Notes for Math 113: Abstract Algebra
UC Berkeley, Spring 2019

Aditya Sengupta

May 13, 2019

Contents

Math 113: Abstract Algebra **Spring 2019**

Lecture 1: Introduction: Sets, Functions, and Relations

Lecturer: Sylvie Corteel *January 23* *Aditya Sengupta*

Note: *LaTeX format adapted from template courtesy of UC Berkeley EECS dept.*

1.1 Logistics

Book will be followed closely. `corteel@berkeley.edu`. Office in Evans 859, office hours on Wednesday 11-12 and Friday 1:30-2:30. Course website: `math.berkeley.edu/~corteel/MATH113.html`.

The midterms will be on 25 February and 8 April, both worth 20% of the grade. Homework will be due at the start of class every week and be worth 20% of the grade (with two drops), and the final is worth 40%.

The first homework will be due on 1 February.

1.2 Introduction

Abstract algebra looks at addition and multiplication in an abstract way. Instead of taking integers, we can take abstract sets and define their own notion of addition. We will study abstract properties of sets with operations, to reveal similarities between operations on matrices, numbers, polynomials, etc. In this way we will gain familiarity with abstractions and proofs.

The first half of this class will be group theory. A group is a set with one operation and certain properties. The second half will deal with rings and fields, which are sets with two operations. We will see that everything we know about groups can generalize nicely to rings.

1.3 Sets and Relations

1.3.1 Sets

A set is a collection of given elements. It can be given explicitly, e.g. $S = \{2, 5, 7\}$, or it can be given by a characteristic property, e.g. T is the set of perfect squares, which is represented as $T = \{n^2 \mid n \text{ is an integer}\}$. Some common sets are

$\mathbb{N}$	set of all nonnegative integers
$\mathbb{Z}$	set of all integers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers

Note that $\mathbb{Q}$ is explicitly given by $\{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$. The superscript $+$ on any set, e.g. $\mathbb{Z}^+$, refers to the set of positive elements of the regular set (such as the positive integers), and the superscript $*$ means nonnegative.

Some more general notation includes

$a \in S$	a is an element of S
$a \ni S$	a is not an element of S
$\varnothing$	the empty set (the set with no elements)
$A \subseteq B$	A is a subset of B
$A \subset B$	A is a proper subset of B

If A is a subset of B, that means every element of A is in B: $\forall x \in A, x \in B$. If A is a proper subset of B, then $A \subseteq B$ and $A \neq B$.

As an example, $S = \{0, 1\}$ has the subsets $\varnothing, 0, 1, 0, 1$, so there are 4 subsets and 3 proper subsets.

1.3.2 Functions

A function $f : X \to Y, x \to f(x)$ goes between sets X and Y, $x \in X$ and $f(x) \in Y$. If $A \subseteq X$, then

$$f(A) = \{f(x) \mid x \in A\}$$

and $f(X)$ is referred to as the image of f.

If $B \subseteq Y$ and $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$, then $f^{-1}(Y)$ is the *inverse image* or preimage of f.

Some important properties of functions are as follows:

1. f is injective or one-to-one if $f(x_1) = f(x_2) \implies x_1 = x_2$. Different elements of X map to different elements of Y. For example, $f : \mathbb{R} \to \mathbb{R}, x \to x^2$ is not injective, because $f(3) = f(-3) = 9$. However, the function $f : \mathbb{R}^+ \to \mathbb{R}^+, x \to x^2$ is injective.
2. f is surjective or onto if $f(X) = Y$, that is, every value in Y is attained by f. For example, $f : \mathbb{R} \to \mathbb{R}, x \to x^2$ is not surjective, because $\nexists x \in \mathbb{R}$ such that $f(x) = -1$. However, the function $f : \mathbb{R}^+ \to \mathbb{R}^+, x \to x^2$ is surjective.
3. f is bijective if it is injective and surjective. If f is bijective, there exists an inverse correspondence $f^{-1}Y \to X$, mapping $y \to$ the unique x such that $f(x) = y$.

We have seen that $f : \mathbb{R}^+ \to \mathbb{R}^+, x \to x^2$ is injective and surjective, which suggests that we can make this inverse relationship: $f^{-1} : \mathbb{R}^+ \to \mathbb{R}^+, y \to \sqrt{y}$.

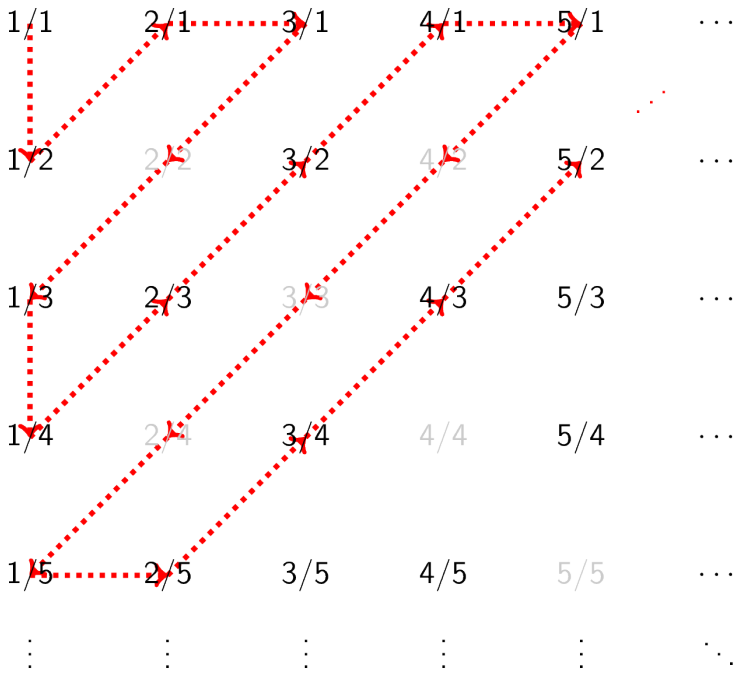
1.3.3 Cardinality

We say that X and Y have the same cardinality if there exists a bijection between them. If the sets are finite, they have the same number of elements.

We claim that $\mathbb{Z}$ and $\mathbb{Z}^+$ have the same cardinality. To prove or disprove this, we want to build a bijection $\mathbb{Z} \to \mathbb{Z}^+$. This bijection can be constructed as

$$n \to \begin{cases} 2n & n > 0 \\ 2|n| + 1 & n \leq 0 \end{cases}$$

Similarly, we can show that $\mathbb{Z}^+$ and $\mathbb{Q}$ have the same cardinality. The sets in bijection with $\mathbb{Z}^+$ are *countable sets*. We produce this bijection by listing the elements of $\mathbb{Q}$ in a table, where the nth row has a denominator of n, and go down the diagonals:



`http://cglab.ca/~discmath/functions-countability.html`

An example of a set that is not countable is $\mathbb{R}$. Subsets, such as $\{x \in \mathbb{R} \mid 0 < x < 1\}$, are also not countable.

1.3.4 Relations

Definition 1. *A relation between two sets A and B is a subset R of $A \times B = \{(a, b) \mid a \in A, b \in B\}$.*

For example, $f : A \to B, \{(x, f(x)) \mid x \in A\}$ is a relation; we can see that $R_f \subseteq A \times B$.

Definition 2. *A partition of a set S is a collection of non empty disjoint subsets whose union is S.*

The subsets are called the *cells* of the partition. For example, if a set $S = \{0, 1, 2\}$, a partition of S is $0, 2, 1$. $0, 2, 1, 2$ is not a partition because 2 is in two different cells, and $0, 2$ is not a partition as 1 is not in any cell.

Given a partition, we can define a relation R on S, xRy iff x and y are in the same cell. For instance, in the valid example $0, 2, 1$ above, a valid relation is $1R1, 0R2, 0R0, 2R0, 2R2$.

Math 113: Abstract Algebra **Spring 2019**

Lecture 2: Equivalence Relations and Binary Relations

Lecturer: Sylvie Corteel *25 January* *Aditya Sengupta*

Definition 3. *An equivalence relation $\sim$ on a set S is a relation which is:*

1. *reflexive: $\forall x \in S, x \sim x$*
2. *symmetric: $\forall x, y \in S$, if $x \sim y$ then $y \sim x$*
3. *transitive: $\forall x, y, z \in S$, if $x \sim y$ and $y \sim z$ then $x \sim z$.*

The canonical example of an equivalence relation is congruence modulo n on $\mathbb{Z}$. We say $a \simeq_n b$ or $a \simeq b \bmod n$ if $n \mid (a - b)$. It can be shown that all three properties stated above are satisfied for this relation.

Theorem 2.1. *Let S be a nonempty set and let $\sim$ be an equivalence relation on S. Then $\sim$ yields a partition of S into equivalence classes of the form $\bar{a} = \{x \in S \mid x \sim a\}$. Conversely, any partition of S determines an equivalence relation $\sim$ on S, where $a \sim b$ if and only if a and b are in the same cell of the partition (that is, $\bar{a} = \bar{b}$.)*

Proof. Let $a \in S$. We want to show that a is in exactly one equivalence class. Since $a \sim a$, by definition, $a \in \bar{a}$. So a is in at least one equivalence class. To show that it is in only one, suppose that $a \in \bar{b}$ for some $b \in S$. We want to show that $b \in \bar{a}$ and therefore that $\bar{a} = \bar{b}$, so that a is in exactly one equivalence class. To show that $\bar{a} = \bar{b}$, we show that each one is a subset of the other: $\bar{a} \subseteq \bar{b}$ and $\bar{b} \subseteq \bar{a}$.

Let $x \in \bar{a}$. Then by definition of the equivalence class, $x \sim a$. Since we are assuming that $a \in \bar{b}$, we know that $a \sim b$, so by transitivity, $x \sim b$ and therefore $x \in \bar{b}$. In the other direction, let $y \in \bar{b}$, so $y \sim b$. We know that $a \sim b$, therefore by symmetry, $b \sim a$. Therefore $y \sim b \sim a \implies y \sim a \implies y \in \bar{a}$. Therefore every element of $\bar{a}$ is an element of $\bar{b}$ and vice versa, so $\bar{a} = \bar{b}$. □

The canonical example of a set of equivalence classes is $\mathbb{Z}_n$, the set of congruence classes modulo n:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

For example, $\mathbb{Z}_3 = \bar{0}, \bar{1}, \bar{2}$. Explicitly, $\bar{0} = \{0, \pm 3, \pm 6, \pm 9, \dots\} = \{3k \mid k \in \mathbb{Z}\}$, and similarly for the others, $\bar{1} = \{3k + 1 \mid k \in \mathbb{Z}\}$ and $\bar{2} = \{3k + 2 \mid k \in \mathbb{Z}\}$.

2.1 Binary Operations

Definition 4. *A binary operation $*$ on a set S is a function $S \times S \to S$. For $a, b \in S$, we write $a * b$ to denote the function output.*

Common examples are the usual operations (addition, subtraction, multiplication) on the usual sets of numbers ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots$). Note that division is not a binary operation on $\mathbb{Q}$, because $0 \in \mathbb{Q}$ but division is

not defined for $q * 0$ for any $q \in \mathbb{Q}$. More examples include addition of matrices in $M_n(\mathbb{R})$, the set of $n \times n$ matrices of real numbers, the `min` operation on $\mathbb{Z}^+$, and exponentiation $a * b = a^b$.

More generally, binary operations can be defined on the set of functions $f : \mathbb{R} \to \mathbb{R}$: we know that

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

All of these are valid binary operations.

To extend the canonical example, we consider $\mathbb{Z}_n$ again. Consider addition: we claim that $\bar{a} + \bar{b} = \overline{a+b}$. We need to check that this is well-defined, i.e. that it does not depend on the choice of representatives. In other words, we need to check that if $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$, then $a \bar{+} b = \overline{a'+b'}$, where $\bar{a}', \bar{b}'$ are different representations of the same equivalence class. This turns out to be the case.

If $\bar{a} = \bar{a}'$ then $n \mid a - a'$, and if $\bar{b} = \bar{b}'$ then $n \mid b - b'$. Since $(a+b) - (a'+b') = (a-a') + (b-b')$, we have $n \mid (a+b) - (a'+b')$ or $a + b = a' + b'$.

This also works for multiplication, with $\bar{a} \cdot \bar{b} = \overline{ab}$. The proof that this is well-defined uses the following: $ab - a'b' = (a-a')b + (b-b')a$.

It is important to note that for a binary operation $*$ to be well-defined, $a * b$ needs to be defined for every $a, b \in S$ unambiguously, and the value of $a * b$ must be an element of S.

Definition 5. *If $*$ is a binary operation on S and $T \subseteq S$, then we say that T is closed under $*$ if $a * b \in T \forall (a, b) \in T \times T$.*

Example 2.2. *Let*

$$u_n = \{e^{2\pi i k/n} \mid k \in \mathbb{Z}\} = \{\text{“the } n^{th} \text{ roots of unity”}\}$$

and consider multiplication as the operation. If $\zeta_n = e^{2\pi i/n}$, then $\zeta_n^k \cdot \zeta_n^l = \zeta_n^{k+l}$.

Math 113: Abstract Algebra **Spring 2019**

Lecture 3: Binary operations and isomorphisms

Lecturer: Sylvie Corteel *January 28* *Aditya Sengupta*

3.1 Binary Operations contd.

Recall that a binary operation is a function $* : S \times S \to S$ for all $(a, b) \in S \times S$. A property of a binary operation is its set is closed under the operation, i.e. $a * b \in S$ for any choice of a and b.

Definition 6. *A binary operation is well-defined on S if*

1. *$a * b$ is defined $\forall\ a, b \in S$*
2. *$a * b \in S$*

Example 3.1. *Consider the set $H = \{n^2 \mid n \in \mathbb{Z}\}$. H is not closed under addition, because $1^2 + 1^2 = 2 \notin H$. However, $\langle H, \cdot \rangle$ is well defined.*

3.2 Structural Properties of Binary Operations

Definition 7. *$*$ is commutative if $\forall\ a, b \in S, a * b = b * a$.*

For example, addition and multiplication on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are commutative, but multiplication of 2×2 matrices are not commutative.

Definition 8. *$*$ is associative if $\forall\ a, b, c \in S, a * (b * c) = (a * b) * c$.*

For example, addition and multiplication on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are associative, and so is multiplication of $n \times n$ matrices. Composing functions is also associative:

$$f \circ (g \circ h)(x) = f(g(h(x))) = (f \circ g) \circ h(x)$$

Subtraction over $\mathbb{Z}$ is not associative.

3.3 Tables

A binary operation on a *finite* set S can be defined by a table:

$*$	$\dots$	b	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
a	$\dots$	$a * b$	$\dots$

Example 3.2. *Consider the set $S = x, y, z$ with a binary operation defined as follows:*

$*$	x	y	z
x	z	y	z
y	x	z	y
z	y	x	z

It is easy to check from this table that this operation is, for example, not commutative, as $x * y \neq y * x$.

3.4 Isomorphic binary structures

Consider two sets with their own binary operations defined over them $\langle S, * \rangle, \langle S', *' \rangle$.

Definition 9. *An isomorphism $\phi : S \to S'$ is a map such that ϕ is a bijection (it is injective and surjective: for every $x \in S$, there exists a unique element $y \in S'$ such that $\phi(x) = y$, and $\phi(x_1) = \phi(x_2)$ implies $x_1 = x_2$) and such that ϕ is homomorphic, that is, $\forall\ x, y \in S, \phi(x * y) = \phi(x) *' \phi(y)$.*

Remark 3.3. *A map satisfying the homomorphic property as stated above is called a homomorphism.*

We can show that two binary structures are isomorphic by constructing the map $\phi : S \to S'$, then showing that ϕ is well-defined, that is $\forall\ x \in S, \phi(x) \in S'$, and that ϕ is surjective and injective, and finally showing that the homomorphic property holds.

Example 3.4. ***Show that** $\langle \mathbb{R}, + \rangle$ **and** $\langle \mathbb{R}^+, \cdot \rangle$ **are isomorphic.***

We want to find a function that translates addition to multiplication of positive real numbers. A candidate is $\phi : \mathbb{R} \to \mathbb{R}^+, x \to e^x$. This is well-defined becuse $\forall\ x \in \mathbb{R}, e^x \in \mathbb{R}^+$, it is injective because $e^x = e^y \implies \ln(e^x) = \ln(e^y) \implies x = y$, and it is surjective. Therefore, we check the homomorphic property, which gives us

$$\forall\ x, y \in \mathbb{R}, \phi(x + y) = e^{x+y} e^x \cdot e^y = \phi(x) \cdot \phi(y)$$

as required.

Example 3.5. ***Consider the set** $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$**, with the property that** $k \in Z$ **implies** $k \in \bar{a}$ **if** $k \simeq a \bmod n$**. Then, consider the roots of unity,** $U_n = \{\left(e^{2i\pi/n}\right)^k \mid k \in \mathbb{Z}\}$**. Show that these sets are isomorphic.***

We define a map $\bar{a} \to \zeta^a = \left(e^{2i\pi/n}\right)^a$ and show that it is isomorphic. We see that it is well-defined and surjective, and that it is injective because $\zeta^a = \zeta^b \implies a \simeq b \mathrm{mod} n$. Finally, we check the homomorphic property by showing that

$$\phi(\bar{a} + \bar{b}) = \phi\overline{a + b} = \zeta^{a+b} = \zeta^a \zeta^b = \phi(a)\phi(b)$$

as required. Therefore $\mathbb{Z}_n$ is isomorphic to U_n.

3.5 Showing that two binary structures are not isomorphic

There are several sufficient conditions to show that binary structures are not isomorphic.

1. Showing that S and S' do not have the same cardinality.
2. Showing that the structural properties are different, e.g. if $*$ is commutative but $*'$ is not.
3. Showing the existence of an identity element for one operation but not the other.
4. Existence of solutions of equations

Definition 10. *$e \in S$ is an identity element for $*$ if $\forall\ s \in S, e * s = s * e = s$.*

For instance, on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, 0 is an identity element for addition and 1 is an identity element for multiplication.

Theorem 3.6. *If an identity element exists, it is unique.*

Proof. If we have two identities e and e', then

$$\begin{aligned} e * e' &= e' \\ e * e' = e' * e &= e \\ e &= e' \end{aligned}$$

□

Theorem 3.7. *Let $\phi : S \to S'$ be an isomorphism. If e is the identity element of $*$ on S, then $\phi(e)$ is the identity element of $*'$ on S'.*

Corollary 3.8. *If $\langle S, * \rangle$ has an identity element and $\langle S', *' \rangle$ does not have an identity element, then $\langle S, * \rangle$ and $\langle S', *' \rangle$ are not isomorphic.*

Proof.

$$\forall\ b \in S' \exists! a \in S\ s.t. \phi(a) = b$$

Then

$$\phi(e) *' b = \phi(e) *' \phi(a) = \phi(e * a) = \phi(a) = b$$

and

$$b *' \phi(e) = \phi(a) *' \phi(e) = \phi(a * e) = \phi(a) = b$$

Therefore $\phi(e)$ is an identity for $*'$. □

The fourth possible condition, existence of solutions, can be shown via the following example: $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Q}, + \rangle$ are not isomorphic because $x + x = 1$ has a solution over $\mathbb{Q}$ but not over $\mathbb{Z}$.

Math 113: Abstract Algebra **Spring 2019**

Lecture 4: Groups

Lecturer: Sylvie Corteel *30 January* *Aditya Sengupta*

4.1 Definition and Examples

Definition 11. *A group $(G, *)$ is a set G closed under $*$ such that*

1. *$*$ is associative: $(\forall\ a, b, c \in G, a * (b * c) = (a * b) * c)$*
2. *G has an identity element: $\exists\ e \in G$ such that $\forall\ g \in G, g * e = e * g = g$*
3. *Every element of G has an inverse: $\forall\ a \in G, \exists a' \in G$ such that $a * a' = a' * a = e$.*

Definition 12. *A group is abelian if $*$ is also commutative.*

When G is abelian, we often use the following notation:

Operation	Identity	Inverse
$+$	0	$-a$
$\cdot$	1	a^{-1}

Some examples of groups are $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$, and $(\mathbb{C}, +)$. $(\mathbb{Z}^+, +)$ is not a group as no inverses exist and there is no identity element. $(\mathbb{Z}^+, \cdot)$ is not a group as inverses do not exist for every element.

$(\mathbb{Q}^*, \cdot)$ is an abelian group, but $(\mathbb{Q}, \cdot)$ is not a group because it includes zero which does not have an inverse.

Consider the set of $n \times n$ matrices with real entries, under addition and matrix multiplication. The former is a group, as its elements follow the same logic as $(\mathbb{R}, +)$ being a group (adding term by term). It is also abelian. The latter is not a group, as inverses do not exist for matrices with determinant zero. We can exclude these to make the set $GL_n(\mathbb{R}) = M \in M_n(\mathbb{R}) \mid \det(M) \neq 0$, which gives us the valid (though non-abelian) group $\{GL_n(\mathbb{R}), \cdot\}$.

Consider the set of ismorphisms $\phi : G \to G$, with composition as the operation. This is a group, with the identity operation being the identity isomorphism $\phi : G \to G, g \to g$.

We return to the canonical example $(\mathbb{Z}_n, +)$. Recall that this is defined as $\mathbb{Z}_n = \{\overline{m} \mid m \in \mathbb{Z}\}$, where $a \in \overline{m}$ iff $a \simeq m \bmod n$. Therefore $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. We can see that this is a valid group under addition. Addition is associative, $\bar{0}$ is a valid identity element, and the inverse of any element $\bar{a}$ is $\overline{n-a}$. Addition modulo n follows the rule $\bar{a} + \bar{b} = \overline{a+b}$, therefore we can say $\bar{a} + \overline{n-a} = \bar{n} = \bar{0}$.

We can extend the definition to only include coprime elements,

$$\mathbb{Z}_n^* = \{\overline{m} \mid m \in \mathbb{Z} \text{ and } \gcd(m, n) = 1\}$$

For example, $\mathbb{Z}_3^* = \{\bar{1}, \bar{2}\}$, and $\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}$.

Here, multiplication is well defined, and $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$. To check that this is well-defined, take any $m_1, m_2 \in \bar{a}$ and any $m_3, m_4 \in \bar{b}$. Then, we can show that

$$m_1 \cdot m_3, m_2 \cdot m_4 \in \overline{a \cdot b}$$

We do this by rewriting m_1. By definition, $m_1 \in \bar{a}$ means $\exists\ k_1$ such that $m_1 = k_1 n + a$, and similarly for $m_3, \exists\ k_3$ such that $m_3 = k_3 n + b$. Multiply them explicitly:

$$m_1 \cdot m_3 = (k_1 n + a)(k_3 n + b) = n(k_1 b + k_3 a + k_1 k_3 n) + ab \in \overline{a \cdot b}$$

We also know that multiplication is associative. To check for a group, we now have to find an identity element, i.e. some $\bar{e}$ such that $\bar{e} \cdot \bar{k} = \bar{k} \cdot \bar{e} = \bar{k}$. This is true of $\bar{1}$. Finally, we need to find an inverse element. Recall that if $\gcd(m, n) = 1$, then $\exists!\ x, y \in \mathbb{Z}$ such that $xm + yn = 1$. With this, we can say that the inverse of $\overline{m}$ is $\bar{x}$.

4.2 Left and right cancellation laws

Theorem 4.1. *$\forall\ a, b, c \in G$, if $a * b = a * c$, then $b = c$, and if $b * a = c * a$, then $b = c$.*

This can be proved using the fact that every element has an inverse and that the operation is associative.

