Solving Polynomials

Part 2 - Eine Kleine Group Theory

Steve Ziskind

February 3, 2020

Algebra Bibliography

- I. N. Herstein, “Topics in Algebra”
- J. J. Rotman, “The Theory of Groups”
- B. L. van der Waerden, “Algebra”
- M. Artin, “Algebra”
- G. Birkoff and S. MacLane, “A Survey of Modern Algebra”

Groups

- A group is an algebraic structure comprised of 2 parts: a set of elements and an operation, denoted $\circledcirc$, that follows certain of the laws of arithmetic.

Groups

- A group is an algebraic structure comprised of 2 parts: a set of elements and an operation, denoted $\circledcirc$, that follows certain of the laws of arithmetic.
- Explicitly, the operation is binary, combining two elements into one, satisfying the following rules:

$$\boxed{\begin{array}{c} (x \circledcirc y) \circledcirc z = x \circledcirc (y \circledcirc z) \quad \forall x, y, z \\ \exists e \text{ so that } x \circledcirc e = e \circledcirc x = x \quad \forall x \\ \forall x \exists y \text{ so that } x \circledcirc y = y \circledcirc x = e \end{array}}$$

Groups

- A group is an algebraic structure comprised of 2 parts: a set of elements and an operation, denoted $\circledcirc$, that follows certain of the laws of arithmetic.
- Explicitly, the operation is binary, combining two elements into one, satisfying the following rules:

$$\boxed{\begin{array}{c} (x \circledcirc y) \circledcirc z = x \circledcirc (y \circledcirc z) \quad \forall x, y, z \\ \exists e \text{ so that } x \circledcirc e = e \circledcirc x = x \quad \forall x \\ \forall x \exists y \text{ so that } x \circledcirc y = y \circledcirc x = e \end{array}}$$

- In words: the operation obeys the Associative Law, there is an identity element, and each element has an inverse.

Groups

- A group is an algebraic structure comprised of 2 parts: a set of elements and an operation, denoted $\circledcirc$, that follows certain of the laws of arithmetic.
- Explicitly, the operation is binary, combining two elements into one, satisfying the following rules:

$$\boxed{\begin{array}{c} (x \circledcirc y) \circledcirc z = x \circledcirc (y \circledcirc z) \quad \forall x, y, z \\ \exists e \text{ so that } x \circledcirc e = e \circledcirc x = x \quad \forall x \\ \forall x \exists y \text{ so that } x \circledcirc y = y \circledcirc x = e \end{array}}$$

- In words: the operation obeys the Associative Law, there is an identity element, and each element has an inverse.
- We do not assume the commutative property. If it does hold the group is called Abelian, in honor and memory of Niels H. Abel (1802-1829).

Some Examples of Groups

- $(\mathbb{R}^n, +)$ is a group, as is any vector space. We ignore scalar multiplication in this. The origin is the identity.

Some Examples of Groups

- $(\mathbb{R}^n, +)$ is a group, as is any vector space. We ignore scalar multiplication in this. The origin is the identity.
- $(\mathbb{R}^+, \times)$ is a group, The identity is 1, inverses are reciprocals.

Some Examples of Groups

- $(\mathbb{R}^n, +)$ is a group, as is any vector space. We ignore scalar multiplication in this. The origin is the identity.
- $(\mathbb{R}^+, \times)$ is a group, The identity is 1, inverses are reciprocals.
- $(GL_n, \times)$, the invertible *nxn* matrices, where the identity matrix is the group identity element. This is also known as the General Linear Group.

Some Examples of Groups

- $(\mathbb{R}^n, +)$ is a group, as is any vector space. We ignore scalar multiplication in this. The origin is the identity.
- $(\mathbb{R}^+, \times)$ is a group, The identity is 1, inverses are reciprocals.
- $(GL_n, \times)$, the invertible *nxn* matrices, where the identity matrix is the group identity element. This is also known as the General Linear Group.
- SO(3) is the group of orthogonal 3x3 matrices with determinant$=$1. These represent the orientation preserving rotations of $\mathbb{R}^3$.

Some Examples of Groups

- The symmetric group, S_n, is the group of permutations of n objects, where the group operation is concatenation. These groups are critical to the problem of solving the fifth degree polynomial algebraically. In general the order of S_n, i.e. the number of elements in it, is $n!$.

Some Examples of Groups

- The symmetric group, S_n, is the group of permutations of n objects, where the group operation is concatenation. These groups are critical to the problem of solving the fifth degree polynomial algebraically. In general the order of S_n, i.e. the number of elements in it, is $n!$.
- The dihedral group, D_n is the group of rigid motions of the regular n-gon that send vertices to vertices. It can be built from rotations and from reflections that pass through the center. As an example, D_4, the motions of a square, has 8 members, built from iterating a 90° rotation and a single reflection. Generally, D_n has order 2n (homework).

