Answer. The elements of $I = \langle x, y\rangle = \{f(x,y) | f(x,y) = xh_1(x,y) + yh_2(x,y)\}$. Note that these elements have no constant terms. Let I be a principal ideal in R. Then $\langle x, y\rangle = \langle h(x,y)\rangle \in R$. Since $x \in \langle x, y\rangle$ we have $x = h(x,y)p(x,y)$. Similarly $y = h(x,y)q(x,y)$. As $\deg_y x = 0 \Rightarrow \deg_y h(x,y)p(x,y) = 0 \Rightarrow \deg_y h(x,y) + \deg_y p(x,y) = 0 \Rightarrow deg_y h(x,y) = 0$. Similarly $\deg_x h(x,y) = 0$. So together this implies $h(x,y) = c$. So the ideal $\langle x, y\rangle = c$. But these elements have no constant terms so this is a contradiction. ⊛

Exercise. Let $R = C[0,1]$ and $a \in [0,1]$. $M_a = \{f \in C[0,1] | f(a) = 0\}$, M_a is an ideal in $C[0,1]$. Prove that this is a maximal ideal.

Answer. Let us define the evaluation map $\varphi C[0,1] \to \mathbb{R}$ at a. So $\varphi(f(x)) = f(a)$. This is surjective since for any $c \in \mathbb{R}$ then we can take $f(x) = c \in C[0,1]$ and $\varphi(f(x)) = c$. We have $\ker\varphi = \{f \in C[0,1] | f(a) = 0\} = M_a$. We claim that $M_a = \langle x - a\rangle$. Since $\varphi(x-a) = a - a = 0$. So $\langle x - a\rangle \subset \ker\varphi$. Let $g(x) \in \ker\varphi = h(x)(x - a) + r$. We have $g(a) = 0 \Rightarrow r = 0$ so $\ker\varphi \subset \langle x - a\rangle$. Now by first isomorphism theorem we have $C[0,1]/\langle x - a\rangle \cong \mathbb{R}$. Since R is a field, we have $\langle x - a\rangle$ is a maximal ideal. ⊛

Appendix B

Quotient Groups

Definition B.0.1 (Equivalence relation)**.** An equivalence relation on the set S is roughly speaking a way of comparing any two elements in the set such that it satisfies the symmetric, reflexive and transitive properties.

Example. $S = \mathbb{Z}$ and let us fix a natural number $n \in \mathbb{N}$. Lets say a is equivalent to b is $a - b$ is divisible by n. We see that if $a \sim b$ then $b \sim a$, $a \sim a$, if $a \sim b$ and $b \sim c$ then $a \sim c$.

Definition B.0.2 (Equivalence classes)**.** Suppose we have equivalence relation $\sim$. Then the equivalence classes are given by $[a] \coloneqq \{b \in S | a \sim b\}$. Note that $[a] \cap [b] = \{[a] = [b]\}$ if $b \sim a$, else $\varnothing$.

Let G be a group and let $N \trianglelefteq G$. Given a normal subgroup N we define a relation $\sim$ as follows. For $a, b \in G$ we say $a \sim b$ if $ab^{-1} \in N$. We can show that this satisfies reflexive, symmetric and transitive properties. Under this relation the equivalence classes are given by $[a] = \{b \in G | ab^{-1} \in N \Rightarrow a = n_1 b\}$. So we have $G/\sim = \{\overline{a_1}, \overline{a_2}, \overline{a_3}, \dots\} = \{Na_1, Na_2, Na_3, \dots\}$. So it is the set of right cosets.

We denote $G/\sim$ by G/N and moreover we can give a group structure on G/N. Identity in G/N is the coset $Ne = N$. We have $Na_i Na_j = Na_i a_j$. And the inverse $(Na_i)^{-1} = Na_i^{-1}$

Let R be a ring and $I \subset R$ be an ideal. We define an equivalence relation on R as follows. $a, b \in R$ and $a \sim b$ if $a - b \in I$. In this case $[a] = \{b \in R | a - b \in I\} = a + I = 1 + I$ (additive cosets). We denote $R/\sim$ as R/I and because I is an ideal, R/I gets a ring structure. A ring structure on R/I is given as follows. We have $0_{R/I} = 0 + I = I$. We have multiplicative identity on $1_{R/I}$. Addition is defined as $a_1 + I + a_2 + I = (a_1 + a_2) + I$. Multiplication is defined as $(a_1 + I)(a_2 + I) = a_1 a_2 + I$.