Proof. Suppose $a * b = a * c$. Let a' be the inverse element of a, that is, $a' * a = e$. Then, we left multiply by a', to get

$$a' * (a * b) = a' * (a * c)$$

Using associativity,

$$\begin{aligned} (a' * a) * b &= (a' * a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

□

The proof for the right cancellation law proceeds similarly.

Theorem 4.2. *If $(G, *)$ is a group and $a, b \in G$, then the equations*

$$\begin{aligned} a * x &= b \\ y * a &= b \end{aligned}$$

have unique solutions in G.

Proof. Let a' be the inverse of a. Then,

$$a' * (a * x) = a' * b$$

By associativity, this is also

$$\begin{aligned}(a' * a) * x &= a' * b \\ e * x &= a' * b \\ x &= a' * b\end{aligned}$$

Therefore a solution exists. Uniqueness can be shown through the uniqueness of the identity and inverse in a group. □

Theorem 4.3. *For any group $(G, *)$, the identity element and inverse element of every element is unique.*

Proof. For some $a \in G$, suppose $\exists a', a'' \in G$, such that $a' * a = a'' * a = e$. We apply the right cancellation law and find that $a' = a''$. (Note: convince yourself that this is not circular. It seems like the right cancellation law is dependent upon inverses being unique.) □

Math 113: Abstract Algebra **Spring 2019**

Lecture 5: Group Properties

Lecturer: Sylvie Corteel *1 February* *Aditya Sengupta*

5.1 Inversion Law

Theorem 5.1. *Let $(G, *)$ be a group and let $a, b \in G$. Then $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Proof. By associativity, we can write

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a{-}1$$

This simplifies to

$$(a * b) * (b^{-1} * a^{-1}) = a * e * a^{-1} = (a * e) * a^{-1}$$

which is

$$(a * b) * (b^{-1} * a^{-1}) = a * a^{-1} = e$$

□

5.2 Finite Groups

Definition 13. *If G has n elements, we say that G is finite and has order n.*

We denote this by $|G| = n$.

If G is isomorphic to G', we write $G \cong G'$. Recall that this means there exists a bijection $\phi : G \to G', g \to \phi(g)$ which satisfies the homomorphic property. Note that $\cong$ is an equivalence relation on the set of groups.

5.3 Groups of order 2

Suppose there is a group $(G, *)$ with $G = \{e, a\}$. We can construct a table defining the binary operation on these two.

$*$	e	a
e	e	a
a	a	e

These arise from necessary conditions on a group, i.e. that the identity must be such that $a * e = e * a = a$ and all elements must have an inverse. We can see this in the group $(\mathbb{Z}_2, +)$, where we send $e \to \bar{0}$ and $a \to \bar{1}$.

5.4 Groups of order 3

We can analyze this similarly.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

For the operation to be well-defined, this must be tbe table. Each element must show up once per row. This group is isomorphic to $(\mathbb{Z}_3, +)$

5.5 Groups of order 4

In general, this is not an easy problem, but for order 4, we can write out both the possibilities. We can write $(\mathbb{Z}_4, +)$,

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

and we can make the Klein 4-group that is not isomorphic to this,

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Although these are not isomorphic, they are both abelian. The Klein 4-group $(V, *)$ is isomorphic to $(\mathbb{Z}_2 \times Z_2, +)$.

5.6 Products of groups

Theorem 5.2. *Let G_1 and G_2 be groups under $*_1$ and $*_2$. Then $G_1 \times G_2$ is a group where $\forall\ x_1, y_1 \in G_1$ and $\forall\ x_2, y_2 \in G_2$, $(x_1, x_2) * (y_1, y_2) = (x_1 * y_1, x_2 * y_2)$.*

Proof. As $*_1$ and $*_2$ are associative, $*$ is associative. The identity is (e_1, e_2), and the inverse of (x_1, x_2) is (x_1^{-1}, x_2^{-1}). □

5.7 Subgroups

Definition 14. *A subgroup $(H, *)$ of a group $(G, *)$ is a subset H of G which is closed under $*$.*

We denote this by $H \leq G$, with the idea that H is a proper subgroup of G denoted by $H < G$.

Remark 5.3. *1. The operations need to be the same. For example, $\mathbb{Q}^+ \subset \mathbb{R}$ and $(\mathbb{Q}^+, \cdot)$ is a group but it is not a subgroup of $(\mathbb{R}, +)$.*

2. Every nontrivial group $(G, *)$ has at least two subgroups: G itself and $(e, *)$.

We can list the subgroups of $(\mathbb{Z}_4, +)$. A candidate for a two-element subgroup is $\bar{0}, \bar{1}$, but this is not closed under addition as $\bar{1} + \bar{1} = \bar{2}$. A two-element subgroup is $\bar{0}, \bar{2}$, and this is isomorphic to $(\mathbb{Z}_2, +)$. The zero element with addition would be a subgroup of this. The subgroups of V can be enumerated as e, a, e, b, e, c.

Theorem 5.4. *If $H \leq G$ then $e \in H$.*

Proof.

$$\forall\ a \in H, a * x = a$$

The above equation has a unique solution in G and in H, that is the same in both. In G this solution is $x = e$ by definition. Therefore this is also the solution in H, and so $e \in H$. □

Theorem 5.5. *If $a \in H$ and $H \leq G$, then $a^{-1} \in H$, where a^{-1} is the inverse of a in G.*

Proof.

$$\forall\ a \in H, a * x = e$$

The above equation has a unique solution in H and G. In G the solution is a^{-1}, therefore $a^{-1} in H$. □

Theorem 5.6. *A subset H of a group G is a subgroup of G if and only if H is closed under the binary operation of G, the identity element $e \in H$, and $\forall\ a \in H, a^{-1} \in H$.*

Proof. If H is a subgroup, it is itself a group, therefore the three conditions hold. Conversely, if the three conditions hold, it must be shown that these are sufficient to show that it is a subgroup. First, the operation is well-defined, the binary operation is associative, there is an identity element, and finally, there is an inverse for every element. Therefore $H \leq G$. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 6: Cyclic groups and orders

Lecturer: Sylvie Corteel *4 February* *Aditya Sengupta*

6.1 Examples of subgroups

Consider $GL_n(\mathbb{R})$, the set of invertible $n \times n$ matrices: $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$. Then, consider $SL_n(\mathbb{R})$, the set of $n \times n$ matrices with determinant 1. Then, we claim that $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Proof. 1. Closure under the binary operation.

$$\det(AB) = \det(A)\det(B)$$

Therefore if $A, B \in SL_n(\mathbb{R})$, then $\det(AB) = 1 \cdot 1 = 1$.

2. The identity element.
   I is the identity element. We know that $\det(I) = 1$, and therefore $I \in SL_n(\mathbb{R})$.
3. The inverse.
   For some matrix $A \in SL_n(\mathbb{R})$, we know that the following condition on the determinant holds true:

$$1 = \det(I) = \det(AA^{-1}) = \det(A)\det(A^{-1}) = 1 \cdot \det(A^{-1})$$

Therefore the determinant of A^{-1} must be 1, so $A^{-1} \in SL_n(\mathbb{R}) \forall\ A \in SL_n(\mathbb{R})$ and the proof is complete.

□

Definition 15. *The center of a group G with operation $*$ is*

$$Z(G) = \{a \in G \mid \forall x \in G, x * a = a * x\}$$

The center of an abelian group is the whole group, and otherwise it is a subgroup. Therefore this definition claims that $Z(G) \leq G$.

Proof. We first show that commutativity is closed under the operation $*$:

$$\forall\ a, b \in Z(G), (a * b) * x = a * (b * x) = a * (x * b) = (a * x) * b = (x * a) * b = x * (a * b)$$

Therefore if two elements commute with any element x of a group for which $*$ is defined, then their product also commutes with x.

Then, by definition of the identity, we can show that $e \in Z(G)$:

$$\forall\ x \in G, x * e = e * x = x \implies e \in Z(G)$$

Finally, we can show that inverses of elements of $Z(G)$ are also in $Z(G)$. Consider an arbitrary commutative product, and left and right multiply it with the inverse,

$$\begin{aligned} x * a = a * x \implies a^{-1} * (x * a) * a^{-1} &= a^{-1} * (a * x) * a^{-1} \\ (a^{-1} * x) * (a * a^{-1}) &= (a^{-1} * a) * (x * a^{-1}) \\ a^{-1} * x * e &= e * x * a^{-1} \\ a^{-1} * x &= x * a^{-1} \end{aligned}$$

□

6.2 Cyclic subgroups

Lemma 6.1. *Let $a \in G$. If a subgroup $H \leq G$ contains a, then it also contains $a^n \forall\ n \in \mathbb{Z}$, i.e. it contains $a^2 = a * a, a^3 = a * a * a, \ldots$ and $a^{-1}, a^{-2} = a^{-1} * a^{-1}, a^{-3} = a^{-1} * a^{-1} * a^{-1}, \ldots$.*

In addition to this, the set of exponentials of any element of a group forms a subgroup of that group:

Theorem 6.2. *Let G be a group and let $a \in G$. Then $H = \{a^n \mid n \in Z\}$ is a subgroup of G.*

Proof. We can show closure as being equivalent to addition in $\mathbb{Z}$; $\forall\ s, r \in \mathbb{Z}, a^s * a^r = a^{s+r}$. The identity element a^0 is present, and the inverse of any a^n is present: $a^n \in H \forall\ n \in Z \implies (a^n)^{-1} = a^{-n} \in H$ because $-n \in \mathbb{Z} \forall\ n \in Z$. Therefore this is a subgroup. □

Remark 6.3. *Given $a \in G$, $H = \{a^n \mid n \in \mathbb{Z}\}$ is the smallest subgroup of G that contains a. (This is intuitively true but prove?)*

Definition 16. *Call $\{a^n \mid n \in \mathbb{Z}\}$ the cyclic subgroup generated by a, and denote it by $\langle a | a \rangle$.*

6.3 Cyclic groups

Definition 17. *A group G is cyclic if there exists $a \in G$ such that $G = \langle a \rangle$. We say that a generates G.*

We claim that if a generates G then so does a^{-1}:

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{a^{-n} \mid n \in \mathbb{Z}\} = \langle a^{-1} \rangle$$

For example, consider the integers modulo 4 under addition, $(\mathbb{Z}_4, +)$. The group is generated by $\bar{1}$. Applying $\bar{1}$ to itself under addition repeatedly, we get

$$\bar{1}, \bar{1}+\bar{1}=\bar{2}, \bar{1}+\bar{1}+\bar{1}=\bar{3}, \bar{1}+\bar{1}+\bar{1}+\bar{1}=\bar{0}$$

which generates the whole group.

As stated above, we know that a^{-1} also generates G if a does. Here, $\bar{3}$ is the inverse of $\bar{1}$, and we can see by repeatedly applying $\bar{3}$ to itself under addition that G is also generated by $\bar{3}$.

Another example is $(\mathbb{Z}, +)$, which is cyclic and is generated either by 1 or -1.

$$\mathbb{Z} = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \langle 1 \rangle$$

$(\mathbb{Z}_n, +)$ is also cyclic and is generated by either $\bar{1}$ or $\overline{n-1}$. Another example that somewhat explains the origin of the term *cyclic* is the n^{th} roots of unity under multiplication.

$$U_n = \{e^{2i\pi k/n} \mid k \in \mathbb{Z}\}$$

Consider the Klein 4-group V from the previous lecture, as defined by a table. We want to find out whether this group is cyclic. We look at the subgroups generated by each element individually,

$$\begin{aligned}\langle a \rangle &= \{e, a\} \\ \langle b \rangle &= \{e, b\} \\ \langle c \rangle &= \{e, c\}\end{aligned}$$

Therefore this group is not cyclic.

$(\mathbb{Q}, +)$ is not cyclic, because $\forall q \in \mathbb{Q}, \langle q \rangle = \{nq \mid n \in \mathbb{Z}\} < \mathbb{Q}$.

Theorem 6.4. *Every cyclic group $(G, *)$ is abelian.*

Proof. Consider a cyclic group G that is generated by a. Then, take $x, y \in G$. Then there exist $r, s \in \mathbb{Z}$ such that $x = a^r, y = a^s$. Therefore

$$x * y = a^r * a^s = a^{r+s} = a^s * a^r = y * x$$

□

Definition 18. *Let G be a group and let $a \in G$. If $a^m = e$ for some $m \in \mathbb{Z}^+$, then we define the smallest such m to be the order of a, and we write $O(a) = m$. We say that a has finite order.*

We propose that if G is a finite group, then all the elements of G have finite order.

Proof. Suppose that $|G| = n$, then, $\forall\ a \in G, a, a^2, a^3, \ldots, a^{n+1}, \cdots \in G$. By the pigeonhole principle, $\exists r < s$ such that $a^r = a^s$. Therefore $a^{s-r} = e$ and so a has finite order. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 7: Cyclic Groups contd.

Lecturer: Sylvie Corteel *6 February* *Aditya Sengupta*

7.1 Cyclic Subgroups

Recall the definition of a cyclic group as given by Definition 17. We state a theorem on cyclic groups:

Theorem 7.1. *Any subgroup of a cyclic group is cyclic.*

The proof of this will depend on the division theorem,

Theorem 7.2. $n \in \mathbb{Z},\ m \in \mathbb{Z}^+$ *means* $\exists q, r \in \mathbb{Z}$ *such that* $n = qm + r$ *and* $0 \leq r < m$.

We can now prove that any subgroup of a cyclic group is cyclic.

Proof. Let G be generated by a and let $H \leq G$. In the case where $H = \{e\}$, then $H = \langle e|e\rangle$, which means H is cyclic as required. In the case where $H \neq \{e\}$, there exists $a^k \in H$ for $k \in \mathbb{Z}^+$, because G is generated by a. Let m be the smallest positive integer such that $a^m \in H$, and let $c = a^m$. We claim that H is generated by c. Since $c \in H$, $\langle c|c\rangle \subseteq H$. So we need to show that $H \subseteq \langle c|c\rangle$. To show this, let $b \in H$, then $\exists n \in \mathbb{Z}$ such that $b = a^n$. By the division theorem, $n = qm + r$ with $q \in \mathbb{Z}$ and $0 \leq r \leq m$. Therefore

$$b = a^n = a^{qm+r} = c^q * a^r$$

Since $b \in H, c \in H$, by closure of H under $*$ we can say

$$c^{-q} * b = a^r$$

Therefore $a^r \in H$. However, we started with the claim that m was the smallest positive integer such that $a^m \in H$, and now we have found an r such that $0 \leq r < m$ and $a^r \in H$. This means $r = 0$ and the identity element $a^0 = e \in H$. This means

$$c^{-q} * b = e \implies b = c^q$$

Therefore, every element of H is a power of c, which implies that $H \subseteq \langle c\rangle$. Since we also showed that $\langle c\rangle \subseteq H$, we can conclude that $H = \langle c\rangle$, i.e. H is the cyclic group generated by c. This completes the proof. □

7.2 Subgroups of $(\mathbb{Z}, +)$

We previously proved that $(\mathbb{Z}, +)$ is cyclic, which means we now know that all the subgroups of it are cyclic. For any $n \in \mathbb{Z}$, the subgroup generated by n is

$$\langle n \rangle = \{nk \mid k \in \mathbb{Z}\} = n\mathbb{Z}$$

which is all the multiples of n. The subgroups of $(\mathbb{Z}, +)$ are precisely $(n\mathbb{Z}, +), n \in \mathbb{N}$.

Definition 19. *Given $r, s \in \mathbb{Z}$, let $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$.*

We claim that H is a subgroup of $(\mathbb{Z}, +)$ with addition.

Proof. We first show that H is closed under addition. Let $n_1, m_1 \in \mathbb{Z}$ and let $n_2, m_2 \in \mathbb{Z}$. We know that

$$n_1 r + m_1 s \in H,\ n_2 r + m_2 s \in H,\ (n_1 + n_2)r + (m_1 + m_2)s \in H$$

because $n_1 + n_2, m_1 + m_2 \in \mathbb{Z}$.

Then, we can show that the identity element exists: $0 \cdot r + 0 \cdot s = 0$. Finally, we can show the existence of an inverse: if $nr + ms \in H$, then $-(nr + ms) = (-n)r + (-m)s \in H$. Therefore $H \leq \mathbb{Z}$. □

As $H \leq \mathbb{Z}$, H is cyclic, therefore $\exists d \in \mathbb{Z}$ such that $H = \langle d \rangle = d\mathbb{Z}$. We claim that this number is the greatest common divisor of r and s: if $H = d\mathbb{Z}$, then $d = \gcd(r, s)$.

Proof. Since $d \in H$, we know that $\exists n, m \in \mathbb{Z}$ such that $d = nr + ms$. $r, s \in H$, because $r = 1r + 0s$ and $s = 0r + 1s$. Therefore d is a divisor of r and a divisor of s. For any divisor d' of r and s, we know that $n \cdot r$ is a multiple of d' and $m \cdot s$ is a multiple of d' as well. Therefore $nr + ms$ is a multiple of d'. But we know that this is a multiple of d. This means $d < \gcd(r, s)$. □

7.3 Structure of cyclic groups

Theorem 7.3. *Let G be a cyclic group. If the order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$. If the order of G is m, then it is isomorphic to $(\mathbb{Z}_m, +)$.*

Proof. Let $a \in G$ and $G = \langle a \rangle$. Consider the first case, with a G of infinite order. $\forall k \in \mathbb{Z}^+, a^k \neq e$, then every element of G can be expressed as a^m for a unique $m \in \mathbb{Z}$.If this were not unique, then there exist m_1, m_2 such that $m_1 < m_2$ and $a^{m_1} = a^{m_2}$, i.e. $a^{m_2 - m_1} = e$ which is a contradiction. Then, we build an isomorphism $\phi : G \to \mathbb{Z}, a^m \to m$. We can verify that this is a bijection, and also that it fulfils the homomorphic property,

$$\phi(a^m * a^n) = \phi(a^{m+n}) = m + n = \phi(a^m) + \phi(a^n)$$

Therefore $(G, *) \simeq (\mathbb{Z}, +)$.

Now, consider the second case, with a G of finite order. We know that $a^k = e$ for some $k \in \mathbb{Z}^+$. Let $m \in \mathbb{Z}^+$ be the smallest such k, i.e. the smallest positive integer such that $a^m = e$. For $s \in \mathbb{Z}$, we use the division theorem, $s = mq + r$ with $0 \leq r < m$ and $q \in \mathbb{Z}$. Therefore

$$a^s = (a^m)^q * a^r = a^r$$

Therefore every element of G is one of $a^0, a^1, \ldots, a^{m-1}$. We know that none of these are equal, otherwise there would be a contradiction with the definition of m. Finally, we can build the isomorphism $\phi : G \to \mathbb{Z}_m$, $a^r \to r$. We can check that it is a bijection, and homomorphic:

$$\phi(a^r * a^s) = a^{r+s} = \overline{r+s} = \phi(a^r) + \phi(a^s)$$

□

Math 113: Abstract Algebra **Spring 2019**

Lecture 8: Generating groups, relations on groups, permutation groups

Lecturer: Sylvie Corteel *8 February* *Aditya Sengupta*

8.1 Logistics

Homework 3 is Section 6, problems 8, 9, 17, 18, 24, 32, 50; Section 7, problems 1, 2, 5; and Section 8, problems 3, 4, 16. Office hours for next week are Tuesday 10am-12pm.

8.2 Structure of cyclic groups

Theorem 8.1. *If G is cyclic and finite and $|G| = n$ then $(G, *) \cong (\mathbb{Z}_n, +)$.*

Lemma 8.2. *Every subgroup of a cyclic group is cyclic.*

Theorem 8.3. *If G is a cyclic group of order n generated by a, and $b = a^r$, then b generates a cyclic subgroup $H \leq G$ of order $\frac{n}{gcd(n,r)}$.*

For example, consider $\mathbb{Z}_{12}$. It has subgroups $\langle\bar{2}\rangle$ and $\langle\bar{3}\rangle$, which share a subgroup $\langle\bar{6}\rangle$. $\langle\bar{2}\rangle$ has a subgroup $\langle\bar{4}\rangle$, and $\langle\bar{3}\rangle$ and $\langle\bar{4}\rangle$ share a subgroup $\langle\bar{0}\rangle$. Here, $\langle\bar{n}\rangle$ represents the set of subsets of $\mathbb{Z}_{12}$ such that they are multiples or divisors of n, e.g. $\langle\bar{4}\rangle = \langle\bar{8}\rangle = \{\bar{0}, \bar{4}, \bar{8}\}$. (Maybe this is actually addition mod 12? I'm a bit confused).

Proof.

$$(G, *) \cong (\mathbb{Z}_n, +)$$
$$\phi : G \to \mathbb{Z}_n, a^k \to k$$
$$\langle\bar{r}\rangle = \{\bar{u}r \mid u \in \mathbb{Z}\} = \{\overline{ur + vn} \mid u, v \in \mathbb{Z}\}$$

Let d be the GCD of n and r. Then

$$\langle d\rangle = d\mathbb{Z} = \{ur + vn \mid u, v \in \mathbb{Z}\}$$

therefore

$$\left\langle\bar{d}\right\rangle = \{\overline{ur + vn} \mid u, v \in \mathbb{Z}\} = \langle\bar{r}\rangle$$

As there are $\frac{n}{d}$ multiples of d in the set $\{0, 1, \ldots, n-1\}$, the order of $\left\langle\bar{d}\right\rangle = \frac{n}{d}$. □

Corollary 8.4. *If a is a generator of a cyclic group G of order n, then the other generators of G are the elements of the form a^r where $gcd(n, r) = 1$. We say that n and r are relatively prime.*

$(\mathbb{Z}_n, +)$ is generated by $\bar{1}$ but also by all $\bar{a}$ that are relatively prime to n.

8.3 Generating sets

Let G be a group and let $a, b \in G$. Let $\langle a \rangle$ be the smallest subgroup containing a. Let $\langle a, b \rangle$ be the smallest subgroup containing a and b, which is the same as the set of all finite products of integral powers of a and b. For example, $a^3b^4a^{-2}b^5a^7 \in \langle a, b \rangle$. (If the group is abelian, this can be simplified, but in general we say that it is not.)

For example, consider the Klein 4-group V. $\langle a \rangle = \{e, a\}$, $\langle b \rangle = \{e, b\}$, and $\langle c \rangle = \{e, c\}$. Also, $V = \langle a, b \rangle = \langle a, c \rangle = \langle b, c \rangle$. We can see by computing products on the Klein 4-group that any $\langle x, y \rangle$ will contain all the elements of V and will therefore be V. For example, $\langle a, c \rangle = \{e, a, c, a * c = b\}$.

Theorem 8.5. *Let G be a group such that $a_i \in G \ \forall i \in I$. The smallest subgroup containing all a_is is the subgroup generated by $\{a_i \mid i \in I\}$, that is, the set of all finite products of integral powers of G.*

Proof. Closure is trivial, the identity is given by $a_i^0 = e$, and inverses are given by

$$(a_1^{m_1} a_2^{m_2} \ldots)^{-1} = \ldots a_2^{-m_2} a_1^{-m_1}$$

□

Remark 8.6. *If this subgroup is all G then $\{a_i \mid i \in I\}$ generates G, and if I is finite, G is finitely generated.*

8.4 Presentation of a group

A group G can be written as

$$G = \langle generators \mid relations \rangle$$

A *relation* of a set of generators of a group is an equation that equates some product of generators and their inverses to the identity.