Subgroups

- When H is a subset of a group G that, all by itself, satisfies the group axioms, we say that H is a subgroup of G.

Subgroups

- When H is a subset of a group G that, all by itself, satisfies the group axioms, we say that H is a subgroup of G.
- Because H will inherit the associative property from G, we only need to check closure, the existence of the identity element, and the existence of inverses.

Subgroups

- When H is a subset of a group G that, all by itself, satisfies the group axioms, we say that H is a subgroup of G.
- Because H will inherit the associative property from G, we only need to check closure, the existence of the identity element, and the existence of inverses.
- Ex: $(\mathbb{R}^2, +)$ is a subgroup of $(\mathbb{R}^3, +)$. (Actually we mean the vectors $\{x, y, 0\}$, which isn't exactly $\mathbb{R}^2$)

Subgroups

- When H is a subset of a group G that, all by itself, satisfies the group axioms, we say that H is a subgroup of G.
- Because H will inherit the associative property from G, we only need to check closure, the existence of the identity element, and the existence of inverses.
- Ex: $(\mathbb{R}^2, +)$ is a subgroup of $(\mathbb{R}^3, +)$. (Actually we mean the vectors $\{x, y, 0\}$, which isn't exactly $\mathbb{R}^2$)
- Ex: $(SL_n, \times) = \{A \in GL_n | det(A) = 1\}$, the Special Linear Group, is a subgroup of $(GL_n, \times)$

Subgroups

- When H is a subset of a group G that, all by itself, satisfies the group axioms, we say that H is a subgroup of G.
- Because H will inherit the associative property from G, we only need to check closure, the existence of the identity element, and the existence of inverses.
- Ex: $(\mathbb{R}^2, +)$ is a subgroup of $(\mathbb{R}^3, +)$. (Actually we mean the vectors $\{x, y, 0\}$, which isn't exactly $\mathbb{R}^2$)
- Ex: $(SL_n, \times) = \{A \in GL_n | det(A) = 1\}$, the Special Linear Group, is a subgroup of $(GL_n, \times)$
- Ex: If $12\mathbb{Z} = \{n \in \mathbb{Z}|$ n is a multiple of 12 $\}$, then $(12\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$

Subgroups

- When H is a subset of a group G that, all by itself, satisfies the group axioms, we say that H is a subgroup of G.
- Because H will inherit the associative property from G, we only need to check closure, the existence of the identity element, and the existence of inverses.
- Ex: $(\mathbb{R}^2, +)$ is a subgroup of $(\mathbb{R}^3, +)$. (Actually we mean the vectors $\{x, y, 0\}$, which isn't exactly $\mathbb{R}^2$)
- Ex: $(SL_n, \times) = \{A \in GL_n | det(A) = 1\}$, the Special Linear Group, is a subgroup of $(GL_n, \times)$
- Ex: If $12\mathbb{Z} = \{n \in \mathbb{Z}|$ n is a multiple of 12 $\}$, then $(12\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$
- Ex: $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$

Cosets and Quotient Groups

- Consider $12\mathbb{Z}$, defined above as a subgroup. We can break $\mathbb{Z}$ into 12 subsets by saying that elements are equivalent (in the same set) when $m \equiv n \pmod{12}$ i.e. when $m - n \in 12\mathbb{Z}$. These 12 subsets have a natural addition modulo 12, inducing on the sets a group operation. This is sometimes called the Clock Group.

Cosets and Quotient Groups

- Consider $12\mathbb{Z}$, defined above as a subgroup. We can break $\mathbb{Z}$ into 12 subsets by saying that elements are equivalent (in the same set) when $m \equiv n \pmod{12}$ i.e. when $m - n \in 12\mathbb{Z}$. These 12 subsets have a natural addition modulo 12, inducing on the sets a group operation. This is sometimes called the Clock Group.
- More generally, with H a subgroup of G, we want to use H to break G into subsets, and induce a group structure into these sets.

Cosets and Quotient Groups

- Consider $12\mathbb{Z}$, defined above as a subgroup. We can break $\mathbb{Z}$ into 12 subsets by saying that elements are equivalent (in the same set) when $m \equiv n \pmod{12}$ i.e. when $m - n \in 12\mathbb{Z}$. These 12 subsets have a natural addition modulo 12, inducing on the sets a group operation. This is sometimes called the Clock Group.
- More generally, with H a subgroup of G, we want to use H to break G into subsets, and induce a group structure into these sets.
- By analogy to $m \equiv n \pmod{12}$ we say that a and b are in the same subset when $ab^{-1} \in H$.