For example, say G has two generators a and b, and is abelian. We can write this as a relation,

$$aba^{-1}b^{-1} = e$$

Another example of a relation is when G has two generators a and b, where b is its own inverse. For this, we can write

$$b^2 = e$$

For example, a *dihedral group* D_n is the group of the symmetries of the $n-$gon. D_n can be generated by two generators, the rotation operator r which rotates the $n - gon$ by $\frac{2\pi}{n}$, and the reflection operator s. Then the group is defined by

$$D_n = \langle r, s \mid r^n = e, s^2 = e, (rs)^2 = e \rangle$$

8.5 Permutation Groups

These are our first non-abelian groups.

Definition 20. *A permutation σ of a set A (usually, but not always, finite) is a bijection from A to itself, i.e. a shuffling of the elements of A.*

We denote a permutation by a two-column bracketed table. Let $A = \{1, 2, \ldots, n\}$, then a general permutation is given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

The binary operation on permutations is composition, which is essentially applying two permutations one after another (right to left). For example, let the two permutations σ and τ be given by

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

Then their product is

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

We claim that $\sigma\tau$ is a permutation.

Proof. We first check that it is one-to-one. If $\sigma\tau(a_1) = \sigma\tau(a_2)$, and by definition $\sigma\tau(a_1) = \sigma(\tau(a_1))$ and $\sigma\tau(a_2) = \sigma(\tau(a_2))$, then we can use the fact that σ is one-to-one to show that $\tau(a_1) = \tau(a_2)$. We also know that τ is one-to-one, therefore $a_1 = a_2$. Then, we check that it is onto. Given $a \in A$, σ is onto, therefore $\exists a' \in A$ such that $\sigma(a') = a$. Also, τ is onto, so $\exists a'' \in A$ such that $\tau(a'') = a'$. Therefore $\exists a'' \in A$ such that $\sigma\tau(a'') = a$. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 9: Permutation groups

Lecturer: Sylvie Corteel *11 February* *Aditya Sengupta*

9.1 Permutation Groups

Let A be a set (not necessarily finite). Recall that a permutation σ of A is a bijection from A to itself. We denote by S_A the set of all permutations of A.. The product of two permutations is their composition, $\sigma\tau = \sigma \circ \tau$.

Theorem 9.1. *$(S_A, \cdot)$ is a group.*

Proof. We check all of the group axioms.

1. S_A is closed under composition; if $\sigma, \tau \in S_A$ then $\sigma\tau \in S_A$. (See the previous lecture.)
2. $\cdot$ is associative, because composition of functions is associative.

$$\forall\ \sigma, \tau, u \in S_A,\ \sigma \cdot (\tau \cdot u) = (\sigma \cdot \tau) \cdot u$$

   This is because $\forall a \in A,\ \sigma \cdot (\tau \cdot u)(a) = \sigma(\tau(u(a))) = (\sigma \cdot \tau) \cdot u(a)$.

3. There is an identity element, which is the permutation that maps every object to itself. $id : A \to A, a \to a$. By composition, it is easy to see that $\sigma \cdot id = id \cdot \sigma = \sigma$.
4. Every element has an inverse. We denote the inverse of σ by σ^{-1}.

$$\forall y \in A \exists! x \in A \text{ such that } \sigma(x) = y$$

   Then, we define $\sigma^{-1}(y) = x$. σ^{-1} is a permutation, and $\sigma \cdot \sigma^{-1} = \sigma^{-1} \cdot \sigma = id$.
   For example, let σ be defined as follows:

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

   Then, σ^{-1} is

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

   It can easily be observed that by carrying out these two permutations one after another, we get the identity.

□

Remark 9.2. *It does not matter what the elements of A are called; if A and B have the same cardinality, then $(S_A, \cdot) \cong (S_B, \cdot)$.*

We can build this isomorphism by assuming there exists a bijection $f : A \to B$. Then the isomorphism is $\phi : S_A \to S_B, \sigma \to f \circ \sigma \circ f^{-1}$. We see that this is an isomorphism because it is a composition of bijections. We can check the homomorphism property,

$$\phi(\sigma\tau) = f \circ \sigma \circ \tau \circ f^{-1} = f \circ \sigma \circ f^{-1} \circ f \circ \tau \circ f^{-1} = \phi(\sigma)\phi(\tau)$$

9.2 Symmetric Groups

Definition 21. *For $n \in \mathbb{Z}^+$, the symmetric group on n letters is the set of all permutations of $\{1, 2, \ldots, n\}$.*

For the case $n = 2$, the symmetric group is given by

$$\{\left(\begin{smallmatrix}1&2\\1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)\}$$

For the case $n = 3$, it is

$$\{\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)\}$$

Here, we are building a pattern relating to the order of S_n. We claim that $|S_n| = n!$.

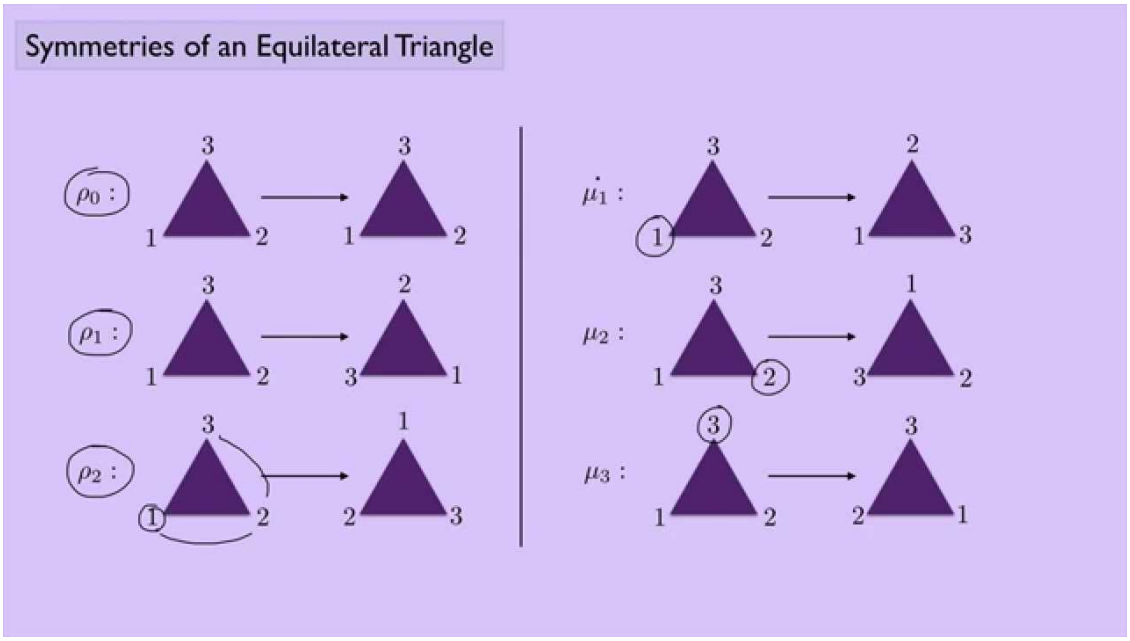
Proof. In a permutation of the integers from 1 to n, there are n choices for the output corresponding to 1, $n-1$ choices for the output corresponding to 2, and so on; overall, we get $n(n-1)(n-2)\cdots = n!$ choices. □

Note that S_3 is not an abelian group. This can be easily shown by multiplying together $\left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$ in both orders and comparing them.

S_3 is also not cyclic, which can be explicitly confirmed.

9.3 Geometric Interpretation

We can examine S_3 by the symmetries of a triangle. We claim that $S_3 \cong D_3$, the group of the symmetries of an equilateral triangle. The symmetries of an equilateral triangle are the rotations and reflections of the plane mapping the triangle to itself.



The symmetries are reflections about each of the three axes of the triangle (going through each vertex to the midpoint of the opposite line segment), and rotations of multiples of $\frac{2\pi}{3}$. We claim that every symmetry acts on the vertices by a permutation, and is uniquely determined by this permutation. By reflection about 1, we generate the mapping $(123) \to (132)$; about 2, we generate $(123) \to (321)$; about 3, we generate $(123) \to (213)$. These are the Levi-Civita indices that output -1. A rotation of $\frac{2\pi}{3}$ generates $(123) \to (231)$, and another generates $(123) \to (312)$. There is also the identity transformation with a rotation of 0, which generates $(123) \to (123)$. Therefore, we see that $\phi_3 : D_3 \to S_3$ is an isomorphism that maps the symmetries of the triangle to the permutations of $1, 2, 3$.

Is this true for any n? To investigate this, we look at the symmetries of the regular $n-$gon in the hopes of finding that D_n and S_n have the same order. Another way of asking this is: is it possible, using reflections and rotations, to reach any combination of indices? An example would be, in a square, the mapping $(1234) \to (2314)$.

This turns out to be false; rotations and reflections cannot change the neighbours of vertices, so there is no way to go from 4 being the neighbour of 1 and 3 to that of 1 and 2.

So what is the order of D_n? We claim that it is $2n$, which just happens to match up with $n!$ for $n = 3$ (because every node has two neighbours).

Proof. Let $1 \to i$, $1 \leq i \leq n$, so that there are n choices for the output to 1. For adjacency, 2 must be mapped to $i \pm 1$ modulo n, which leaves 2 choices. After this, the other elements are fixed. Therefore there are $2n$ choices. □

We get an injective homomorphism, i.e. a mapping $\phi_n : D_n \to S_n$ such that ϕ_n is injective and $\phi_n(xy) = \phi_n(x)\phi_n(y)$. We view the elements of D_n as permutations of the vertices. This is the first time an injective homomorphism has come up, so it is defined as follows:

Definition 22. *An injective homomorphism $\phi : G \to G'$ is an injective map such that $\phi(x * y) = \phi(x) *' \phi(y)$, where $(G, *)$ and $(G', *')$ are groups.*

Lemma 9.3. *Let $\phi : G \to G'$ be an injective homomorphism, where*

$$\phi[G] = \{g' \in G' \mid \exists g \in G \text{ such that } \phi(g) = g'\}$$

Then $(\phi[G], *') \cong (G, *)$.

Proof. We start by claiming that $\phi[G] \leq G'$. We see this because we know that $\phi[G]$ is closed under $*'$, $\phi(e) \in \phi[G]$, and inverses are present, $\phi(x^{-1}) = \phi(x)^{-1}$. To prove that $\phi : G \to \phi[G]$ is an isomorphism, we need to show it is a bijection and homomorphic. We know that it is injective and homomorphic, but it is also surjective by definition. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 10: Cayley's theorem, orbits and cycles

Lecturer: Sylvie Corteel *13 February* *Aditya Sengupta*

10.1 Cayley's theorem

Theorem 10.1. *Every group is isomorphic to a subgroup of a group of permutations.*

This is Cayley's theorem. We can prove it as follows,

Proof. We will show that G is a subgroup of S_G. The key observation is that in a group table, each row is a permutation in S_G. For example, we can define G as shown,

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Then, each row is a permutation of the elements of the group, i.e. each row is a member of S_G. We can therefore construct an injective homomorphism, $\phi : G \to S_G$. For $x \in G$, $\lambda_x : G \to G, g \to x * g$.

We claim that $\lambda_x \in S_G$. To do this, we need to prove that ϕ is a bijection. $\forall\, y \in G$, $\lambda_x(x^{-1} * y) = x * x^{-1} * y = y$, therefore λ_x is onto. $\forall\, y_1, y_2 \in G$, $\lambda_x(y_1) = \lambda_x(y_2)$ implies $x * y_1 = x * y_2$. By the cancellation law, $y_1 = y_2$ and so λ_x is one-to-one.

Therefore we construct the map $\phi : G \to S_G, x \to \lambda_x$. We claim that ϕ is an injective homomorphism. To show that it is injective, let $x_1, x_2 \in G$ such that $\phi(x_1) = \phi(x_2)$. This implies $x_1 * y = x_2 * y$, so by the cancellation law $x_1 = x_2$ and the map is injective. To show that it is a homomorphism, let $x, y \in G$. Given $g \in G$, we can say

$$\lambda_{x*y}(g) = x * y * g = x * \lambda_y(g) = \lambda_x(\lambda_y(g))$$

Therefore $\lambda_{x*y} = \lambda_x \cdot \lambda_y$ and we have the homomorphism property. By the lemma, since we know that there exists an injective homomorphism between an arbitrary group and a subgroup of the group of permutations, we know that there exists an isomorphism between them, and the theorem follows. □

10.2 Orbits and cycles

Let σ be a permutation of a set A. σ determines an equivalence relation on A. Given $a, b \in A$, $a \sim b$ if and only if $\exists n \in \mathbb{Z}$ such that $b = \sigma^n(a)$.

We claim that $\sim$ is an equivalence relation. To do this, we have to show the reflexive, symmetric, and transitive properties.

1. Reflexive: $\forall a \in A, a = \sigma^0(a)$.
2. Symmetric: if $a \sim b$ then $\exists n \in \mathbb{Z}$ such that $\sigma^n(a) = b$, therefore $\sigma^{-n}(b) = a$, so $b \sim a$.
3. Transitive: if $a \sim b$ and $b \sim c$, then $\exists n \in \mathbb{Z}$ such that $b = \sigma^n(a)$ and $\exists m \in \mathbb{Z}$ such that $c = \sigma^m(b)$. Then $c = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a)$, so $a \sim c$.

We can therefore partition A into the equivalence classes of A, which are called the *orbits* of σ. For example, consider the following permutations,

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

We repeatedly apply σ to itself, starting with the input 1. We see that $\sigma(1) = 4, \sigma^2(1) = 7, \sigma^3(1) = 1$. Therefore, an orbit of σ is $\{1, 4, 7\}$. Similarly, we find that the other orbits are $\{2, 5, 6\}$, $\{3\}$, and $\{8\}$. The size of an orbit is its number of elements. If an orbit has size 1, it is called a trivial orbit.

Similarly, τ has the cycles $\{1, 3, 4, 6\}$, $\{2, 7, 10\}$, and $\{5, 8, 9\}$.

Definition 23. *Given $\sigma \in S_A$, on each orbit, σ acts by a cyclic permutation. $\sigma \in S_A$ is a cycle if it has at most one nontrivial orbit.*

For example, consider a permutation given as follows,

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

The orbits of μ are $\{1, 3, 4, 6\}$ and the trivial orbits $\{2\}, \{5\}, \{7\}, \{8\}, \{9\}, \{10\}$. We write μ as the cycle $(1, 3, 6, 4)$ and stipulate that $\mu \in S_{10}$, which we note is equivalent to $(3, 6, 4, 1)$ or any other rotation of μ. This means that $\mu(1) = 3, \mu(3) = 6, \mu(6) = 4, \mu(4) = 1$. An integer not appearing in the cyclic notation is assumed to map to itself, i.e. it is fixed by the permutation.

Theorem 10.2. *Every permutation σ of a finite set is a product of disjoint cycles.*

Proof. Let $B_1, B_2, \ldots, B_r$ be the orbits of σ and $1 \leq i \leq r$. Define $\mu^{(i)}$ to be the cycle defined by

$$\mu^{(i)}(x) = \begin{cases} \sigma(x) & x \in B_i \\ x & \text{otherwise} \end{cases}$$

We claim that $\forall i$, $\mu^{(i)}$ is a cycle. The $\mu^{(i)}$s are disjoint because the B_is are disjoint. Clearly $\sigma = \mu^{(1)} \ldots \mu^{(r)}$, so it is the product of disjoint cycles and the proof is complete. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 11: Permutations, transpositions

Lecturer: Sylvie Corteel *15 February* *Aditya Sengupta*

11.1 Order of a permutation

The order of a permutation σ in S_n is the smallest possible m such that $\sigma^m = e$. If σ is a cycle, $(a_1, a_2, \ldots, a_k)$ then its order is k. If σ is the product of disjoint cycles, $\sigma = \tau_1\tau_2 \ldots \tau_n$, then exponentiation works: $\sigma^k = \tau_1^k\tau_2^k \ldots \tau_n^k$. Therefore the order $o(\sigma)$ is the least common multiple of the length of the τ_is.

Consider a perfect shuffle of a deck of 16 cards, in which cards alternate going into the left and right hands. This can be represented by a permutation,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 \end{pmatrix}$$

How many times do we have to do this shuffle before we get back to where we started? This number is equal to $o(\sigma)$. To find this, we write σ in cyclic notation,

$$\sigma = (2\ 3\ 5\ 9)(4\ 7\ 13\ 10)(6\ 11)(8\ 15\ 14\ 12)$$

The LCM of the lengths of the cycles (4, 4, 2, 4) is 4, so the order of σ is 4.

11.2 Transpositions, even and odd permutations

Definition 24. *A transposition is a cycle of length 2. That is, it swaps two elements and leaves all other elements fixed.*

Theorem 11.1. *Every cycle can be written as a product of transpositions.*

Consider a cycle $(a_1, a_2, \ldots, a_k)$. This is the product of left multiplying a series of transpositions,

$$(a_1, a_2, \ldots, a_k) = (a_1a_k) \ldots (a_1a_4)(a_1a_3)(a_1a_2)$$

Since any permutation can be written as a product of cycles, it can also be written as a product of transpositions. This representation is not unique; for example, $(1\ 5)(3\ 2) = (1\ 5)(1\ 3)(1\ 2)(1\ 3)$.

Theorem 11.2. *A product of an even number of transpositions cannot equal a product of an odd number of transpositions.*

Proof. We can denote a transposition by a matrix. The composition of two permutations then corresponds to matrix multiplication. Let A_σ be an $n \times n$ matrix with entries

$$a_{ij} = \begin{cases} 1 & i = \sigma(j) \\ 0 & \text{otherwise} \end{cases}$$

The action of the permutation σ on $(1\ 2\ \dots\ n)$ corresponds to left multiplication. For example, if the permutation is $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)$ then the corresponding matrix is

$$A_\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

We can verify by left multiplying that this creates the desired permutation of (1 2 3). We can check that $A_{\sigma\tau} = A_\sigma A_\tau$. Component-wise, this corresponds to

$$A_\sigma A_\tau = \sum_k a_{ik} b_{kj} = \begin{cases} 1 & a_{ik} = 1 \text{ and } b_{kj} = 1 \\ 0 & \text{otherwise} \end{cases}$$

which is the same as

$$A_{\sigma\tau,ij} = \begin{cases} 1 & i = \sigma \circ \tau(j) \\ 0 & \text{otherwise} \end{cases}$$

Suppose that $\sigma = \tau_1 \tau_2 \dots \tau_m$ where each τ_i is a transposition. Then $A_\sigma = A_{\tau_1} = A_{\tau_2} \dots A_{\tau_m}$, so by properties of determinants we have

$$\det(A_\sigma) = \det(A_{\tau_1}) \dots \det(A_{\tau_m})$$

Since each transposition corresponds to interchanging two rows of the identity matrix, we have $\det(\tau_i) = -1$, and so

$$\det(A_\sigma) = (-1)^m$$

If σ can be written as an even number of transpositions, its determinant is 1. If it can be written as an odd number of transpositions, its determinant is -1. So no permutation σ can be written as both. □

Definition 25. *If a permutation can be written as an even number of transpositions, we call it even, and if it can be written as an odd number of transpositions, we call it odd.*

Theorem 11.3. *Let A_n be the set of all even permutations in S_n. Then A_n is a subgroup of S_n.*

Proof. If $\sigma, \tau \in A_n$ then clearly $\sigma\tau \in A_n$. Since $e = (1\ 2)(1\ 2)$, for example, e is even. For inverses, assume that $\sigma \in A_n$ and we can show that $\sigma^{-1} \in A_n$. This can be written as transpositions,

$$\sigma = \tau_1\tau_2 \dots \tau_{2m}$$
$$\sigma^{-1} = \tau_{2m}^{-1}\tau_{2m-1}^{-1} \dots \tau_2^{-1}\tau_1^{-1} = \tau_{2m}\tau_{2m-1} \dots \tau_2\tau_1$$

Therefore the inverse exists, and is also even. □

A_n is called the alternating group on n letters.

We propose that $|A_n| = \frac{n!}{2}$.

Proof. Left multiplication by $(1\ 2)$ is a bijection from S_n to S_n. This maps even transpositions to odd ones and vice versa. Therefore the number of even and odd permutations must be equal, and they must sum to $n!$. We conclude that $|A_n| = \frac{n!}{2}$. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 12: Lagrange's Theorem, Cosets

Lecturer: Sylvie Corteel *20 February* *Aditya Sengupta*

12.1 Lagrange's Theorem

Theorem 12.1. *Let H be a subgroup of a finite group G. Then, the order of H divides the order of G.*

For example, let H be $(\mathbb{Z}_n, +)$. We saw previously that the subgroup generated by some element r, $\langle \bar{r} \rangle$, is of order $\frac{n}{d}$ where $d = \gcd(n, r)$. Another example is $(S_n, \cdot)$, which has subgroups A_n of order $\frac{n!}{2}, n \geq 2$ and D_n of order $2n$.Both of these divide $n!$

To go about proving Lagrange's theorem, we introduce some new terminology. If $H \leq G$, then $\forall a, b \in G$,

$$a \sim_L b \leftrightarrow a^{-1}b \in H$$
$$a \sim_R b \leftrightarrow ba^{-1} \in H$$

Then $\sim_L$ and $\sim_R$ are equivalence relations. If G is abelian, then $\sim_L$ and $\sim_R$ are the same. We can prove that these are equivalence relations.

Proof. To show that $\sim_L$ is an equivalence relation, it must be shown that it is reflexive, symmetric, and transitive. We know it is reflexive:

$$\forall\ a \in G, a^{-1}a = e \in H$$

Symmetric:

$$\forall\ a, b \in G, a \sim_L b \implies a^{-1}b \in H \implies (a^{-1}b)^{-1} \in H$$
$$b^{-1}a \in H \implies b \sim_L a$$

Transitive:

$$a \sim_L b, b \sim_L c \implies a^{-1}b \in H, b^{-1}c \in H$$

H is closed under the binary operation, so

$$(a^{-1}b)(b^{-1}c) \in H \implies a^{-1}c \in H \implies a \sim_L c$$

□

The equivalence classes for $\sim_L$ are the cells of a partition. For $a \in G$, what is the cell containing a?

Given $b \in G$, $a \sim_L b$ if and only if $a^{-1}b \in H$. Therefore $\exists h \in H$ such that $h = a^{-1}b$, or $ah = b$. Therefore, the cell containing a is $\{ah \mid h \in H\}$. We call this cell the *left coset* of H containing a, and we denote it by

$$aH := \{ah \mid h \in H\}$$

Similarly for $\sim_R$, we define the right coset of H containing a,

$$Ha := \{ha \mid h \in H\}$$

If G is abelian, the right and left cosets are the same. Later, we will see examples of groups having identical right and left cosets without the group being abelian.

Definition 26. *A subgroup $H \leq G$ is normal if its right and left cosets coincide.*

$$\forall\ a \in G, aH = Ha$$

For example, consider $(\mathbb{Z}_4, +)$, with a subgroup generated by 2, $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}$. We want to compute the left cosets of this group.

$$\bar{0} + \{\bar{0}, \bar{2}\} = \{\bar{0}, \bar{2}\}$$
$$\bar{1} + \{\bar{0}, \bar{2}\} = \{\bar{1}, \bar{3}\}$$

$\bar{2}$ and $\bar{3}$ are the same as $\bar{0}$ and $\bar{1}$ under addition of the subgroup elements in turn. Therefore, there are two left cosets, $\{\bar{0}, \bar{2}\}$ and $\{\bar{1}, \bar{3}\}$.

Another example is the Klein 4-group $V = \{e, a, b, c\}$, with the subgroup $\langle a \rangle = \{e, a\}$.

$$a * \{e, a\} = \{e, a\} = e * \{a, e\}$$
$$b * \{e, a\} = \{b, c\} = c * \{e, a\}$$

Therefore there are two left cosets, $\{e, a\}$ and $\{b, c\}$.

Another example is $(\mathbb{Z}, +)$ with a subgroup $(n\mathbb{Z}, +)$. There are n cosets, which are $3\mathbb{Z}, 1 + 3\mathbb{Z}$, etc.

Now, we can prove Lagrange's theorem. We do this by first proving that all cosets have the same cardinality.

Proof. We want to show that if $H \leq G$, then for all $a \in G$, $|aH| = |H|$. We do this by constructing a bijection,

$$\phi : H \to aH, h \to ah$$

ϕ is onto or surjective by the definition of aH, and ϕ is one-to-one:

$$\forall h_1, h_2 \in H, ah_1 = ah_2 \implies h_1 = h_2$$

Therefore ϕ is a bijection, so $|aH| = |H|$. Therefore all cosets have the same cardinality. $\square$

Math 113: Abstract Algebra **Spring 2019**

Lecture 13: Cosets, Lagrange's Theorem

Lecturer: Sylvie Corteel *22 February* *Aditya Sengupta*

13.1 Consequences of Lagrange's Theorem

Last time, we showed that aH and H have the same cardinality for any left coset aH. We can use this to prove Lagrange's theorem.

Proof. Given that $H \leq G$ for a finite G, we want to show that $|H|$ divides $|G|$. Let $|G| = n$ and let $|H| = m$. As shown before, every coset of H has the same cardinality as H, i.e. it has m elements. Let r be the number of cosets. As the cosets form a partition of G, we know that $n = r \cdot m$. Therefore m divides n. □

Theorem 13.1. *Every group of prime order (a finite group whose order is a prime number) is cyclic.*

Proof. Let $|G| = p$ where p is prime. Lagrange's theorem tells us that G has two subgroups; G itself and $\{e\}$. This is because the order of any subgroup must divide the order of the group, and by definition only 1 and p divide p. Let $a \in G, a \neq e$, and consider the subgroup $H = \langle a \rangle$. We know that H must include e, so its order is at least 2. Since its order is greater than 1, it must be p because this is the only other valid order of a subgroup for a group of prime order. Therefore $H = G$, so G is cyclic. □

Corollary 13.2. *If p is prime, there exists only one group of order p up to isomorphism.*

Recall the definition of an order of an element of a finite group,

Definition 27. *The order of an element $a \in G$ is the smallest integer $m \in \mathbb{Z}^+$ such that $a^m = e$. We denote this by $O(a) = m$.*

We can use this to state the following theorem.

Theorem 13.3. *Let $a \in G$ where G is finite. The order of a divides the order of the group.*

Proof. Let $a \in G$ and let $m = O(a)$. We know that $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. The order of $\langle a \rangle$ is m, and it is a subgroup. Therefore, since the order of a is the same as the order of $\langle a \rangle$, by Lagrange's theorem, m divides $|G|$. □

13.2 Indices of subgroups

Definition 28. *The index of H in G, denoted $(G : H)$, is the number of left cosets of H in G.*

For example, if $G = \mathbb{Z}_4$ and $H = \langle \bar{2} \rangle$, then $(G : H) = 2$. Another example is if $G = S_3$ and $H = \langle (12) \rangle$ then $(G : H) = 3$. This does not just apply to finite groups: if $G = \mathbb{Z}$ and $H = m\mathbb{Z}$ then $(G : H) = m$.

Remark 13.4. *If G is finite, then $(G : H) = \frac{|G|}{|H|}$.*

Theorem 13.5. *Let H, K be subgroups of G such that $K \leq H \leq G$. If $(H : K)$ is finite and $(G : H)$ is finite, then $(G : K) = (G : H)(H : K)$.*

We can prove this by explicitly multiplying the quotients of orders that make up the indices $(G : H)$ and $(H : K)$. If G is infinite, but the indices are finite (say $(G : H) = m$ and $(H : K) = r$), then G is partitioned into m left cosets, denoted a_iH, for $a_i \in G$. Similarly H is partitioned into r left cosets denoted b_jK. We claim that G is now partitioned into mr left cosets for K, by combining these two cosets. We want to show that $\forall g \in G \exists! i, j$ such that $g \in a_i b_j K$, but this is left as an exercise.

13.3 Maximal subgroups

Definition 29. *A subgroup K of a group G is maximal if there is no subgroup H such that $K < H < G$.*

Corollary 13.6. *If $K < G$ and $(G : K) = p$ with p prime then K is maximal.*

Proof. By contradiction, if there exists an H such that $K < H < G$ then $(G : K) = (G : H)(H : K)$. But $(G : K)$ is prime, so $(G : H) = 1$ or $(H : K) = 1$. This implies that either $H = G$ or $H = K$, i.e. $K < H < G$ does not hold. Therefore K is maximal. □

Definition 30. *The center of a group G is*

$$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\} \tag{13.1}$$

Definition 31. *Let $x \in G$, then the centralizer of x in G is $C_x(G) = \{g \in G \mid gx = xg\}$.*

We claim that $C_x(G) \leq G$ and $Z(G) \leq G$, so $Z(G) \leq C_x(G) \forall x \in G$.

We propose that if G is finite, either G is abelian (i.e. the center and the centralizer of G are both G itself) or $Z(G)$ is not maximal.

Proof. If G is abelian, this is trivial. If not, then $\exists x \notin Z(G)$ such that $Z(G) < C_x(G) < G$, i.e. $Z(G)$ is not maximal. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 14: Product Groups

Lecturer: Sylvie Corteel *27 February* *Aditya Sengupta*

14.1 Direct products

Let $G_1, \ldots, G_n$ be groups. Define the product of groups as follows:

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in G_i, i = 1, \ldots, n\} \tag{14.1}$$

For example, $\mathbb{Z}_2 \times \mathbb{Z}_3$ has six elements: $(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)$ with bars over all of them to denote congruence classes.

A valid operation on products of groups is component-wise multiplication, defined straightforwardly as

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n) \tag{14.2}$$

Theorem 14.1. *Let $G_1, \ldots, G_n$ be groups with operation $\cdot$; then, the direct product of $G_1, G_2, \ldots, G_n$, which is $\prod_{i=1}^{n} G_i$, is a group.*

Proof. We check the group axioms.

1. Closure: if $a_i, b_i \in G_i$, then $a_i b_i \in G_i$ because G_i is a group. Therefore $\prod_{i=1}^{n} G_i$ is closed under the operation.
2. Associativity: let $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$, $(c_1, \ldots, c_n) \in \prod_{i=1}^{n} G_i$. Then their products are $a_i(b_i c_i) = (a_i b_i c_i) = (a_i b_i)c_i$ as each G_i is a group. Therefore the operation is associative.
3. Identity: let e_i be the identity of G_i. Then, $(e_1, e_2, \ldots, e_n)$ will be the identity of $\prod G_i$. We can verify by taking products that this is an identity on the product group.
4. Inverse: $\forall (a_1, \ldots, a_n) \in \prod G_i, (a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$.

□

Addition can be considered to be component-wise. For example, in $\mathbb{Z}_2 \times \mathbb{Z}_3$, $(1,0) + (1,2) = (0,2)$; the first sum is done modulo 2 and the second is done modulo 3. This notion can allow us to define the idea of cyclic product groups; $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic and generated by $(1,1)$ as can be verified. This suggests that $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$. Similarly, we can see that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. It is isomorphic to the Klein 4-group V.

It seems like the product group defined by $\mathbb{Z}$ modulo two different integers is isomorphic to $\mathbb{Z}$ modulo the product of those integers if the integers are relatively prime. This turns out to be a theorem.

Theorem 14.2. *$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, and isomorphic to $\mathbb{Z}_{mn}$, if and only if gcd$(m, n) = 1$.*

Proof. Consider the cyclic subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by $a = (1, 1)$. $a + a + \cdots + a = (k, k)$ for a sum repeated k times. Then $(k, k) = (0, 0)$ if and only if k is a multiple of m and k is a multiple of n, i.e. k is a multiple of $\text{lcm}(m, n)$. We know that $\text{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$, so $\text{lcm}(m, n) = mn$ if and only if $\gcd(m, n) = 1$. If m and n are relatively prime, then $\langle a \rangle$ has order mn. Therefore $\langle a \rangle = \mathbb{Z}_m \times \mathbb{Z}_n$, and $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

We can prove this in the other direction: if $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and isomorphic to $\mathbb{Z}_{mn}$, then m and n are relatively prime. We proceed by contraposition. Suppose $\gcd(m, n) = d > 1$. We need to prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. To do this, we show that the subgroup generated by any element of $\mathbb{Z}_m \times \mathbb{Z}_n$ is a *proper* subgroup of the group. That is, for any $(u, v) \in \mathbb{Z}_m \times \mathbb{Z}_n$, $\langle (u, v) \rangle < \mathbb{Z}_m \times \mathbb{Z}_n$. The subgroup is defined by (ru, rv) where r is the number of additions of the same element carried out. If $(ru, rv) = (0, 0)$ then $r = \text{lcm}(m, n)$ (as r is a multiple of m and a multiple of n), which implies $r = \frac{mn}{d}$. So the order of any element of the group is less than or equal to r, which is less than mn as long as $d > 1$. Therefore the order of $\langle (u, v) \rangle$ is strictly less than mn. This implies that there is no element in $\mathbb{Z}_m \times \mathbb{Z}_n$ that generates the entire group, and $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. □

Corollary 14.3.

$$\prod_{i=1}^{n} \mathbb{Z}_{m_i} \mid m_i \in \mathbb{Z}^+$$

is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \ldots m_n}$ if and only if the m_is are pairwise relatively prime, i.e. gcd$(m_i, m_j) = 1$ for all $i \neq j$.

In particular, let $N = \prod p_i^{n_i}$. Then $\mathbb{Z}_N \simeq \prod \mathbb{Z}_{p_i^{n_i}}$. For example, $\mathbb{Z}_{60}$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

Theorem 14.4. *Let $(a_1, \ldots, a_n) \in \prod G_i$, and suppose that a_i has order r_i in G_i for $i = 1, 2, \ldots, n$. Then $(a_1, \ldots, a_n)$ has order lcm$(r_1, r_2, \ldots, r_n)$ in $\prod G_i$.*

Proof. $(a_1, \ldots, a_n)^k = (a_1^k, \ldots, a_n^k)$. This is the identity element iff k is a multiple of each r_i, which is equivalent to k being a multiple of the LCM of the r_is. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 15: Direct Product Groups

Lecturer: Sylvie Corteel *1 March* *Aditya Sengupta*

Recall that the order of an element in a direct product group is the LCM of the individual orders. For example, the order of $(4, 6, 15)$ in $\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20}$ is $\text{lcm}(3, 2, 4)$, which is 12. Another example is the order of $(4, (124)(35))$ in $\mathbb{Z}_{10} \times S_5$. 4 has order 5 and $(124)(35)$ has order 6, therefore the overall order is 30.

Remark 15.1. *Changing the order of factors in a direct product group yields a group isomorphic to the previous one. For example,*

$$G_1 \times G_2 \times G_3 \simeq G_3 \times G_1 \times G_2$$

with an isomorphism $\phi : G_1 \times G_2 \times G_3 \to G_3 \times G_1 \times G_2$, $(g_1, g_2, g_3) \to (g_3, g_1, g_2)$.

15.1 The structure of finitely generated abelian groups

Definition 32. *A group G is finitely generated if there exist $a_1, \ldots, a_k \in G$ such that*

$$\langle a_1, \ldots, a_k \rangle = G.$$

That is, there exists a finite subset of the elements of G that generates G.

Theorem 15.2. *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups.*

$$G \simeq \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z}^m$$

where $p_1, \ldots, p_n$ are prime and not necessarily distinct, and $r_1, \ldots, r_n$ are positive. This decomposition is unique up to the reordering of the factors.

For example, abelian groups of order 24 are (up to isomorphism) one of $\mathbb{Z}_8 \times \mathbb{Z}_3$, $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_4$, or $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition 33. *An integer is square free if it is not divisible by the square of any prime.*

An example of the structure theorem is the statement that if m is square free than any abelian group of order m is cyclic. From m being square free, we know that $m = \prod p_i$ where the p_is are distinct. Let G be an abelian group of order m. Then we know that $G \simeq \prod \mathbb{Z}_{p_i}$ Since $\gcd(p_i, p_j) = 1$ for all $i \neq j$, G is the product of relatively prime cyclic groups and so it is cyclic.

Using this theorem, we can show that $(\mathbb{Q}, +)$ is not finitely generated. Any subset of Q, consisting of $\frac{p_i}{q_i}$, $p_i \in \mathbb{Z}, q_i \in \mathbb{Z}^*$, $1 \leq i \leq k$, generates a subgroup of $\mathbb{Q}$ contained in $\frac{1}{lcm(q_i)}\mathbb{Z} < \mathbb{Q}$.

15.2 Decomposable Groups

Definition 34. *A group is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups.*

For example, $\mathbb{Z}_{mn}$ is decomposable into $\mathbb{Z}_m \times \mathbb{Z}_n$ if m and n are relatively prime.

Theorem 15.3. *The finite indecomposable abelian groups are exactly the cyclic groups of order equal to a power of a prime.*

Proof. By classification, if G is finite and abelian, then $G \simeq \prod \mathbb{Z}_{p_i^{r_i}}$. G is indecomposable if and only if $n = 1$, i.e. $G \simeq \mathbb{Z}_{p_1^{r_1}}$. □

Theorem 15.4. *If m divides the order of a finite abelian group G, then G has a subgroup of order m.*

Proof. By classification, $G \simeq \prod Z_{p_i^{r_i}}$. If m divides $|G|$, then $\exists 0 \leq s_i \leq r_i$ for $i = 1, \ldots, n$ such that

$$m = \prod_{i=1}^{n} p_i^{s_i}$$

For each $i = 1, 2, \ldots, n$, $\mathbb{Z}_{p_i^{r_i}}$ has a subgroup of order $p_i^{s_i}$, i.e. $\left\langle p_i^{r_i - s_i} \right\rangle$. Then the direct product of the subgroups thus generated has order m. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 16: Real Group Theory

Lecturer: Sylvie Corteel *4 March* *Aditya Sengupta*

16.1 Homomorphisms

Let G and G' be groups, both having the operation $\cdot$; then a map $\phi : G \to G'$ is a homomorphism if $\forall x, y \in G, \phi(xy) = \phi(x)\phi(y)$. For example, a trivial homomorphism would be $G \to G', g \to e'$ where e' is the identity of G'. We get

$$\phi(xy) = e' = e' \cdot e' = \phi(x)\phi(y)$$

Another example is left matrix multiplication, $\phi : \mathbb{R}^m \to \mathbb{R}^n, v \to Av$, where $A \in M_{m\times n}(\mathbb{R})$. ϕ is a homomorphism from $(\mathbb{R}^m, +)$ to $(\mathbb{R}^n, +)$, which we see as follows:

$$\phi(v_1 + v_2) = A(v_1 + v_2) = Av_1 + Av_2 = \phi(v_1) + \phi(v_2)$$

A third example is the determinant, $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*, \phi(A) = \det(A)$. This is a homomorphism because $\forall A, B \in GL_n(\mathbb{R}), \phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$.

Homomorphisms can represent most operations on groups; for example, a valid homomorphism is $S_n \to \mathbb{Z}_2, \sigma \to \begin{cases} 0 & \sigma \text{ is even} \\ 1 & \sigma \text{ is odd} \end{cases}$. Projection, and the modulo operator, can both also define homomorphisms.

16.2 Properties of homomorphisms

Definition 35. *Let ϕ be a map from X to Y where X, Y are sets. Then, the direct image of a subset $A \subseteq X$ under ϕ is*

$$\phi[A] = \{\phi(x) \mid x \in A\} \subseteq Y$$

and $\phi[X]$ is called the range of X.

For example, let $X = \{1, 2, 3, 4, 5, 6\}$ and let $Y = \{0, 1, 2, 3\}$. Consider $\phi : X \to Y, x \to x \bmod 3$. $A = \{2, 3, 5\}$, which has the image $\phi[A] = \{0, 2\}$. The range of X is $\phi(X) = \{0, 1, 2\}$.

Definition 36. *The inverse image of a subset $B \subseteq Y$ under ϕ is*

$$\phi^{-1}[B] = \{x \in X \mid \phi(x) \in B\} \subseteq X \tag{16.1}$$

Remark 16.1. *ϕ^{-1} does not exist as a map $Y \to X$ unless ϕ is bijective, but the inverse image is well defined for any map.*

Theorem 16.2. *Let $\phi : G \to G'$ be a homomorphism between groups G and G'. Then:*

1. *Let $e \in G, e' \in G'$ be the identity elements in both groups. Then $\phi(e) = e'$.*
2. *$\forall a \in G, \phi(a^{-1}) = \phi(a)^{-1}$.*
3. *$\forall H \leq G, \phi[H] \leq G'$.*
4. *$\forall H' \leq G', \phi^{-1}[H'] \leq G$.*

Proof.

1. $\phi(e) \cdot \phi(e) = \phi(e \cdot e) = \phi(e) = \phi(e) \cdot e'$. Then apply the left cancellation law to get $\phi(e) = e'$.
2. Let $a \in G$. Then $\phi(a) \cdot \phi(a^{-1}) = \phi(a \cdot a^{-1}) = \phi(e) = e'$. Left multiply by $\phi(a)^{-1}$, and we get $\phi(a^{-1}) = \phi(a)^{-1}$.
3. $H \leq G$. Let $a, b \in H$, $ab \in H$. We know that $\phi(a)\phi(b) = phi(ab) \in \phi[H]$, so $\phi[H]$ is closed under $\cdot$ which is the first subgroup axiom. We know that $\phi(e) \in \phi[H]$ as $e \in H$, and $\forall a \in H$, $\phi(a) \in \phi[H]$. Therefore $a^{-1} \in H$ as $H \leq G$, so $\phi(a^{-1}) = \phi(a)^{-1} \in \phi[H]$. Therefore $\phi[H]$ is a subgroup of G.
4. $H' \leq G'$ implies that $\forall a, b \in \phi^{-1}[H']$, $\phi(ab) = \phi(a)\phi(b) \in H'$, so $ab \in \phi^{-1}[H']$. $\phi(e) = e' \in H' \implies e \in \phi^{-1}[H']$. Finally, if $a \in \phi^{-1}[H']$ then $\phi(a^{-1}) = \phi(a)^{-1} \in H'$, so $a^{-1} \in \phi^{-1}[H']$. Therefore $\phi^{-1}[H'] \leq G$.

□

Math 113: Abstract Algebra **Spring 2019**

Lecture 17: Group homomorphisms

Lecturer: Sylvie Corteel *6 March* *Aditya Sengupta*

Definition 37. *The kernel of ϕ is Ker $\phi = \{x \in G \mid \phi(x) = e'\} = \phi^{-1}[\{e'\}]$, where e' is the identity of G'.*

For example, let $\phi_n : S_n \to \mathbb{Z}_2, \sigma \to \begin{cases} 0 & \sigma \text{ even} \\ 1 & \sigma \text{ odd} \end{cases}$. Then, $\operatorname{Ker} \phi_n$ is the set of permutations that map to zero, i.e. A_n.Another example is $\phi_n : \mathbb{Z} \to \mathbb{Z}_n, x \to x \mod n$. Then $\operatorname{Ker} \phi_n = n\mathbb{Z}$.

Corollary 17.1. *The kernel of ϕ is a subgroup of G.*

Proof. We proved that if $H \leq G$ then $\phi^{-1}[H^{-1}] \leq G$. As $\{e'\} \leq G', \operatorname{Ker} \phi \leq G$. □

Theorem 17.2. *Let $\phi : G \to G'$ be a group homomorphism. Let $H = \operatorname{Ker} \phi$ and $a \in G$. Then $\phi^{-1}[\{\phi(a)\}] = aH = Ha$.*

Recall that $aH = \{ah \mid h \in H\}$ and $Ha = \{ha \mid h \in H\}$. Therefore the above statement is equivalent to $\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\}$ (interpret this later). To prove this, we show that the sets are subsets of one another.

Proof. Fix $a \in G$ and let $S = \{x \in G \mid \phi(x) = \phi(a)\}$. We first try and show that $S \subseteq aH$. Let $x \in S$. Then $\phi(x) = \phi(a) \implies \phi(a)^{-1}\phi(x) = e'$. As ϕ is a homomorphism, we know that

$$\phi(a^{-1})\phi(x) = \phi(a^{-1}x) \implies a^{-1}x \in H \implies a(a^{-1}x) \in aH \implies x \in aH.$$

Therefore $S \subseteq aH$. Now we try the other direction. Let $y \in aH$. Then $\exists h \in H$ such that $y = ah$. Using the homomorphism property,

$$\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a),$$

because H is the kernel of ϕ. Since $\phi(y) = \phi(a)$, we know that $y \in S$ by definition. Therefore $aH \subseteq S$. This implies that $S = aH$. The argument proceeds similarly for the right cosets. □

An example of this is the kernel of ϕ_n as defined above. ϕ collapses the elements of $\operatorname{Ker} \phi = A_n$ to $e' = 0$, and any of the left cosets of ϕ collapses the elements of $\operatorname{Ker} \phi$ to the corresponding element of G'.

Corollary 17.3. *A group homomorphism ϕ is one-to-one or injective if and only if* $\operatorname{Ker} \phi = \{e\}$.

Proof. Suppose ϕ is one-to-one. Let $x \in \operatorname{Ker} \phi$. Then $\phi(x) = e' = \phi(e)$. Therefore $x = e$, so $\operatorname{Ker} \phi = \{e\}$. In the other direction, suppose $\operatorname{Ker} \phi = \{e\}$. Then $\forall a \in G$, let $x \in G$ such that $\phi(x) = \phi(a)$. Then $x \in aH$ where $H = \operatorname{Ker} \phi = \{e\}$. Therefore $aH = \{a\}$, implying that $x = a$. Therefore ϕ is one-to-one. □

Corollary 17.4. *$\phi : G \to G'$ is a group isomorphism if and only if ϕ is a group homomorphism,* $\operatorname{Ker} \phi = \{e\}$, *and ϕ is onto.*

Definition 38. *$H \leq G$ is normal if and only if $gH = Hg$ for all $g \in G$.*

Corollary 17.5. *If $\phi : G \to G'$ is a group homomorphism then* $\operatorname{Ker} \phi$ *is a normal subgroup.*

Theorem 17.6. *Given a subgroup $H \leq G$, the following are equivalent ways of expressing that H is a normal subgroup.*

1. $ghg^{-1} \in H \forall h \in H, g \in G$
2. $gHg^{-1} = H \forall g \in G$
3. $gH = Hg \forall g \in G$.

(Proof TBD.)

Math 113: Abstract Algebra **Spring 2019**

Lecture 18: Quotient Groups

Lecturer: Sylvie Corteel *8 March* *Aditya Sengupta*

Recall that the cosets of a subgroup $H \leq G$ are the set $aH = \{ah \mid h \in H\}$. Let $a, b \in G$; then $aH = bH$ if and only if $b \in aH$, or equivalently $a \in bH$. Recall also that a group homomorphism $\phi : G \to G'$ allows us to define its kernel, $H = \operatorname{Ker} \phi = \{x \in G \mid \phi(x) = e'\}$. For $a \in G$, $\phi^{-1}(\{\phi(a)\}) = aH = Ha$.

There exists a map

$$\mu : \{\text{cosets of } \operatorname{Ker} \phi\} \to \phi[G], aH \to \phi(a). \tag{18.1}$$

Theorem 18.1. *Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a quotient group where*

$$(aH) \cdot (bH) = abH \tag{18.2}$$

Moreover, μ is an isomorphism.

Denote the set of cosets of H by G/H, where $H \leq G$ and H is normal.

Proof. Let us first prove that μ is an isomorphism. μ is trivially well-defined, because $\phi(a) \in \phi[G] \forall a \in G$. Then, consider $a, a' \in G$. $aH = a'H$ if and only if $\phi(a) = \phi(a')$, so μ is a bijection. Finally,

$$\mu((aH)(bH)) = \mu(abH) = \phi(ab) = \phi(a) \cdot \phi(b) = \mu(aH) \cdot \mu(bH), \tag{18.3}$$

so the homomorphism property holds.

Now, we want to show that coset multiplication satisfies the group axioms.

1. Associativity: $\forall a, b, c \in G, ((aH)(bH))(cH) = (abH)(cH) = ((ab) \cdot c)H = (aH)(bcH) = (aH)((bH)(cH))$.
2. Identity: $eH = H$. $\forall a \in G, aH \cdot eH = aH$ and $eH \cdot aH = aH$. So eH is the identity element.
3. Inverse: $\forall aH \in G/H, aH \cdot a^{-1}H = aa^{-1}H = eH = H$ and $a^{-1}H \cdot aH = (a^{-1}a)H = eH$. So $(aH)^{-1} = a^{-1}H \in G/H$.

□

Recall that $H \leq G$ is a normal subgroup if and only if $\forall a \in G, aH = Ha$. We propose that if $H \leq G$ is a normal subgroup, then coset multiplication is a well defined operation on G/H.

Proof. What we need to prove is that for $a, a', b, b' \in G$, if $aH = a'H$ and $bH = b'H$ then $abH = a'b'H$. By definition, $\exists h_1, h_2 \in H$ such that $a' = ah_1$ and $b' = bh_2$. As H is normal, $bH = Hb$. So $\exists h_3 \in H$ such that $bh_3 = h_1 b$. Therefore,

$$\begin{aligned} a'b' &= ah_1bh_2 \\ &= a(h_1b)h_2 \\ &= abh_3h_2 \end{aligned} \tag{18.4}$$

As $H \leq G$, $h_3h_2 \in H$. Therefore $a'b' \in abH$. So $a'b'H = abH$. □

As an example, consider $\phi : \mathbb{Z} \to \mathbb{Z}_n, a \to a \mod n$. Then $\operatorname{Ker}\phi = n\mathbb{Z}$, and the set of cosets $G/\operatorname{Ker}\phi = \{a + n\mathbb{Z} \mid a = 0, 1, \ldots, n-1\}$. Then $\mu : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n, a + n\mathbb{Z} \to a \mod n$ associates to each coset of $n\mathbb{Z}$ its smallest non-negative element.

In $\mathbb{Z}/n\mathbb{Z}$, $a + n\mathbb{Z} + b + n\mathbb{Z} = a + b + n\mathbb{Z}$, and in $\mathbb{Z}_n$, $\bar{a} + \bar{b} = \overline{a+b}$.

Theorem 18.2. *Let $H \leq G$. Then left coset multiplication is well defined if and only if H is normal.*

Proof. We just proved that if H is normal then coset multiplication is well defined. We try and prove this in the other direction. Suppose that left coset multiplication is well defined, that is, $\forall a, b, a', b' \in G$, if $aH = a'H$ and $bH = b'H$ then $abH = a'b'H$. $\forall a \in G, \forall x \in aH$, we get $xHa^{-1}H = aHa^{-1}H = H$. Therefore $x \in Ha$, so $aH \subseteq Ha$. In the other direction, $\forall x \in Ha, \exists h \in H$ such that $x = ha$, so $x^{-1} \in a^{-1}H$. Therefore $\exists h_2 \in H$ such that $x^{-1} = h_2a^{-1}$, so $x \in aH$. Therefore $Ha \subseteq aH$, and the proof is complete. □

Theorem 18.3. *Let $H \leq G$ be a normal subgroup. Then G/H equipped with coset multiplication is a group called the quotient group.*

The proof is identical to the case $H = \operatorname{Ker}\phi$.

Math 113: Abstract Algebra **Spring 2019**

Lecture 19: Quotient Groups

Lecturer: Sylvie Corteel *11 March* *Aditya Sengupta*

Theorem 19.1. *Let $H \leq G$ be normal. Then $\gamma : G \to G/H, x \to xH$ is a surjective homomorphism with kernel H.*

Proof. We first show that it is a homomorphism.

$$\forall x, y \in G, \gamma(x \cdot y) = xyH = xH \cdot yH = \gamma(x) \cdot \gamma(y)$$

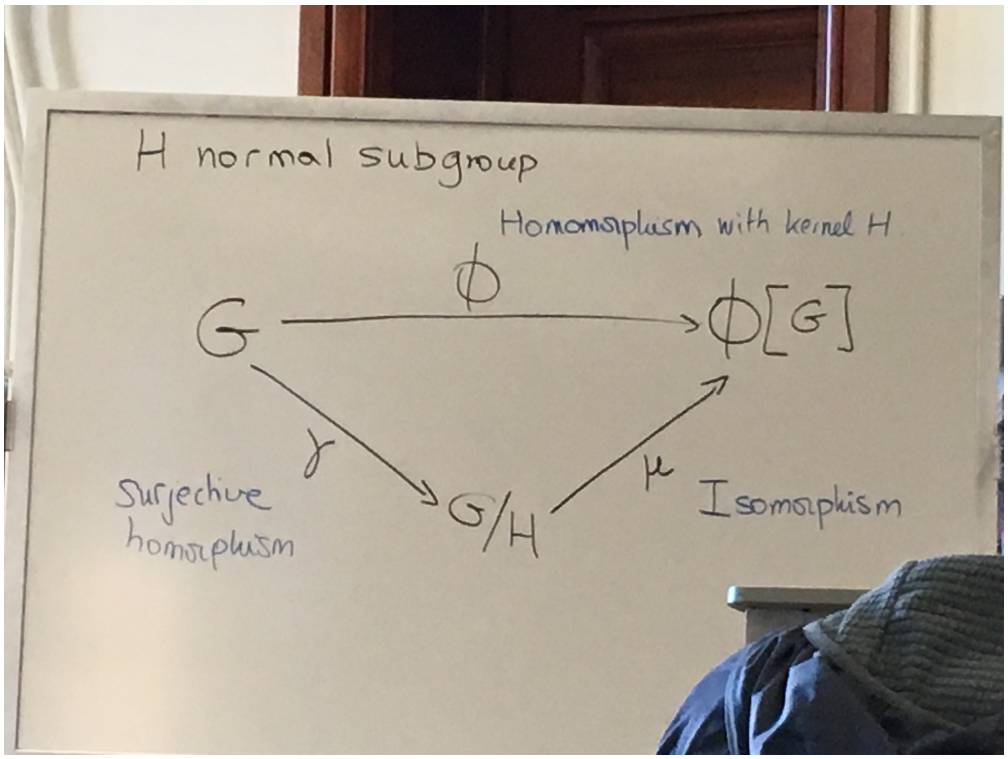
Then, we show it is surjective. Given any coset $aH \in G/H$, $a \in G$ and $\gamma(a) = aH$. So γ is surjective.

Finally, we compute the kernel and show that it is H.

$$\begin{aligned} \operatorname{Ker}\gamma &= \{x \in G \mid \gamma(x) = \gamma(e)\} \\ &= \{x \in G \mid \gamma(x) = H\} \\ &= \{x \in G \mid xH = H\} \\ &= \{x \in G \mid x \in H\} = H \end{aligned} \tag{19.1}$$

□

If H is a normal subgroup, then both a homomorphism $\phi : G \to \phi[G]$ with kernel H, and a surjective homomorphism $\gamma : G \to G/H$, can be defined. There also exists an isomorphism $\mu : G/H \to \phi[G]$.



Theorem 19.2. *Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\phi : G/H \to \phi[G], xH \to \phi(x)$ is an isomorphism. Moreover, if $\gamma : G \to G/H, x \to xH$ is a homomorphism, then $\phi = \mu \circ \gamma$.*

This is referred to as the *fundamental homomorphism theorem.*

For example, G/G is isomorphic to the trivial group. It has one coset, which is G itself. As another example, $G/\{e\} \simeq G$, where the cosets are single elements of G. Consider the homomorphism $pr : G_1 \times G_2 \to G_1, (x_1, x_2) \to x_1$. The kernel of pr is $\{e_1\} \times G_2$, and the cosets are

$$\{(x_1, e_2) \cdot \mathrm{Ker}(pr) \mid x_1 \in G_1\}$$
$$G_1 \times G_2/\{e_1\} \times G_2 \simeq G_1$$

Theorem 19.3. *The quotient of a cyclic group is cyclic.*

Proof. Let $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. If N is a normal subgroup of G, then by definition

$$G/N = \{a^n N \mid n \in \mathbb{Z}\}$$

Then, we use coset multiplication to find the generating element of the quotient group,

$$a^n N = (aN)^n; a^{-n} N = (a^{-1} N)^n = (aN)^{-n}$$

So G/N is cyclic and generated by aN. □

Example 19.4. *What is $\mathbb{Z} \times \mathbb{Z}/\langle (1,1) \rangle$? The subset is $H = \{(x,x) \mid x \in \mathbb{Z}\}$, so the cosets are*

$$\{(x,y) + H \mid (x,y) \in \mathbb{Z} \times \mathbb{Z}\} = \{(x,0) + H \mid x \in \mathbb{Z}\}$$

So $\mathbb{Z} \times \mathbb{Z}/H \simeq \mathbb{Z}$. This defines a group homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (x,y) \to x - y$. This is a group homomorphism with kernel equal to H.

Example 19.5. *What is $\mathbb{Z}_4 \times \mathbb{Z}_6/\langle (2,3) \rangle$? The subgroup is $\{(0,0),(2,3)\}$, of order 2. So the quotient group is of order 12, which means it is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. To find which, we claim that $(1,0) + H$ has order 4, which we can verify by noting that $(1,0) + H$ through $(3,0) + H$ are not H, but $(4,0) + H = H$. Therefore $\mathbb{Z}_4 \times \mathbb{Z}_6/\langle (2,3) \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$. We know this because we can verify that there is no element of order 4 in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$; any element $(a_1,a_2,a_3) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ has order $lcm(r_1,r_2,r_3)$ where r_i is the order of a_i. As r_1 divides 2, r_2 divides 2, and r_3 divides 3, the lcm of r_1,r_2,r_3 cannot be 4.*

Example 19.6. *Consider the dihedral group D_4 of the symmetries of the square. Its generators are rotation of $\frac{\pi}{2}$ and reflection about the y axis. We know that $r^4 = e, s^2 = e, (sr)^2 = e$. We can therefore write the cosets.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 20: Simple Subgroups, Commutators, Group Actions

Lecturer: Sylvie Corteel *13 March* *Aditya Sengupta*

Definition 39. *A group is simple if it is nontrivial and has no nontrivial, proper normal subgroups.*

Example 20.1. *$A_3 \leq S_3$ is simple since $A_3 = \{id, (123), 132\}$ has non nontrivial proper subgroups.*

In general, $\mathbb{Z}_p$ for a prime p are all simple, since they have no nontrivial proper subgroups.

Example 20.2. *A_4 is not simple, but $A_n, n \geq 5$ is simple. This was done by checking cases with a computer.*

Classifying simple groups took around 30 years but now it's done. There are 18 infinite families, and 26 sporadic groups (called that because there is no good intuition for them). The largest of these is the Munster Group, with order 8.08×10^{53}.

Definition 40. *Let G be a group. For any $a, b \in G$, the commutator is defined as $[a, b] = aba^{-1}b^{-1}$.*

Remark 20.3. *$[e, e] = e$ and $[a, a] = e$. If G is abelian then $[a, b] = e$ and $[b, a] = [a, b]^{-1}$.*

Proposition 20.4. *Consider $C = \{[a_i, b_i]_{i=0}^n \mid n > 0; a_i, b_i \in G\}$. Then $C \leq G$.*

Proof. $e = [e, e] \in C$, so the group has an identity element. C is closed under products by definition, since it expresses all products of a particular form. For inverses, let $[a_1, b_1] \dots [a_n, b_n] \in C$, then its inverse is just $[a_n, b_n]^{-1} \dots [a_1, b_1]^{-1} = [b_n, a_n] \dots [b_1 a_1] \in C$. □

Theorem 20.5. *C is a normal subgroup of G.*

Proof. First consider $[a, b] \in C$. Then $g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = ga(g^{-1}g)b(g^{-1}g)b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})($
$[gag^{-1}, gbg^{-1}]$. Each piece is a commutator in C from earlier, so the product is in C, and we conclude C is normal. □

Theorem 20.6. *For $N \leq G$ normal, G/N is abelian if and only if $C \subseteq N$.*

Proof. Suppose G/N is abelian, and let $aN, bN \in G/N$. Then $(aN)(bN) = (bN)(aN)$, so $abN = baN$ which requires $ab(ba)^{-1} \in N$. So $aba^{-1}b^{-1} \in N$ and $[a, b] \in N$. Since this holds $\forall a, b$, and N is closed under products, $C \subseteq N$.

Now suppose $C \subseteq N$, and we want to show G/N is abelian. Since $C \subseteq N, b^{-1}a^{-1}ba \in N$, so $b^{-1}a^{-1}baN = N$, and we have $abN = abN = (ab)(b^{-1}a^{-1}ba)N = baN = bNaN$, and so G/N is abelian. □

Definition 41. *An action of a group G on a set X is a map $* : G \times X \to X$ such that $e * x = x$ and $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G$. X with the operation $*$ is a G-set.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 21: Group Actions

Lecturer: Sylvie Corteel *15 March* *Aditya Sengupta*

Definition 42. *An action of a group G on a set X is a map $\phi : G \times X \to X, (g, x) \to g * x$ such that $e * x = x \forall x \in X$ and $(g_1 g_2) * x = g_1 * (g_2 * x) \forall g_1, g_2 \in G, x \in X$.*

We call X with this action a $G-$set. For example, if $X \subseteq S_x$ is a subgroup of the permutations of X, then H acts on X by $\sigma * x = \sigma(x)$. Another example is D_4 acting on a square, so it acts on the set $\{1, 2, 3, 4\}$ of the vertices of the square.

In general, G acts on itself by permutations, $g \in G$ sends $x \in X = G$ to $g * x$.

Theorem 21.1. *Given a $G-$set X, and $g \in G$, the map $\sigma_G : X \to X, x \to g * x$ is a permutation of X, and the map $\phi : G \to S_X$ is a group homomorphism $g \to \sigma_g$.*

It seems weird to say that σ_g is a permutation, but we can prove this using the group action axioms.

Proof.

$$\sigma_g(\sigma_{g^{-1}}(x)) = g * (g^{-1} * x) = (g * g^{-1}) * x = e * x = x = \mathrm{id}_x(x) \tag{21.1}$$

Similarly $\sigma_{g^{-1}}(\sigma_g(x)) = x$, so σ_g is a permutation.

We can verify that ϕ is a homomorphism, by the following:

$$\phi(g_1 g_2)x = sigma_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \sigma_{g_1}(\sigma_{g_2}(x)) = \phi(g_1)\phi(g_2) \tag{21.2}$$

□

Definition 43. *An action is faithful if the map ϕ is injective. This is equivalent to the statement that $\operatorname{Ker} \phi = \{e\}$; the only element of G that acts as the identity permutation is the actual identity.*

For example, S_x acts faithfully on X, and any subgroup $H \subseteq S_x$ acts faithfully. Again returning to D_4, a 180-degree rotation in D_4 that leaves all the lines of symmetry in place is not a faithful action. If $N = \operatorname{Ker} \phi$, then G/N acts faithfully on X.

Definition 44. *Given a $G-$set X and $x \in X$, define $G_x = \{g \in G \mid g * x = x\}$.*

Theorem 21.2. *$G_x \subseteq G$ is a subgroup. This is called the isotropy or stabilizer subgroup of X.*

Proof. Clearly $e \in G_x$. If $g \in G_x$ then $\sigma_{g^{-1}}(\sigma_g(x)) = x = \sigma_{g^{-1}}(x)$. So $g^{-1} * x = x$, so $g^{-1} \in G_x$. For closure, if $g_1, g_2 \in G_x$ then $(g_1 g_2) * x = g_1 * (g_2 * x) = g_1 * x = x$ so $g_1 g_2 \in G_x$. □

21.1 Orbits

Theorem 21.3. *For $x_1, x_2 \in X$, set $x_1 \sim x_2$ if and only if $\exists g \in G$ such that $g * x_1 = x_2$. Then $\sim$ is an equivalence relation.*

Proof. For the reflexive property, set $g = e$. For the symmetric property, if $x_1 \sim x_2$ then $g * x_1 = x_2$ for some $g \in G$. Then $x_1 = g^{-1} * x_2$, so $x_2 \sim x_1$. For the transitive property, if $x_1 \sim x_2$, $x_2 \sim x_3$, then say $x_2 = g_1 * x_1$, $x_3 = g_2 * x_2$. Therefore $x_3 = g_2 * g_1 * x_1 = (g_2 g_1) * x_1$, so $x_3 \sim x_1$. □

The orbits are the equivalence classes under this equivalence relation.

Definition 45. *An orbit of the $G-$set X is an equivalence class for this relation.*

We denote this by $G * x = \mathrm{Orb}(x) = \{g * x \mid g \in G\}$.

If the isotropy subgroup (the subgroup that fixes an element under a permutation) is large, then the orbits are correspondingly small.

Theorem 21.4. $|G * x| = (G : G_x)$.

Corollary 21.5. *If $|G| < \infty$, then $|G * x| = \frac{|G|}{|G_x|}$.*

Proof. Claim that $g_1 * x = g_2 * x$ if and only if $g_1 G_x = g_2 G_x$. Start from the left statement and left multiply by g_1^{-1}. We get $x = g_1^{-1}(g_2 * x) = (g_1^{-1} g_2) * x$. This is true if and only if $g_1^{-1} g_2 \in G_x$, which in turn implies $g_2 = g_1 h$ for some $h \in G_x$. Therefore $g_1 G_x = g_2 G_x$. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 22: Rings

Lecturer: Sylvie Corteel *18 March* *Aditya Sengupta*

Definition 46. *A ring $(R, +, \cdot)$ is a set R with two binary operations $+, \cdot$, such that $(R, +)$ is an abelian group, $\cdot$ is associative, and such that the ring is distributive, i.e. $a \cdot (b + c) = a \cdot b + a \cdot c \ \forall a, b, c \in R$, and $(a + b) \cdot c = (a \cdot c) + (b \cdot c) = a \cdot c + b \cdot c$.*

22.1 Direct Product of Rings

Let $R_1, \ldots, R_n$ be rings. Then $R_1 \times \cdots \times R_n$ is a ring. $\forall (a_1, \ldots, a_n), (b_1, \ldots, b_n) \in R_1 \times \cdots \times R_n$, addition and multiplication are defined component-wise:

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n) \tag{22.1}$$

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n) \tag{22.2}$$

We write 0 as the identity for $+$, and $-a$ for the additive inverse of a, $\forall a \in R$. For $n \in \mathbb{Z}$,

$$na = \begin{cases} a + \cdots + (\text{n times}) + \cdots + a & n > 0 \\ 0 & n = 0 \\ (-a) + \cdots + (\text{n times}) + \cdots + (-a) & n < 0 \end{cases} \tag{22.3}$$

22.2 Ring Properties

Theorem 22.1. *$\forall a, b \in R$ the following hold:*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$.

Note that we cannot use cancellation for products as inverses do not exist in general for $\cdot$. For example, $0 \cdot a = 0 \cdot b$ does not imply $a = b$.

Proof.

1. $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0$. Therefore we apply left cancellation on $(R, +)$ to get $a \cdot 0 = 0$. By the same arguments, $0 \cdot a = 0$.
2. $a \cdot (-b) + a \cdot b = a \cdot (b + (-b)) = a \cdot 0 = 0$. Therefore $a \cdot (-b)$ is the additive inverse of $a \cdot b$, i.e. $a \cdot (-b) = -(a \cdot b)$. We use the same logic to show $(-a) \cdot b = -(a \cdot b)$.
3. Apply the above statement: $(-a) \cdot (-b) = -((-a) \cdot b) = -(-(a \cdot b)) = a \cdot b$ as it is the inverse of an inverse.

□

22.3 Ring Homomorphisms

Let R and R' be rings. A ring homomorphism ϕ is a map $\phi : R \to R'$ such that $\forall a, b \in R$, the following properties hold:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Remark 22.2. *ϕ in particular is a group homomorphism. The usual results hold. For example, ϕ is injective if and only if* $\operatorname{Ker} \phi = \{0\}$.

For example, let F be the set of functions $f : \mathbb{R} \to \mathbb{R}$. Then $(F, +, \cdot)$ is a ring. For all $a \in \mathbb{R}$, $\phi_a : F \to \mathbb{R}, f \to f(a)$ is a homomorphism, called the *evaluation homomorphism*. A second example is $\phi : \mathbb{Z} \to \mathbb{Z}_n, a \to a \mod n$. This is a ring homomorphism between $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Z}_n, +, \cdot)$.

22.4 Ring Isomorphisms

Definition 47. *A ring isomorphism is a bijective ring homomorphism.*

If $\phi : R \to R'$ is an isomorphism, then the operations of R and R' are the same up to relabelling via the bijection ϕ. For example, if $\gcd(r, s) = 1$, then $\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s$. This gives the ring isomomorphism $\mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s, n \to (n \mod r, n \mod s)$.

To show that this is a homomorphism, we proceed as follows:

$$\begin{aligned} \phi(n + m) &= (n + m \mod r, n + m \mod s) \\ &= (n \mod r, n \mod s) + (m \mod r, m \mod s) \\ &= \phi(n) + \phi(m) \end{aligned} \tag{22.4}$$

and similarly for multiplication,

$$\phi(n \cdot m) = (n \cdot m \mod r, n \cdot m \mod s) = \phi(n) \cdot \phi(m) \tag{22.5}$$

Multiplication is always associative in rings, but it is not always commutative. If it is commutative, R is called a commutative ring. Multiplication does not always have an identity element. For example, $(2\mathbb{Z}, +, \cdot)$ is a ring where $\cdot$ does not have an identity element.

Definition 48. *If multiplication has an identity element, call it unity and say R is a ring with unity.*

Usually we denote unity by 1. It has the property that $1 \cdot a = a \cdot 1 = a$. If 1 exists, it is unique.

Math 113: Abstract Algebra **Spring 2019**

Lecture 23: Fields

Lecturer: Sylvie Corteel *20 March* *Aditya Sengupta*

Definition 49. *The zero ring is $R = \{0\}$ with $0 + 0 = 0$ and $0 \cdot 0 = 0$. Here, 0 is the additive and multiplicative identity, so 1 = 0.*

We claim that this is the only time when $1 = 0$. More concretely, if R is a ring with unity and R is not the zero ring, then $1 \neq 0$.

Definition 50. *A multiplicative inverse of an element a in a ring R with unity and $1 \neq 0$ is $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. If the multiplicative inverse exists, it is unique.*

Multiplicative inverses do not exist for every element in a ring, because $0 \in R$ for any ring R, and $\forall a \in R, 0 \cdot a = 0$. $(R, \cdot)$ is never a group.

Definition 51. *If R is a ring with unity and $1 \neq 0$, then $a \in R$ is a unit if it has a multiplicative inverse in R.*

Definition 52. *If every nonzero element of a ring with unity is a unit, then we say that R is a division ring.*

Definition 53. *A field is a commutative division ring.*

$(\mathbb{Z}, +, \cdot)$ is not a field, as the only units are ± 1. $(\mathbb{Q}, +, \cdot)$ is a field, because for any $\frac{p}{q} \in \mathbb{Q}^*$, $\frac{q}{p} \in \mathbb{Q}^*$ and $\frac{p}{q}\frac{q}{p} = 1$. $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are also fields. Also, $\mathbb{Z}_p$ is a field if p is prime.

Definition 54. *A subring S is a subset of a ring closed under $+$ and $\cdot$ and is a ring for those operations.*

We denote this by $S \leq R$. To prove that S is a subring of R, we show that $(S, +)$ is a subgroup of $(R, +)$ and we also show that S is closed under multiplication. Associativity and distributivity follow.

For example, $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$.

Definition 55. *A subfield is a subset of a field closed under the two operations of the field, and is a field for those operations.*

For example, $(\mathbb{Z}, +, \cdot)$ is not a subfield of $(\mathbb{R}, +, \cdot)$ as $\mathbb{Z}$ is not a field.

23.1 Divisors of zero

Our goal is to solve equations with one indeterminate $x \in \mathbb{R}$. In $\mathbb{Z}$, this can be something like $x^2 - 5x + 6 = 0$. This is equivalent to $(x - 2)(x - 3) = 0$, which in turn admits the solutions $x = 2$ or $x = 3$. We get this because in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, a product is equal to zero if one of the factors is equal to zero. This is not necessarily the case in other rings. For example, suppose we tried to solve the same equation in $\mathbb{Z}_{12}$. We get the solutions $x = 2, x = 3, x = 6, x = 11$.

Definition 56. *If $a, b \in R$ such that $a \neq 0, b \neq 0$ but $a \cdot b = 0$, we say that a and b are divisors of zero.*

For example, in $\mathbb{Z}_{12}$ the divisors of zero are $2, 3, 4, 6, 8, 9, 10$, by non-exhaustive pairs $(2, 6), (3, 4), (8, 9), (6, 10)$. In general, we can say the following:

Theorem 23.1. *In $\mathbb{Z}_n$ the divisors of zero are the integers that are not relatively prime to n.*

Proof. Let us suppose that n and r are relatively prime. We will prove that r is not a divisor of zero. We proceed by contradiction. Suppose that $s \neq 0$, $s \in \mathbb{Z}_n$ and $s \cdot r \equiv 0 \mod n$. This means that n divides $s \cdot r$. As n and r are relatively prime, this means n divides s. So $s = 0$ in $\mathbb{Z}_n$ which is a contradiction. Therefore r is not a divisor of zero.

Now, suppose that $\gcd(n, r) = d > 1$. Then $s = \frac{n}{d}$ with $1 \leq s < n$ so $s \neq 0$. Therefore $s \cdot r = \frac{n}{d} \cdot r = n \cdot \frac{r}{d} \equiv 0 \mod n$. Therefore $s \cdot r = 0$ in $\mathbb{Z}_n$ nd r is a divisor of zero. □

Corollary 23.2. *If p is prime then $\mathbb{Z}_p$ has no divisor of zero.*

Theorem 23.3. *Multiplicative cancellation holds in R (i.e. $a \cdot b = a \cdot c \implies b = c$) if and only if R has no divisor of zero.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 24: Integral domains, field properties, Fermat's Little Theorem

Lecturer: Sylvie Corteel *22 March* *Aditya Sengupta*

24.1 Cancellation

Let $a, b, c \in R$ with $a \neq 0$. If $a \cdot b = a \cdot c$ then in general $b = c$ is **not** true. For example, in $\mathbb{Z}_{12}, 6 \cdot 3 = 6 \cdot 1$, but $3 \neq 1$. This is a consequence of the previous theorem, that multiplicative cancellation holds if and only if R has no divisor of zero. We can prove this.

Proof. Case 1: If R has some divisors of zero, then there exist $a, b \in R$ such that $a \neq 0, b \neq 0$, and $a \cdot b = 0$. We prove that $\forall a \in R, a \cdot 0 = 0$. So we have $a \cdot 0 = a \cdot b$ and $b \neq 0$, so cancellation does not hold.

Case 2: If R does not have divisors of zero, and $a \cdot b = a \cdot c$ given $a \neq 0$ and $a, b, c \in R$. If a is a unit, the we multiply a^{-1} on both sides. We get $a^{-1}ab = a^{-1}ac$, so $b = c$. Otherwise, $a \cdot b + (-a \cdot c) = 0$. Then by distributivity, $a \cdot (b - c) = 0$, so $b - c = 0 \implies b = c$ as a is not a divisor of zero. □

As a consequence, if R is a ring with no divisors of zero, then the equation $ax = b$ for $a, b \in R$ and $a \neq 0$ has at most one solution in R. (Because cancellation holds, if $ax = b$ and $ax' = b$ then $x = x'$.)

24.2 Integral domains

Definition 57. *An integral domain is a commutative ring with unity $1 \neq 0$ and containing no divisors of zero.*

Remark 24.1. *1. Cancellation holds in an integral domain.*

2. A polynomial equation with an unknown in the integral domain can be factored and solved in the usual manner, i.e. one of the factors must be zero.

For example, $(\mathbb{Z}, +, \cdot)$ is an integral domain. $(\mathbb{Z}_n, +, \cdot)$ is an integral domain if n is prime, but not otherwise. If R and S are integral domains, then $R \times S$ is not an integral domain, because $(r, 0) \times (0, s) = (0, 0)$ so the product ring has divisors of zero. $M_2(\mathbb{Z})$ is not an integral domain, because $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and also it is non-commutative.

Theorem 24.2. *Every field is an integral domain.*

Proof. We need to check that there are no divisors of zero in a field. We suppose that $a \neq 0$ and $a \cdot b = 0$. We multiply by a^{-1} and see that $b = 0$. Therefore there are no divisors of zero. □

Not every integral domain is a field. $(\mathbb{Z}, +, \cdot)$ is an integral domain but not a field. However, if an integral domain is finite, it is a field.

Theorem 24.3. *Every finite integral domain is a field.*

Corollary 24.4. *If p is prime, $\mathbb{Z}_p$ is a field.*

Proof. Suppose R is a finite integral domain with n elements, a_1 through a_n. This includes 0 or 1. We need to show that every nonzero element is a unit. Let $a \in R, a \neq 0$. Then $a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_n$ are all distinct. As cancellation holds, if $a \cdot a_i = a \cdot a_j$ then $a_i = a_j$. So there exists some i such that $a \cdot a_i = 1$. Hence $a^{-1} = a_i$ and R is a field. □

Remark 24.5. *For any $\phi : R \to R$, ϕ being injective implies that ϕ is bijective. (Not sure why this is the case.)*

Proposition 24.6. *The zero elements of a field F form an abelian group F^* under multiplication.*

Proof.
1. F^* is closed under multiplication, as there are no divisors of zero.
2. $\cdot$ is associative by definition of a ring.
3. $1 \in F^*$ is the identity element.
4. $\forall a \in F^*, \exists a^{-1} \in F^*$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

The group is abelian because a field is necessarily a commutative ring. □

For example, $(\mathbb{Z}_p^*, \cdot)$ is a group of order $p - 1$ if p is prime.

Theorem 24.7. *Fermat's Little Theorem: $a^{p-1} \equiv 1 \mod p$.*

Proof. As $\mathbb{Z}_p^*$ is a group of order $p-1$, for any $a \in \mathbb{Z}_p^*$, $a^{p-1} = 1$ in $\mathbb{Z}_p^*$, because the order of any element of a finite group divides the order of a group. If $a = i + kp$, for $1 \leq i \leq p-1$ and $k \in \mathbb{Z}^*$, then i does not divide p and $i \in \mathbb{Z}_p^*$. Therefore $a^{p-1} \equiv i^{p-1} \equiv 1 \mod p$. □

This is a powerful number theory result. For example, $5^{273403} \mod 101 \equiv 5^{273400} \cdot 5^3 \mod 101 \equiv 5^3 \mod 101 \equiv 24 \mod 101$. It can be used to prove more general results too. For example, $\forall a \in \mathbb{Z}, a^{25} - a$ is divisible by 91. We can get this by proving using Fermat's little theorem that $a^{25} - a$ is divisible by 13 and by 7.

Math 113: Abstract Algebra **Spring 2019**

Lecture 25: Linear equations, Euler's generalization of FLT

Lecturer: Sylvie Corteel *1 April* *Aditya Sengupta*

Proposition 25.1. *In $\mathbb{Z}_n$, the following are equivalent: $a \neq 0$ is not a divisor of 0, a is a unit, and* $\gcd(a, n) = 1$.

Proof. (3 $\implies$ 2) if $\gcd(a, n) = 1$, then $\exists u, v \in \mathbb{Z}$ such that $au + nv = 1$. Therefore $au \equiv 1 \mod n$ and $a^{-1} = u \mod n$, so a is a unit.

(1 $\implies$ 3) if $\gcd(a, n) > 1$ then $b = \frac{n}{\gcd(n,a)}$. $a \cdot b = 0$ in $\mathbb{Z}_n$ and a is a divisor of zero, and a is not a unit. The contrapositive of this also shows that 2 $\implies$ 3. □

Theorem 25.2. *The units of a ring with unity form a group under multiplication.*

Proof. We check the group axioms.

1. Closure: if $a, b \in R$ are units, then $a \cdot b \cdot b^{-1} \cdot a^{-1} = 1$. So $a \cdot b$ is a unit and $(ab)^{-1} = b^{-1} \cdot a^{-1}$
2. Associativity: this is true by definition of a ring.
3. 1 is a unit, so an identity element exists.
4. If $a \in R$ is a unit then so is a^{-1} because $\left(a^{-1}\right)^{-1} = a$.

□

Corollary 25.3. *$\mathbb{Z}_p^*$ is a group of order $p - 1$ if p is prime.*

Fermat's Little Theorem was stated in the previous lecture. Euler's generalization of Fermat's Little Theorem is as follows:

Corollary 25.4. *$\mathbb{Z}_n^*$ is a group of order $\varphi(n)$ where $\varphi(n) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.*

For example, $\mathbb{Z}_{12}^*$ has order 4, consisting of the elements $\{1, 5, 7, 11\}$.

Theorem 25.5. *For any positive integer n and for any integer a that is coprime with n,*

$$a^{\varphi(n)} \equiv 1 \mod n$$

Proof. Let $b \in \mathbb{Z}_n^*$ such that $a \equiv b \bmod n$. Because $\gcd(a, n) = 1$, we know that $a \bmod n \in \mathbb{Z}_n^*$. As $b \in \mathbb{Z}_n^*$, $b^{\varphi(n)} = 1$ in $\mathbb{Z}_n^*$. As $a \equiv b \bmod n$, we get $a^{\varphi(n)} \equiv b^{\varphi(n)} \bmod n$. So $a^{\varphi(n)} \equiv 1 \bmod n$. □

To solve equations of the form $ax \equiv b \bmod n$ in $\mathbb{Z}_n$, we can employ Fermat's little theorem.

Theorem 25.6. *If $\gcd(a, n) = 1$ then the equation $ax \equiv b \bmod n$ has a unique solution.*

Proof. If $\gcd(a, n) = 1$ then a is a unit. $ax \equiv b \bmod n$ implies $a^{-1}ax \equiv a^{-1}b \bmod n$, so $x \equiv a^{-1}b \mod n$. Since we are looking for solutions in $\mathbb{Z}_n$ this is valid. □

Theorem 25.7. *If* $\gcd(a, n) = d > 1$ *then the equation* $ax \equiv b \bmod n$ *has solutions iff* d *divides* b*. In this case it has* d *solutions in* $\mathbb{Z}_n$*.*

Proof. If $\gcd(a, n) = d$ then $\exists u, v \in \mathbb{Z}$ such that $ua + vn = d$. If $ax \equiv b \bmod n$, then $\exists y \in \mathbb{Z}$ such that $ax + ny = b$, which implies $ax + ny \in d\mathbb{Z}$. So if d does not divide b, then the equation has no solution.

If d divides b then define $a' = \frac{a}{d}, b' = \frac{b}{d}$, and $n' = \frac{n}{d}$. Then the equation becomes

$$a'x' \equiv b' \bmod n$$

with $\gcd(a', n') = 1$. So there is a unique solution $x' = (a')^{-1} \cdot b$ in $\mathbb{Z}_{n'}$. The d solutions in $\mathbb{Z}_n$ are $x', x' + n', \ldots, x' + (d-1)n'$. □

Example 25.8. *Consider the equation* $12x \equiv 27 \bmod 18$. $\gcd(12, 18) = 6$ *and* 6 *does not divide* 27 *so there are no solutions.*

Example 25.9. *Consider the equation* $15x \equiv 27 \bmod 18$. $\gcd(15, 18) = 3$ *and* 3 *divides* 27*, so the equation can be reduced to* $5x' = 9 \bmod 6$*. In* $\mathbb{Z}_6$ *the unique solution is 3, so in* $\mathbb{Z}_{18}$ *the solutions are* $3, 9, 15$*.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 26: Field of quotients

Lecturer: Sylvie Corteel *3 April* *Aditya Sengupta*

Consider an integral domain D, and the set $S = \{(a, b) \in D \times D\} \mid b \neq 0$. We can define an equivalence relation $(a, b) \sim cd$ iff $a \cdot d = b \cdot c$.

Lemma 26.1. *$\sim$ is an equivalence relation.*

Proof. We show it is reflexive, symmetric, and transitive.

1. Reflexive: $(a, b) \sim (a, b)$ as $a \cdot b = a \cdot b \; \forall (a, b) \in S$
2. Symmetric: $\forall (a, b), (c, d) \in S$, if $(a, b) \sim (c, d)$ then $a \cdot d = b \cdot c$. Then $c \cdot b = d \cdot a$ because the ring is commutative, so $(c, d) \sim (a, b)$.
3. Transitive: $\forall (a, b), (c, d), (e, f) \in S$, if $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ then $a \cdot d = b \cdot c$ and $c \cdot f = d \cdot e$. Multiplying the first equation on both sides by f and the second on both sides by b, we get $f \cdot a \cdot d = b \cdot c \cdot f = d \cdot e \cdot b$. So $d \cdot a \cdot f = d \cdot e \cdot b$, so $a \cdot f = e \cdot b$ and $(a, b) \sim (e, f)$.

□

Let F be the set of equivalence classes $[(a, b)]$, where $[(a, b)] = [(c, d)]$ if and only if $a \cdot d = b \cdot c$. For example, $[(0, b)] = [(0, 1)]$. We claim that this set is a field. Recall that a field is a commutative ring R with unity, such that every nonzero element is a unit, $(R, +)$ is an abelian group, $(R^*, \cdot)$ is an abelian group, and the distributive laws hold. So claiming that F is a field requires that we define addition and multiplication, which are defined as follows:

$$[(a, b)] + [(c, d)] = [(a \cdot d + b \cdot c, b \cdot d)] \tag{26.1}$$

$$[(a, b)] \cdot [(c, d)] = [(a \cdot c, b \cdot d)] \tag{26.2}$$

To show that F is a field, we consider each of the requirements separately.

Lemma 26.2. *Addition is well defined.*

Proof. We want to show that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then

$$[(a, b)] + [(c, d)] \sim [(a', b')] + [(c', d')] \tag{26.3}$$

From the congruences, we know that $ab' = ba'$ and $cd' = dc'$. Multiply the first by dd' and the second by bb' on both sides, to get $ab'dd' = ba'dd'$ and $cd'bb' = dc'bb'$. Adding these two, we get $adb'd' + cbd'b' = a'd'bd + b'c'bd$, or $(ad + bc)b'd' = (a'd' + b'c')bd$, as was to be shown. □

Lemma 26.3. *Multiplication is well defined.*

Proof. If $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$ then $(a \cdot c, b \cdot d) \sim (a'c', b'd')$. We know that $ab' = ba'$ and $cd' = c'd$. So $acb'd' = bda'c'$ and $(ac, bd) \sim (a'c', b'd')$. □

Lemma 26.4. *$(F, +)$ is an abelian group.*

Proof. We need to show that addition is commutative and that $(F, +)$ satisfies all the group axioms.

1. We show that addition is commutative, by $[(a,b)] + [(c,d)] = [(a \cdot d + b \cdot c, bd)]$ and $[(c,d)] + [(a,b)] = [(cb + da, db)] = [(ad + bc, bd)]$.
2. We also show that it is associative, $([(a,b)] + [(c,d)]) + [(e,f)] = [(adf + bcf + bde, bdf)] = [(a,b)] + ([(c,d)] + [(e,f)])$.
3. We show that the identity exists and it is $[(0,1)]$, as $[(a,b)] + [(0,1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a,b)]$.
4. We show that an additive inverse exists for any element, $[(-a,b)]$. $[(a,b)] + [(-a,b)] = [(a \cdot b + (-a) \cdot b, b^2)] = [(0, b^2)] = [0,1]$.

□

Lemma 26.5. *$(F^*, \cdot)$ is an abelian group.*

Proof. We need to show that multiplication is commutative and that $(F^*, \cdot)$ satisfies all the group axioms.

1. We show that multiplication is commutative, by $[(a,b)] \cdot [(c,d)] = [(ac, bd)] = [(ca, db)] = [(c,d)] \cdot [(a,b)]$.
2. We show that multiplication is associative, by $([(a,b)] \cdot [(c,d)]) \cdot [(e,f)] = [(ace, bdf)] = [(a,b)] \cdot ([(c,d)] \cdot [(e,f)])$.
3. We show that the identity exists and it is $[(1,1)]$, as $[(a,b)] \cdot [(1,1)] = [(a \cdot 1, b \cdot 1)] = [(a,b)]$.
4. We show that a multiplicative inverse exists for any element, $[(b,a)]$. $[(a,b)] \cdot [(b,a)] = [(a \cdot b, a \cdot b)] = [(1,1)]$.

□

Lemma 26.6. *$(F, +, \cdot)$ obeys the distributive law.*

Proof.

$$\begin{aligned} ([(a,b)] + [(c,d)]) \cdot [(e,f)] &= [((ad + bc) \cdot e, b \cdot d \cdot f)] \\ &= [(a,b)] \cdot [(e,f)] + [(c,d)] \cdot [(e,f)] \\ &= [(ae, bf)] + [(ce, df)] \\ &= [(aedf + bfce, bfdf)] = [(aed + bec, bdf)] \\ &= [(ad + bc)e, bdf] \end{aligned} \tag{26.4}$$

□

We say F is an enlargement of D, and D is isomorphic to a subdomain of F. For example, $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$.

Math 113: Abstract Algebra **Spring 2019**

Lecture 27: Polynomials

Lecturer: Sylvie Corteel *10 April* *Aditya Sengupta*

Let R be a ring. Then $R[x]$ is the ring of polynomials with one indeterminate x, with polynomial coefficients in R. For example, $\mathbb{Z}_2[x]$, and we can write something like $x^2 + x \in \mathbb{Z}_2[x]$. (We write $1 \cdot x = x$.)

Definition 58. *A polynomial $f(x)$ with coefficients in R is a formal sum*

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

with $a_i \in R$ for all i and only finitely many a_is are nonzero.

Remark 27.1. *A polynomial is not a function of x.*

Definition 59. *If at least one of the a_is is not zero, the degree of $f(x)$ is the largest i such that $a_i \neq 0$. We denote this by* $\deg(f(x))$.

If $\deg(f(x)) = n$, we can write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Usually we do not write the coefficients equal to 0. For example, for $\mathbb{Z}[x]$, we write $0 + 2x + 1x^2$ as $2x + x^2$.

We want to show that $R[x]$ is a ring. For this, we need to define the two binary operations on polynomials, addition and multiplication. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$, and let $g(x) = \sum_{i=0}^{\infty} b_i x^i$. Then, addition is

$$f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and multiplication is

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k \cdot b_{i-k} \right) x^i \tag{27.1}$$

For example, in $\mathbb{Z}_2[x]$, $(x+1) \cdot (x+1) = x^2 + (1+1) \cdot x + 1 = x^2 + 1$.

Theorem 27.2. *$(R[x], +, \cdot)$ is a ring. If R is a commutative ring, then $R[x]$ is a commutative ring. If R has unity 1 then $R[x]$ has unity 1.*

Proof. We can show that $(R[x], +)$ is an abelian group, that multiplication is associative, and that the distributivity laws hold. To check that R being commutative implies $R[x]$ is commutative, we write down a generic polynomial product,

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x^i$$

Then, because R is commutative, we switch the order of the coefficients,

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} b_{i-k} \cdot a_k \right) x^i = g(x) \cdot f(x) \tag{27.2}$$

Finally, if R has unity 1, then $1 \in R[x]$ is the unity element. We see that $1 \cdot f(x) = f(x)$. □

Proposition 27.3. *If R is an integral domain, then so is $R[x]$.*

Proof. We know that $R[x]$ is a ring, so we just need to check that it has no divisors of zero. Suppose $f(x), g(x) \in R[x]$ are both nonzero. Suppose that they are of degree n and m respectively. Then, the highest-order term will have degree $m+n$. The coefficient on x^{m+n} is guaranteed to be nonzero because R is an integral domain meaning it has no divisors of zero, and $a_n, b_m \neq 0$. Therefore $f(x) \cdot g(x)$ is not zero, so $R[x]$ is an integral domain. □

Corollary 27.4. *If F is a field then $F[x]$ is an integral domain (as any field is any integral domain).*

Remark 27.5. *$F[x]$ is not a field as x has no multiplicative inverse.*

We can build the field of quotients of $F[x]$, the field of rational functions in one indeterminate.

We can define the *evaluation homomorphism* on polynomials.

Definition 60. *Let R be a commutative ring and let $\alpha \in R$. Then the evaluation homomorphism $\phi_\alpha : R[x] \to R$ defined by $\phi_\alpha(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$.*

Theorem 27.6. *ϕ_α is a ring homomorphism.*

Proof. Let $f(x), g(x) \in R[x]$. Then

$$\phi_\alpha(f(x) + g(x)) + \phi_\alpha(\sum_{i=0}^{\infty}(a_i + b_i)x^i) = \sum_{i=0}^{\infty}(a_i + b_i)\alpha^i$$
$$\phi_\alpha(f(x) + g(x)) = \sum_{i=0}^{\infty} a_i\alpha^i + \sum_{i=0}^{\infty} b_i\alpha^i = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$$

We also need to show the homomorphism property holds for multiplication,

$$\phi_\alpha(f(x) \cdot g(x)) = \phi_\alpha \left(\sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x_i \right) = \sum_{i=0}^{\infty} (\sum_{k=0}^{i} a_k b_{i-k})\alpha^i$$

Because R is commutative, we can split $\alpha^i = \alpha^k \cdot \alpha^{i-k}$, and write this as

$$\phi_\alpha(f(x) \cdot g(x)) = \left(\sum_{i=0}^{\infty} a_i\alpha^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i\alpha^i \right) = \phi_\alpha(f(x)) \cdot \phi_\alpha(g(x)) \tag{27.3}$$

□

Definition 61.

$$f(\alpha) = \phi_\alpha(f(x))$$

Remark 27.7. *ϕ_α maks R to itself, as $\forall \alpha in R, \phi_\alpha(a_0) = a_0$.*

Example 27.8.

$$\phi_0(f(x)) = a_0$$

Example 27.9.

$$\begin{aligned} f(x) &= x^2 + x \\ \phi_0(f(x)) &= 0 \\ \phi_1(f(x)) &= 1^2 + 1 = 0 \end{aligned}$$

Evaluation of f at all elements of $\mathbb{Z}_2$ is zero, but $f(x) \neq 0$.

Math 113: Abstract Algebra **Spring 2019**

Lecture 28: Rings of polynomials, division algorithm

Lecturer: Sylvie Corteel *12 April* *Aditya Sengupta*

Let F be a field, and let $F[x]$ be a set of polynomials in x whose coefficients are in F. $F[x]$ is an integral domain, and $f(x) \in F[x]$ for any $f(x) = \sum_{i=0}^{\infty} a_i x^i, a_i \in F$ if only finitely many a_is are nonzero.

We are interested in finding the zeroes of polynomials in $F[x]$, i.e. finding all α such that the evaluation homomorphism $\phi_\alpha(f(x)) = 0$. To do this, we factorize them. Since F is an integral domain, if we can write $f(x) = h(x)g(x)$ then $\phi_\alpha(f(x)) = \phi_\alpha(h(x)) \cdot \phi_\alpha(g(x)) = h(\alpha)g(\alpha)$. So if $f(\alpha) = 0$ then $h(\alpha) = 0$ or $g(\alpha) = 0$.

In order to find this factorization, we use the division algorithm. Let $f(x) = \sum_i a_i x^i$ have order n and let $g(x) = \sum_i b_i x^i$ have order m. Both $f(x)$ and $g(x)$ are elements of $F[x]$.

Theorem 28.1. *There exist unique polynomials $q(x), r(x) \in F[x]$ such that*

1. $f(x) = q(x) \cdot g(x) + r(x)$
2. $r(x) = 0$ *or* $\deg(r(x)) < \deg(g(x))$

Proof. We first prove existence, then present an algorithm to find these polynomials.

If $\deg(f(x)) < \deg(g(x))$ then $f(x) = 0 \cdot g(x) + f(x)$, so $q(x) = 0$ and $r(x) = f(x)$. Fix $g(x)$ and we use induction on the degree of $f(x)$. Our base case is $\deg(f(x)) < m$ as was just shown. The inductive step is to assume this is true if $\deg(f(x)) < n$, and consider $\deg(f(x)) = n$, that is, $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ and $n \geq m$. Let $\widetilde{f}(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$. Then $\widetilde{f}(x)$ has degree less than n. By induction $\widetilde{f}(x) = \tilde{q}(x) \cdot g(x) + \tilde{r}(x)$ where $\deg(\tilde{r}(x)) < m$. Then $f(x) = \left(\tilde{q}(x) + \frac{a_n}{b_m} x^{n-m}\right) g(x) + \tilde{r}(x)$, which is the required decomposition. □

For example, let $f(x) = x^3 + 2x^2 + 3x - 1$ and let $g(x) = x - 1$ in $\mathbb{Z}_5$.

$$
\begin{array}{r|l}
 & X^2 + 3X + 6 \\
\hline
X - 1 & X^3 + 2X^2 + 3X - 1 \\
 & \underline{-X^3 + X^2} \\
 & \quad 3X^2 + 3X \\
 & \quad \underline{-3X^2 + 3X} \\
 & \quad\quad 6X - 1 \\
 & \quad\quad \underline{-6X + 6} \\
 & \quad\quad\quad 5
\end{array}
$$

Because this is a $\mathbb{Z}$-based in-built LaTeXthing we get a remainder of $5x$, which in $\mathbb{Z}_5$ is just zero. (I'll figure out how to display long division not in $\mathbb{Z}$ or $\mathbb{R}$ later.) Therefore $f(x) = (x^2 + 3x + 1)(x - 1)$.

Next, we prove uniqueness of the polynomials $q(x)$ and $r(x)$.

Proof. We proceed by contradiction, supposing that two possible distinct pairs of polynomials exist and showing eventually that this cannot be the case. Suppose that $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$,

with $\deg(r_1(x)) < m$ and $\deg(r_2(x)) < m$. Then $(q_1(x) - q_2(x))\, g(x) = r_2(x) - r_1(x)$. If $q_1(x) - q_2(x) \neq 0$, then the left hand side has degree $\geq m$ and the right hand side has degree $< m$, which is a contradiction. Therefore $q_1(x) - q_2(x) = 0$ and $r_2(x) - r_1(x) = 0$, and uniqueness holds. □

Corollary 28.2. *$a \in F$ is a zero of $f(x) \in F[x]$ if and only if $(x - a)$ divides $f(x)$ in $F[x]$.*

Proof. Consider the evaluation homomorphism ϕ_a.

$$\phi_a(f(x)) = \phi_a(x - a)\phi_a(g(x)) + \phi_a(r(x)) = \phi_a(r(x)) \tag{28.1}$$

Because the degree of $x - a$ is 1, the degree of $r(x)$ must be less than 1 because $\deg(r(x)) < \deg(g(x))$. Therefore it must be a constant, i.e. $\phi_a(f(x)) = r$. So $\phi_a(f(x)) = 0$ iff $r = 0$. □

Corollary 28.3. *A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n distinct zeroes in a field F.*

Proof. If $a_1 \in F$ is a zero of $f(x)$, then $f(x) = (x - a_1)q_1(x)$. If $a_2 \neq a_1 \in F$ is a zero of $f(x)$, then $f(a_2) = (a_2 - a_1)q_1(a_2)$. The first term is not zero as the zeroes are distinct, so a_2 is a zero of $q_1(x)$. Therefore we write $q_1(x) = (x - a_2)q_2(x)$. Therefore there are at least r distinct zeroes $f(x) = (x - a_1)(x - a_2)\dots(x - a_r)q_r(x)$ with $q_r(x) \neq 0$. There cannot be $n + 1$ zeroes as $\deg(f(x)) = n$. □

Corollary 28.4. *If F is a field and G is a finite subgroup of $(F^*, \cdot)$ then G is cyclic.*

Proof. As $G \leq F^*$, G is abelian. So G is a finite abelian group. If G is of order m, then it can be decomposed by the structure theorem of finitely generated abelian groups, $G \simeq \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$ where $m = d_1 d_2 \dots d_n$, and the d_is all have prime power order. $r = \operatorname{lcm}(d_1, \dots, d_n) \leq m$, so $\forall g \in G$, $g^r = 1$, so $x^r - m$ has at least m zeroes in $F[x]$. Therefore $r \geq m$. This tells us $r = m$, therefore the group G is cyclic and has order m. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 29: Rings of polynomials, irreducible polynomials

Lecturer: Sylvie Corteel *15 April* *Aditya Sengupta*

Corollary 29.1. *(to the division algorithm) $a \in F$ is a zero of $f(x) \in F[x]$ if $x - a$ divides $f(x)$.*

Definition 62. *A nonconstant polynomial $f(x) \in F[x]$ is irreducible if it cannot be expressed as $g(x)h(x)$ of polynomials in $F[x]$ of strictly lower degree.*

For example, $x^2 - 3 = (x + \sqrt{3})(x - \sqrt{3})$ is irreducible over $\mathbb{Q}$ but not over $\mathbb{R}$.

Lemma 29.2. *If $f(x)$ has degree 2 or 3, then $f(x)$ is reducible if and only if it has a zero in F.*

Proof. If $f(x)$ has a zero α in F, then $f(x) = (x - \alpha)g(x)$ where $g(x)$ has degree 1 or 2, so it is reducible. If $f(x)$ is reducible then $f(x) = g(x)h(x)$ of which at least one has degree 1. Suppose $g(x) = ax + b$ with $a \neq 0$. Then $-\frac{b}{a}$ is a zero of $f(x)$. □

29.1 Irreducibility over $\mathbb{Q}$

If a polynomial in $\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$, then it factors in $\mathbb{Z}[x]$.

Theorem 29.3. *If $f(x) \in \mathbb{Z}[x]$ factors as $g(x) \cdot h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$, then $\exists c \in \mathbb{Q}^*$ such that $g_1(x) = c \cdot g(x) \in \mathbb{Z}[x]$ and $h_1(x) = \frac{1}{c}h(x) \in \mathbb{Z}[x]$.*

For example, $f(x) = x^3 - 5x^2 + 8x - 4 = \left(\frac{4}{3}x^2 - 4x + \frac{8}{3}\right)\left(\frac{3}{4}x - \frac{3}{2}\right) = (x^2 - 3x + 2)(x - 2)$.

Corollary 29.4.

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \tag{29.1}$$

If f has a zero $m \in \mathbb{Q}$, then $m \in \mathbb{Z}$ and m divides $a_0 \neq 0$.

Proof. If m is a zero of f, then $f(x) = (x - m)g(x)$ and $g(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$. We suppose that $m \in \mathbb{Q}$. By the theorem, $\exists c \in \mathbb{Q}^*$ such that $c(x - m) \in \mathbb{Z}[x]$. Then $\frac{1}{c}g(x) \in \mathbb{Z}[x]$. If $c = 1$ then $m \in \mathbb{Z}$. The coefficient of x^0 in $f(x)$ is a_0 and in $(x - m)g(x)$ is $m \cdot b_0$. Therefore m divides a_0. □

Theorem 29.5. *Eisenstein criterion: let $p \in \mathbb{Z}$ be a prime. Then $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. If $a_n \not\equiv 0 (\text{mod } p)$ and $a_i \equiv 0 (\text{mod } p), 0 \leq i < n$ with $a_0 \not\equiv 0 (\text{mod } p^2)$, then $f(x)$ is irreducible.*

For example, by the Eisenstein criterion, $29x^4 - 9x^2 + 36x + 12$ is irreducible over $\mathbb{Q}$ with $p = 3$.

Proof. Assume $f(x) = \left(\sum_{i=0}^{r} b_i x^i\right)\left(\sum_{j=0}^{s} c_i x^i\right)$, where $r+s = n$. Then $a_n = b_r \cdot c_s$ where $b_r, c_s \not\equiv 0 (\text{ mod } p)$. Then $a_0 = b_0 \cdot c_0$; p divides b_0 or c_0 but not both. Suppose it divides b_0. Then $a_1 = b_0c_1 + c_0b_1$, which is a multiple of p plus something that is not. Therefore for $a_1 \equiv 0 (\text{ mod } p)$, we get $b_1 \equiv (0 \text{ mod } p)$. By the same argument on each a_i, we get that each b_i is $0 (\text{mod } p)$. Therefore $b_r \equiv 0 (\text{mod } p)$. We have a contradiction because of our starting assumption, so $f(x)$ is irreducible. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 30:

Lecturer: Sylvie Corteel *17 April* *Aditya Sengupta*

Corollary 30.1. *(of Eisenstein Criterion): if p is prime, $\frac{x^p-1}{x-1} = 1 + x + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}$.*

To prove this, we invoke the following lemma:

Lemma 30.2. *$f(x)$ is irreducible over $\mathbb{Q}$ if and only if $f(x+1)$ is irreducible.*

Proof. We prove the contrapositive, which due to being an if-and-only-if condition proves the lemma. We define a map $\varphi : F[x] \to F[x], f(x) \to f(x+1)$ where φ is a ring homomorphism. So if f is not irreducible then $f(x) = h(x)g(x)$ and $\varphi(f(x)) = \varphi(h(x))\varphi(g(x))$, i.e. $f(x+1)$ is not irreducible. □

Proof. (of the corollary): let $f(x) = \frac{x^p-1}{x-1}$. Then $f(x+1) = \frac{(1+x)^p-1}{x}$ and by the binomial theorem we get

$$f(x+1) = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} \tag{30.1}$$

The coefficient of the leading term is 1, and p does not divide 1, and all the other coefficients are multiples of p, since they are $\frac{p!}{k!(p-k)!} = p\left(\frac{(p-1)!}{k!(p-k)!}\right)$. The constant term is p, which is clearly divisible by p but not p^2. So the Eisenstein criterion applies and $f(x)$ is irreducible. □

Theorem 30.3. *If $p(x) \in F[x]$ is irreducible and divides $r_1(x) \cdot r_2(x)$, then $p(x)$ divides $r_i(x)$ for at least one i.*

Theorem 30.4. *If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored into a product of irreducible polynomials in $F[x]$. The factors are unique up to reordering and multiplication by units.*

Proof. We first show existence: if $f(x) = h(x)g(x)$ with $deg(g(x)), deg(h(x)) < deg(f(x))$, then if $h(x)g(x)$ are irreducible the theorem is shown, and if not, we repeat this process. We then have to answer whether the process will terminate, which it will, because the degree of polynomials is finite and decreases at each step.

Second, we show uniqueness. Suppose $f(x) = \prod_{i=1}^{r} p_i(x) = \prod_{i=1}^{s} q_i(x)$, and without loss of generality take $r \leq s$. Then by the above theorem that if $p(x)$ divides $r_1(x) \cdot r_2(x)$ it divides at least one of them, we know that $p_1(x)$ divides $q_j(x)$ for some $1 \leq j \leq s$. Since each $q_j(x)$ is irreducible, we must have $p_1(x) = q_j(x)$. Dividing $p_1(x) \dots p_r(x)$ and $q_1(x) \dots q_s(x)$ by $p_1(x) = q_j(x)$ and repeating this process, we rearrange factors and find that $p_i(x) = a_i q_i(x)$, where $a_i \in F[x]$ is a unit. Therefore we have $s = r$ and $\prod_i a_i = 1$. So uniqueness holds. □

Definition 63. *Let R, R' be rings. A ring homomorphism is a map $\varphi : R \to R'$ such that φ is well defined and $\forall x, y \in R$, $\varphi(x+y) = \varphi(x) +' \varphi(y)$, and $\varphi(xy) = \varphi(x) \cdot' \varphi(y)$.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 31: Ring Homomorphisms

Lecturer: Sylvie Corteel *19 April* *Aditya Sengupta*

31.1 Properties of Ring Homomorphisms

Theorem 31.1. *If $\phi : R \to R'$ is a ring homomorphism, then*

1. $\phi(0) = 0'$
2. $\phi(-x) = -\phi(x)$
3. *If $S' \leq R'$ then $\phi^{-1}[S'] \leq R$.*
4. *If $S \leq R$ then $\phi[S] \leq R'$.*
5. *If R has unity 1 then $\phi[1]$ is unity for $\phi[R]$.*

Remark 31.2. *$\phi(1)$ might not be unity for R'. For example, consider $\phi : \mathbb{Z}_2 \to \mathbb{Z}_8, 0 \to 0, 1 \to 4$. Then $\phi[\mathbb{Z}_2] = \{0, 4\} \leq \mathbb{Z}_8$. Then 4 is unity for $\{0, 4\}$ but not for $\mathbb{Z}_8$*

Proof. As ϕ is a group homomorphism from $(R, +)$ to $(R', +)$, the first two follow from group theory.
To show the third statement, we know that $\left(\phi^{-1}[S'], +\right)$ is a subgroup of $(R, +)$. We just need to check that the inverse image of S' is closed under multiplication. For any $a, b \in \phi^{-1}[S']$, $\phi(a), \phi(b) \in S'$ and $\phi(ab) = \phi(a) \cdot \phi(b)$, as S' is a subring of R'. Therefore $\phi(ab) \in S'$, which implies $ab \in \phi^{-1}[S']$.
To show the fourth statement, we need to check that $\phi[S]$ is closed under multiplication. Take $s_1', s_2' \in \phi[S]$; then there exist $s_1, s_2 \in S$ such that $\phi(s_1) = s_1'$ and $\phi(s_2) = s_2'$. Then $\phi(s_1) \cdot \phi(s_2) = \phi(s_1 s_2) \in \phi[S]$. As $S \leq R$, $s_1 s_2 \in S$.
To show the fifth statement, we state that for any $r' \in \phi[R]$, there exists $r \in R$ such that $\phi(r) = r'$. Then $\phi(r)\phi(1) = \phi(r) = r'$, and $\phi(1)\phi(r) = \phi(r) = r'$, so $\phi(1)$ is unity in $\phi[R]$. □

Definition 64. *Let $\phi : R \to R'$ be a ring homomorphism. The kernel of ϕ is* $\operatorname{Ker}\phi = \phi^{-1}[0'] = \{r \in R \mid \phi(r) = 0'\}$.

From this, we can show some facts:

1. The kernel $\operatorname{Ker}(\phi)$ is a subring of R. This can be shown directly with the theorem that $S' = 0'$ is a subring of R'.
2. Additive cosets: $\forall a \in R$, $\phi^{-1}(\phi(a)) = \{x \in R \mid \phi(x) = \phi(a)\} = a + \operatorname{Ker}(\phi)$.
3. ϕ is injective if and only if $\operatorname{Ker}(\phi) = \{0\}$.
4. Let $H = \operatorname{Ker}(\phi)$. Then $\forall a \in R, h \in H$, $ah \in H$ and $ha \in H$, as $\phi(ah) = \phi(a)\phi(h) = 0'$ so $ah \in H$ and the same the other way.

31.2 Quotient Rings

Theorem 31.3. *Let $\phi : R \to R'$ be a ring homomorphism with $\mathrm{Ker}(\phi) = H$ Then the additive cosets of H form a ring R/H for coset addition, $(a + H) + (b + H) = (a + b) + H$ and coset multiplication, $(a + H)(b + H) = a \cdot b + H$. Additionally, there exists a ring isomorphism $\mu : R/H \to \phi[R]$, $a + H \to \phi(a)$.*

Proof. From group theory, we know that $(R/H, +)$ is an abelian group, so it remains to be shown that multiplication is well defined. For any $a' \in a + H, b' \in b + H$ we need to show that $a'b' \in ab + H$. If $a' \in a + H$ then there exists $h_1 \in H$ so that $a' = a + h_1$. If $b' \in b + H$ then there exists $h_2 \in H$ so that $b' = b + h_2$. Then we multiply them: $a'b' = (a + h_1)(b + h_2) = ab + h_1b + ah_2 + h_1h_2$. By definition of the kernel the last three terms are in H, therefore $a'b' \in ab + H$. We also need to show that multiplication is associative:

$$((a + H)(b + H))(c + H) = (ab) \cdot c + H = a(bc + H) = (a + H)((b + H)(c + H)) \tag{31.1}$$

Then, we check the distributive laws. For all $a, b, c \in R$,

$$\begin{aligned}(a + H)((b + H) + (c + H)) &= a \cdot (b + c) + H \\ &= (a \cdot b + a \cdot c) + H \\ &= (a + H)(b + H) + (a + H)(c + H)\end{aligned} \tag{31.2}$$

The same argument follows for the right distributive law. Therefore R/H is a ring.

To show that μ is a ring isomorphism, we just need to show that it is a homomorphism under multiplication, because we know it is a group isomorphism. This can be shown by $\mu((a+H)(b+H)) = \mu(ab+H) = \phi(ab) = \phi(a)\phi(b) = \mu(a + H)\mu(b + H)$. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 32: Ideals, fundamental homomorphism theorem

Lecturer: Sylvie Corteel *22 April* *Aditya Sengupta*

Consider a ring homomorphism $\phi : R \to R'$ and let $H = \operatorname{Ker}\phi$. Then let $R/H = \{a + H \mid a \in R\}$.

Theorem 32.1. *R/H is a ring with coset addition $(a+H)+(b+H) = (a+b)+H$ and coset multiplication $(a + H) \cdot (b + H) = a \cdot b + H$.*

Example 32.2. *Consider $\phi : \mathbb{Z} \to \mathbb{Z}_n, a \to a \bmod n$. Then ϕ is a ring homomorphism where $\operatorname{Ker}\phi = n\mathbb{Z}$. The additive cosets are $a + n\mathbb{Z}$ where $a = 0, 1, \ldots, n-1$. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$, which allows us to define the ring isomorphism $\mu : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n, a + n\mathbb{Z} \to a$.*

Theorem 32.3. *Let H be an additive subgroup of $(R, +)$. Then multiplication of additive cosets is well defined if and only if $\forall x \in R, \forall h \in H$, $xh \in H$ and $hx \in H$.*

Proof. Let us prove that multiplication is well defined if $\forall x \in R, \forall h \in H$, $hx \in H, xh \in H$. If $a' \in a+H, b' \in b+H$, then $\exists h_1, h_2 \in H$ such that $a' = a+h_1$, $b' = b+h_2$. So $a'b' = (a+h_1)(b+h_2) = ab+h_1b+ah_2+h_1h_2$, so $a'b' \in ab + H$. This means multiplication is well defined.

If multiplication is well defined, then $\forall x \in R, \forall h \in H$, $(x+H)(h+H) = xh+H$. Because $h \in H, h+H = 0+H$ and therefore $(x + H)(0 + H) = x0 + H = H$. Therefore $xh \in H$. Similarly we see that $hx \in H$. □

Definition 65. *An ideal in a ring R is an additive subgroup H of R such that $\forall x \in R$, $xH \subseteq H$ and $Hx \subseteq H$.*

Example 32.4. *$n\mathbb{Z}$ is ideal in $\mathbb{Z}$; $\forall x \in \mathbb{Z}, \forall h \in n\mathbb{Z}, hx \in n\mathbb{Z}$.*

Corollary 32.5. *For any $\phi : R \to R'$, $\operatorname{Ker}\phi$ is an ideal in R.*

Theorem 32.6. *Let $H \leq R$ be an ideal. Then the additive cosets of H form a ring R/H with coset addition and coset multiplication. This ring is called the quotient ring. Moreover $\gamma : R \to R/H, x \to x + H$ is a surjective ring homomorphism with $\operatorname{Ker}\gamma = H$.*

Theorem 32.7. ***The Fundamental Homomorphism Theorem**: Let $\phi : R \to R'$ be a ring homomorphism with $\operatorname{Ker}\phi = H$. Then H is an ideal in R and the subring $\phi[R]$ is isomorphic to R/H by $\mu : R/H \to \phi[R], x + H \to \phi(x)$. Moreover, ϕ factors as $R \to \gamma[R] = R/H \to \mu[R/H] = \phi[x]$.*

Example 32.8. *$\mathbb{Z}$ is an integral domain and $n\mathbb{Z}$ is its ideal. Then $\mathbb{Z}/n\mathbb{Z} \equiv \mathbb{Z}_n$ is a field if n is prime and has divisors of zero if n is not prime (it is just a commutative ring with unity.)*

Example 32.9. *$\mathbb{Z} \times \mathbb{Z}$ is a commutative ring with unity (it has divisors of zero), and it has an ideal $N = \{0\} \times \mathbb{Z} = \{(0, a) \mid a \in \mathbb{Z}\}$.*

Theorem 32.10. *If R is a ring with unity and H is an ideal in R, then if H contains a unit, then $H = R$.*

Proof. Let $a \in H$ be a unit. Then $\exists a^{-1} \in R$ so that $aa^{-1} = a^{-1}a = 1$, so $1 \in H$ because $\forall b \in R$ and $\forall h \in H, bh \in H$. $\forall x \in R, x \cdot 1 \in H$, i.e. $\forall x \in R, x \in H$. Therefore $H = R$. □

Corollary 32.11. *If F is a field, the only ideals of F are $\{0\}$ and F.*

Remark 32.12. *Every ring R has at least two ideals, $\{0\}$ and itself.*

Remark 32.13. *R/R is isomorphic to the zero ring.*

Remark 32.14. *$R/\{0\}$ is isomorphic to R.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 33: Quotient Rings

Lecturer: Sylvie Corteel *24 April* *Aditya Sengupta*

Recall that an ideal of a ring is the generalization of a normal subgroup. We extend this definition to include the notion of no ideal superset of an ideal existing, which we call *maximal*:

Definition 66. *A maximal ideal of a ring R is an ideal $M \neq R$ (i.e. $M \subset R$) such that there is no ideal N with $M \subset N \subset R$.*

Example 33.1. *$p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ if p is prime.*

All the ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ with $n \in \mathbb{Z}$, but only the prime ones are maximal. We can show this; if $p\mathbb{Z}$ is not maximal, then there exists $m \in \mathbb{Z}$ such that $p\mathbb{Z} \subset m\mathbb{Z}$. This holds iff m divides p. As p is prime, we get $m = 1$ or $m = p$. Therefore there exists no m such that $p\mathbb{Z}$ is a proper subset of $m\mathbb{Z}$, and $m\mathbb{Z}$ is a proper subset of $\mathbb{Z}$. Therefore $p\mathbb{Z}$ is maximal.

Theorem 33.2. *If R is a commutative ring with unity, and if M is an ideal of R, then R/M is a field if and only if M is a maximal ideal.*

Remark 33.3. *If R has unity and N is an ideal of R, then R/N has unity $1 + N$.*

Remark 33.4. *If R is a commutative ring and N an ideal of R then R/N is commutative. (This can be shown explicitly with the definition of coset multiplication.)*

Proof. Let M be a maximal ideal, $M \subset R$. So $\exists a \in R$ such that $a \notin M$; $a \neq 0$ as $0 in M$. By contradiction, we suppose that $a + M$ has no multiplicative inverse in R/M, that is, R/M is not a field. Then there does not exist $r \in R$ such that $(r + M)(a + M) = (1 + M)$. This is equivalent to saying $\nexists r \in R, \nexists m \in M$ so that $ra + m = 1$. Let $H = \{ra + m \mid r \in R, m \in M\}$. We show first that H is an ideal of R. This requires that we show H is an additive subgroup of R, which just requires that we check the subgroup axioms (exercise to the reader!). It also requires that H is an ideal under multiplication; more formally, that $\forall x \in R$ and $\forall ra + m \in H$, $x \cdot (ra + m) \in H$. We easily show this using associativity of multiplication: $x \cdot (ra + m) = (xr)a + (xm) \in H$ as it is of the form $ra + m$. Therefore H is an ideal of R. Now, we show that $M \subset H$; $\forall m \in M, 0 \cdot a + m \in H$ so $m \in H$, i.e. $M \subseteq H$. But $a \in H$ as $a = 1 \cdot a + 0$ and $a \notin M$. Hence $M \subset H$. Therefore M is not maximal, which is a contradiction. Thereore, if M is maximal then R/M is a field.

We prove this in the other direction. Let us suppose that R/M is a field, and there exists an ideal N such that $M \subset N \subset R$. Let $\gamma : R \to R/M, x \to x + M$ be a surjective ring homomorphism, $\gamma[N] = \{n + M \mid n \in N\}$. We claim that $\gamma[N] = R/M$. First we show that $\gamma[N]$ is an ideal of R/M. By the theorem on homomorphisms, $\gamma[N]$ is an additive subgroup of R/M. Also, under multiplication, we can show that $\gamma[N]$ is an ideal: $\forall x \in R, \forall n \in N$, $(x + M)(n + M) = xn + M \in \gamma[N]$ because $xn \in N$. As R/M is a field, it has two ideals, $\{0 + M\}$ and R/M itself. We suppose that $M \subset N$. So $\exists n \in N, n \notin M$ so $n + M \in \gamma[N]$ but $n + M \neq 0 + M$, so $\gamma[N] = R/M$. Therefore, $\forall a \in R, \exists n \in N$ such that $a + M = n + M$. Therefore $a \in n + M \subseteq N$. So $R \subseteq N$ but N is an additive subgroup, so $N \subseteq R$. Therefore $R = N$ and M is maximal. □

Example 33.5. *The maximal ideals of $\mathbb{Z}$ are exactly $p\mathbb{Z}$.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 34: Prime and Principal Ideals

Lecturer: Sylvie Corteel *26 April* *Aditya Sengupta*

34.1 Prime Ideals

Definition 67. *An ideal $N \subset R$ in a commutative ring is a prime ideal if $a, b \in R$ and $ab \in N$ then $a \in N$ or $b \in N$.*

Recall that an integral domain is a commutative ring with no divisors of zero. For a quotient ring, this means if $a + N, b + N \in R/N$ such that $(a + N)(b + N) = 0 + N$ then $a + N = 0 + N$ or $b + N = 0 + N$.

Theorem 34.1. *If R is a commutative ring with unity and N is an ideal of R, then R/N is an integral domain if and only if N is a prime ideal.*

Proof. R/N is an integral domain if it has no divisors of zero, i.e. if $(a+N)(b+N) = 0+N \iff ab+N = 0 + N$, i.e. if $ab \in N$, then $a + N = 0 + N$ (if and only if $a \in N$) or $b + N = 0 + N$ (if and only if $b \in N$). Hence if $ab \in N$ then $a \in N$ or $b \in N$, thus N is prime. □

If M is a maximal ideal, we know that R/M is a field, which means R/M is an integral domain, i.e. by the above theorem M is a prime ideal.

Corollary 34.2. *Every maximal ideal is a prime ideal.*

34.2 Principal Ideals

Let $a \in R$ and $\langle a \rangle = \{ra \mid r \in R\}$. Then $\langle a \rangle$ is the principal ideal generated by a.

Remark 34.3. *$\langle a \rangle$ is the smallest ideal containing a.*

Example 34.4. *The ideals of $\mathbb{Z}$ are $\{n\mathbb{Z} \mid n \in \mathbb{Z}\}$. Every ideal of $\mathbb{Z}$ is principal.*

34.3 Ideals in rings of polynomials

Theorem 34.5. *Every ideal of $F[x]$, a ring of polynomials in one indeterminate x and coefficients in a field F, is principal.*

Proof. Let N be an ideal of $F[x]$. If $N = \{0\}$ then $N = \langle 0 \rangle$. Otherwise N contains at least one nonzero polynomial. Let $g(x)$ be a nonzero polynomial in N of minimal degree. If $\deg(g(x)) = 0$ then $g(x) = c \in F$. Then $N = F[x] = \langle 1 \rangle$. Otherwise we will show that $N = \langle g(x) \rangle$. Given $f(x) \in N$, by the division algorithm $f(x) = q(x)g(x)+r(x)$ with $\deg(r(x)) < \deg(g(x))$. We rearrange this to get $r(x) = f(x)-q(x)g(x)$. Because N is ideal, $q(x)g(x) \in N$, and because N is an additive subgroup, $f(x) - q(x)g(x) \in N$. Then $N \subseteq \langle g(x) \rangle$. But as $g(x) \in N$, $\langle g(x) \rangle \subseteq N$. Hence $N = \langle g(x) \rangle$. □

Theorem 34.6. *A nontrivial ideal $\langle p(x)\rangle$ of $F[x]$ is maximal if and only if $p(x)$ is irreducible over F.*

Proof. Suppose $\langle p(x)\rangle$ is maximal. Then $\langle p(x)\rangle \subset F[x]$, so $p(x)$ is not a constant polynomial. Let us assume that $p(x)$ is reducible. Then $\exists g(x), h(x)$ with $\deg(g(x)) < \deg(h(x)) < \deg(f(x))$ such that $p(x) = g(x)h(x)$. So $g(x)h(x) \in \langle p(x)\rangle$ as R has unity. As $\langle p(x)\rangle$ is maximal, $\langle p(x)\rangle$ is prime. So $g(x) \in \langle p(x)\rangle$ or $h(x) \in \langle p(x)\rangle$. But as $\langle p(x)\rangle = \{q(x)p(x) \mid q(x) \in F[x]\}$ all the polynomials in $\langle p(x)\rangle$ must have degree at least $\deg(p(x))$, so $g(x)$ or $h(x)$ cannot be elements of $\langle p(x)\rangle$. Therefore $p(x)$ is irreducible.

Conversely, suppose that $p(x)$ is irreducible over F and assume that there exists N such that $\langle p(x)\rangle \subset N \subset F[x]$, i.e. $\langle p(x)\rangle$ is not maximal. Let $N = \langle g(x)\rangle$ for $g(x) \in F[x]$. As $\langle p(x)\rangle \subset N$, then $p(x) \in \langle g(x)\rangle$. Hence $\exists q(x)$ such that $p(x) = q(x)g(x)$. But $p(x)$ is irreducible, so either $\deg(q(x)) = 0$, i.e. $\langle p(x)\rangle = \langle g(x)\rangle$ and $N = \langle p(x)\rangle$, or $\deg g(x) = 0$ and $N = \langle c\rangle = \langle F[x]\rangle$. Hence $\langle p(x)\rangle$ is maximal. □

Math 113: Abstract Algebra **Spring 2019**

Lecture 35: Factorization over polynomial rings, extension fields

Lecturer: Sylvie Corteel *28 April* *Aditya Sengupta*

35.1 Extension fields

We previously proved that every ideal of $F[x]$ is principal. Also, we know that $\langle p(x)\rangle$ is maximal if and only if $p(x)$ is irreducible. Therefore

Corollary 35.1. *$F[x]/\langle p(x)\rangle$ is a field iff $p(x)$ is irreducible.*

This can be applied to provide unique factorizations over F,

Theorem 35.2. *If $p(x) \in F[x]$ is irreducible over F, then if $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$ then $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.*

Proof. If $p(x)$ divides $r(x)s(x)$, then $r(x)s(x) \in \langle p(x)\rangle$, as $\langle p(x)\rangle = \{h(x)p(x) \mid h(x) \in F[x]\}$. As $p(x)$ is irreducible, $\langle p(x)\rangle$ is maximal and therefore prime. As $r(x)s(x) \in \langle p(x)\rangle$, $r(x) \in \langle p(x)\rangle$ or $s(x) \in \langle p(x)\rangle$. Hence $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$. □

35.2 Extension fields

Definition 68. *A field E is an extension of a field F if F is a subfield of E.*

Theorem 35.3. *(Kronecker's Theorem) Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists an extension field E of F and $\alpha \in E$ such that $f(\alpha) = 0$.*

To set up the proof, we list the following facts:

1. Over F, $f(x)$ factors into irreducible polynomials. Let $p(x)$ be one of them. Then it is sufficient to find E such that $\alpha \in E$ and $p(\alpha) = 0$. Then $f(\alpha) = 0$.
2. The principal ideal $\langle p(x)\rangle = \{h(x)p(x) \mid h(x) \in F[x]\}$ is maximal iff $p(x)$ is irreducible.
3. $F[x]/\langle p(x)\rangle$ is a field iff $p(x)$ is irreducible, where $F[x]/\langle p(x)\rangle = \{g(x) + \langle p(x)\rangle \mid g(x) \in F[x]\}$

Proof. Define $\psi : F \to F[x]/\langle p(x)\rangle, a \to a + \langle p(x)\rangle$. ψ is a ring homomorphism by the definitions of coset addition and multiplication. ψ is injective, because $\operatorname{Ker}\psi = \{0\}$. If $a \in \operatorname{Ker}\psi$, then $a + \langle p(x)\rangle = 0 + \langle p(x)\rangle = \langle p(x)\rangle$. This is true if and only if $a \in \langle p(x)\rangle$ and $a \in F$, which in turn is if and only if a is divisible by $p(x)$ and $a \in F$, so $a = 0$. Therefore ψ is injective.

As ψ is injective, F is isomorphic to a subfield of $F[x]/\langle p(x)\rangle$. Let $E = F[x]/\langle p(x)\rangle$. E is an extension of F. Now, let $\alpha = x + \langle p(x)\rangle \in E$. Let $p(x) = \sum_{i=0}^{n} a_i x^i$, and consider the evaluation homomorphism $\phi_\alpha : F[x] \to E, f(x) \to f(\alpha)$. Then $\phi_\alpha(p(x)) = a_0 + a_1(x + \langle p(x)\rangle) + \cdots + a_n(x + \langle p(x)\rangle)^n$. By coset multiplication, $(x + \langle p(x)\rangle)^k = x^k + \langle p(x)\rangle$. For any $c \in F$, $c\langle p(x)\rangle = \langle p(x)\rangle$. Therefore, the evaluation homomorphism comes out to $\phi_\alpha(p(x)) + p(x) + \langle p(x)\rangle = \langle p(x)\rangle$. So $\phi_\alpha(p(x)) = 0 + \langle p(x)\rangle = 0_E$. □

Example 35.4. *Let $F = \mathbb{R}$ and let $f(x) = x^2 + 1$. Then $E = \mathbb{R}[x]/\langle x^2 + 1\rangle$ is a field extension of $\mathbb{R}$, and $\alpha = x + \langle x^2 + 1\rangle$ satisfies $\alpha^2 + 1 = 0$ (we will prove that $E \equiv \mathbb{C}$.)*

Definition 69. *Given a field extension E of a field F and $\alpha \in E$, α is algebraic over F if there exists $f(x) \in F[x]$ such that $f(\alpha) = 0$. Then α is algebraic over F if there exists $f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise α is transcendental over F.*

Example 35.5. *Let $F = \mathbb{Q}$ and $E = \mathbb{C}$. Then i is algebraic over $\mathbb{Q}$, because there exists $x^2 + 1 \in \mathbb{Q}[x]$ such that $f(i) = 0$. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ for $f(x) = x^2 - 2$. π is transcendental over $\mathbb{Q}$, but showing this is hard. π is algebraic over $\mathbb{R}$, however, with $f(x) = x - \pi$.*

Math 113: Abstract Algebra **Spring 2019**

Lecture 36: Extension fields

Lecturer: Sylvie Corteel *1 May* *Aditya Sengupta*

Recall that E is an extension of a field F if F is a subfield of E. Let $p(x)$ be an irreducible polynomial in $F[x]$. Then an extension field of F is $E = F[x]/\langle p(x)\rangle$. Let $\alpha = x + \langle p(x)\rangle$; then $\phi_\alpha(p(x)) = 0 + \langle p(x)\rangle$.

Recall also that $\alpha \in E$ is algebraic over F if $\exists f(x) \in F[x]$ such that $f(x) \neq 0$ and $f(\alpha) = 0$. Otherwise α is transcendental.

Theorem 36.1. *Let $E \geq F$ and $\alpha \in E$, and define $\phi_\alpha : F[x] \to E, f(x) \to f(\alpha)$. Then α is transcendental if and only if ϕ_α is injective.*

Proof. α is transcendental over F if and only if $\nexists f(x) \in F[x]$ such that $f(x) \neq 0$ and $f(\alpha) = 0$, i.e. $\forall f(x) \in F[x]$ such that $f(x) \neq 0$, $\phi_\alpha(f(x)) \neq 0$, i.e. $\operatorname{Ker}\phi_\alpha = \{0\}$. Therefore ϕ_α is injective. □

Theorem 36.2. *Let E be a field extension of F and let α be an algebraic number over F, $\alpha \in E$. Then there exists an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. Moreover $p(x)$ is unique up to multiplication by a nonzero constant.*

Proof. As α is algebraic, $\operatorname{Ker}\phi_\alpha = \{f(x) \in F[x] \mid f(\alpha) = 0\}$ is a nontrivial ideal of $F[x]$. As every ideal of $F[x]$ is principal, there exists a polynomial $p(x) \in F[x]$ such that $\operatorname{Ker}\phi_\alpha = \langle p(x)\rangle$. Recall that $p(x)$ is defined as $\langle p(x)\rangle = \{h(x)p(x) \mid h(x) \in F[x]\}$. $\langle p(x)\rangle$ consists of all the elements of $F[x]$ having α as a zero. Therefore if $f(x) \in F[x]$ such that $f(x) \neq 0$ and α is a zero of $f(x)$, then $f(x) \in \langle p(x)\rangle$ so $p(x)$ divides $f(x)$. $p(x)$ is a polynomial of minimal degree ≥ 1, such that α is a zero of $p(x)$.

Let us suppose that $p(x)$ is reducible. Then $p(x) = r(x)s(x)$ with $\deg r < \deg p$ and $\deg s < \deg p$. As $p(\alpha) = 0$, $r(\alpha)s(\alpha) = 0$. As E is a field, $r(\alpha) \in E$ and $s(\alpha) \in E$. Then $r(\alpha) = 0$ or $s(\alpha) = 0$. This contradicts our assumption that $p(x)$ is of minimal degree. Therefore $p(x)$ is irreducible. As $p(x)$ divides every $f(x)$ in $\langle p(x)\rangle$, every polynomial of the same degree is equal to $cp(x)$ with $c \in F^*$, as required. □

Definition 70. *Let $f(x) \in F[x]$ such that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. $f(x)$ is monic iff $a_n = 1$.*

Definition 71. *Given α algebraic over F, we denote by $irr(\alpha, F)$ the unique monic irreducible polynomial such that α is a zero of this polynomial. Then* $\deg(\alpha, F) = \deg(irr(\alpha, F))$.

Example 36.3. *Let $F = \mathbb{Q}$ and $\alpha = \sqrt{2}$. Then $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$.*

Definition 72. *Given α algebraic over F, $F(\alpha)$ is the smallest subfield containing F and α. $\phi_\alpha : F[x] \to F(\alpha), f(x) \to f(\alpha)$ is a ring homomorphism with $\operatorname{Ker}\phi_\alpha = \langle p(x)\rangle$ where $p(x) = irr(\alpha, F)$. So $\phi_\alpha[F[x]] \equiv F[x]/\langle p(x)\rangle$, and so $F(\alpha) \equiv F[x]/\langle p(x)\rangle$.*

Definition 73. *Let E be an extension field of F. E is a simple extension if there exists $\alpha \in E$ such that $E = F(\alpha)$.*

Theorem 36.4. *If $E = F(\alpha)$ is a simple extension of F with α algebraic over F and $n = \deg(\alpha, F) \geq 1$, then every element $\beta \in E$ can be expressed uniquely as $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ for $b_i \in F$.*

Proof. We know that $\phi_\alpha[F[x]] = F(\alpha)$ so every element of E is the evaluation of a polynomial in $F[x]$, so every element of E is the evaluation of a polynomial in $F[x]$. $\phi_\alpha(c_0 + c_1x + \cdots + c_mx^m) = c_0 + c_1\alpha + \cdots + c_m\alpha^m$. Let $p(x) = irr(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. As $p(\alpha) = 0$, we get

$$\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - a_0 \tag{36.1}$$

so all powers α^k can be written as a linaer combination of $1, \alpha, \ldots, \alpha^{n-1}$. So $\exists b_0, \ldots, b_{n-1}$ such that $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$.

Now to prove uniqueness we suppose that $\beta = \sum_{i=0}^{n-1} b_i\alpha^i = \sum_{i=0}^{n-1} b_i'\alpha^i$. So $\sum_{i=0}^{n-1}(b_i - b_i')\alpha^i = 0$. If $b_i \neq b_i'$ for some i, this polynomial is of degree $< n$ and α is a zero of this polynomial. This is impossible as $p(x)$ is the polynomial of minimal degree such that $p(\alpha) = 0$. Therefore $b_i = b_i'$ and we have uniqueness. $\square$

Math 113: Abstract Algebra **Spring 2019**

Lecture 37: Extension fields contd., review

Lecturer: Sylvie Corteel *3 May* *Aditya Sengupta*

Remark 37.1. *If F is finite and $\deg(\alpha, F) = n$ then $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent. If F is finite then E has $|F|^n$ elements, as we have $|F|$ choices for each b_i.*

Example 37.2. *Let $F = \mathbb{Z}_2$ and $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. This has no zeroes in $\mathbb{Z}_2$ so it is irreducible. Set $\alpha = x + \langle x^2 + x + 1 \rangle$; then $\mathbb{Z}_2(\alpha) = \{b_0 + b_1\alpha \mid b_0, b_1 \in \mathbb{Z}_2\} = \{0, \alpha, 1, 1 + \alpha\}$. So $\mathbb{Z}_2(\alpha)$ is a field with 4 elements.*

Example 37.3. *Let $F = \mathbb{R}$ and $p(x) = x^2 + 1$. $p(x)$ is irreducible over $\mathbb{R}$. Then $\alpha = x + \langle p(x) \rangle$; $\mathbb{R}(\alpha) = \{b_0 + b_1\alpha \mid b_0, b_1 \in \mathbb{R}\}$. $\varphi : \mathbb{R}(\alpha) \to \mathbb{C}, b_0 + b_1\alpha \to b_0 + b_1 i$ is a field isomorphism.*

Example 37.4. *Let $F = \mathbb{Z}_3$ and $p(x) = x^3 - x + 2 \in \mathbb{Z}_3[x]$. $p(x)$ iteratively has no zero in $\mathbb{Z}_3$ and is irreducible. Now let $\alpha = x + \langle p(x) \rangle$ such that $\alpha^3 - \alpha + 2 = 0$; then $\mathbb{Z}_3(\alpha) = \{b_0 + b_1\alpha + b_2\alpha^2 \mid b_0, b_1, b_2 \in \mathbb{Z}_3\}$ is a field extension with $3^3 = 27$ elements.*

Now let's do math 110 in a few minutes.

Definition 74. *A vector space V over a field F is an abelian group for addition together with scalar multiplication $F \times V \to V$ such that $\forall a, b \in F, \forall u, v \in F$,*

1. $a(bu) = (ab)u$
2. $(a + b) \cdot u = au + bu$
3. $a(u + v) = au + av$
4. $1 \cdot u = u$

Some facts about vector spaces:

1. $\alpha_1, \ldots, \alpha_n \in V$ span V if every element $v \in V$ is a linear combination $v = \sum_i a_i\alpha_i$ with $a_i \in F$. $\{\alpha_i\}$ is a generating set.
2. V is finite dimensional if there exists a finite generating set
3. $\alpha_1, \ldots, \alpha_n \in V$ are linearly independent if $\sum_i a_i\alpha_i = 0$ implies all $\alpha_i = 0$.
4. $\alpha_1, \ldots, \alpha_n$ is a basis if they span V and are linearly independent.
5. In a finite-dimensional vector space, every basis has the same number of elements, called the dimension of V.

Back to field extensions: let α be algebraic over F and $\deg(\alpha, F) = n$. Then

$$F(\alpha) = \{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \mid a_0, \ldots, a_n \in F\} \tag{37.1}$$

$1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent.

Theorem 37.5. *Let $E \geq F$ be an extension field and let $\alpha \in E$ be algebraic over F, with $\deg(\alpha, F) = n$. Then $F(\alpha)$ is a vector space of dimension n over F with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Moreover, every element $\beta \in F(\alpha)$ is algebraic over F with $\deg(\beta, F) \leq n$.*

Proof. As $\deg(\alpha, F) = n$ we know that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent. So $\beta \in F(\alpha)$ can be written as a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. So $1, \alpha, \ldots, \alpha^{n-1}$ span $F(\alpha)$, i.e. they are a basis for $F(\alpha)$. So $F(\alpha)$ is a vector space of dimension n. Therefore if $\beta \in F(\alpha)$, then $1, \beta, \beta^2, \ldots, \beta^n$ cannot be linearly independent. So $\exists c_0, \ldots, c_n \in F$ such that $c_0 + c_1\beta + \cdots + c_n\beta^n = 0$. Hence $\deg(\beta, F) \leq n$. $\square$