Cosets and Quotient Groups

- Consider $12\mathbb{Z}$, defined above as a subgroup. We can break $\mathbb{Z}$ into 12 subsets by saying that elements are equivalent (in the same set) when $m \equiv n \pmod{12}$ i.e. when $m - n \in 12\mathbb{Z}$. These 12 subsets have a natural addition modulo 12, inducing on the sets a group operation. This is sometimes called the Clock Group.
- More generally, with H a subgroup of G, we want to use H to break G into subsets, and induce a group structure into these sets.
- By analogy to $m \equiv n \pmod{12}$ we say that a and b are in the same subset when $ab^{-1} \in H$.
- This means that the subsets of G are of the form $Ha = \{ha | h \in H\}$. Such a set is called a right coset. We want to define a group operation on cosets by defining $(Ha)(Hb) = Hab$. But ... does this actually work?

Cosets and Quotient Groups

- To begin, we must insure that the operation is well defined. i.e. we need $(Ha)(Hb)$ to be independent of the representatives chosen from H. In other words, given any h_1ah_2b there must be some h_3 for which $h_1ah_2b = h_3ab$

Cosets and Quotient Groups

- To begin, we must insure that the operation is well defined. i.e. we need $(Ha)(Hb)$ to be independent of the representatives chosen from H. In other words, given any $h_1 a h_2 b$ there must be some h_3 for which $h_1 a h_2 b = h_3 ab$
- Multiplying by $b^{-1}a^{-1}$ on the right and by h_1^{-1} on the left, this requires that $a h_2 a^{-1} \in H$.

Cosets and Quotient Groups

- To begin, we must insure that the operation is well defined. i.e. we need $(Ha)(Hb)$ to be independent of the representatives chosen from H. In other words, given any h_1ah_2b there must be some h_3 for which $h_1ah_2b = h_3ab$
- Multiplying by $b^{-1}a^{-1}$ on the right and by h_1^{-1} on the left, this requires that $ah_2a^{-1} \in H$.
- The identity coset will be H. We need to be sure that $(Hg)(Hg^{-1}) = H$, which means that we always have $h_1gh_2g^{-1} \in H$, and this requires that we always have $ghg^{-1} \in H$.

Cosets and Quotient Groups

- To begin, we must insure that the operation is well defined. i.e. we need $(Ha)(Hb)$ to be independent of the representatives chosen from H. In other words, given any $h_1 a h_2 b$ there must be some h_3 for which $h_1 a h_2 b = h_3 ab$
- Multiplying by $b^{-1}a^{-1}$ on the right and by h_1^{-1} on the left, this requires that $ah_2a^{-1} \in H$.
- The identity coset will be H. We need to be sure that $(Hg)(Hg^{-1}) = H$, which means that we always have $h_1 g h_2 g^{-1} \in H$, and this requires that we always have $ghg^{-1} \in H$.
- A subgroup H of G is called a <u>normal subgroup</u> when $gHg^{-1} \subset H \quad \forall g \in G$. This is written $H \lhd G$.

Cosets and Quotient Groups

- To begin, we must insure that the operation is well defined. i.e. we need $(Ha)(Hb)$ to be independent of the representatives chosen from H. In other words, given any h_1ah_2b there must be some h_3 for which $h_1ah_2b = h_3ab$
- Multiplying by $b^{-1}a^{-1}$ on the right and by h_1^{-1} on the left, this requires that $ah_2a^{-1} \in H$.
- The identity coset will be H. We need to be sure that $(Hg)(Hg^{-1}) = H$, which means that we always have $h_1gh_2g^{-1} \in H$, and this requires that we always have $ghg^{-1} \in H$.
- A subgroup H of G is called a normal subgroup when $gHg^{-1} \subset H \quad \forall g \in G$. This is written $H \lhd G$.
- The resulting group of cosets, with the induced group operation, is called the quotient group, and denoted G/H.

Cosets and Lagrange's Theorem

- Any 2 (right) cosets of a subgroup are either disjoint or identical. For suppose that Ha and Hb overlap. Then $h_1 a = h_2 b$ so that $a = h_1^{-1} h_2 b \in Hb$. Thus $Ha \subset Hb$, and conversely by symmetry.

Cosets and Lagrange's Theorem

- Any 2 (right) cosets of a subgroup are either disjoint or identical. For suppose that Ha and Hb overlap. Then $h_1 a = h_2 b$ so that $a = h_1^{-1} h_2 b \in Hb$. Thus $Ha \subset Hb$, and conversely by symmetry.
- (Lagrange) If H is a subgroup of G, and G has a finite number of elements (its <u>order</u>, denoted $|G|$), then$|H|$ divides $|G|$. To prove this just exhaust G by disjoint cosets of H. The number of disjoint cosets, the <u>index</u> of H in G, is denoted $[G : H]$. Thus we find that, for a finite group G, $|G| = |H|[G : H]$

Cosets and Lagrange's Theorem

- Any 2 (right) cosets of a subgroup are either disjoint or identical. For suppose that Ha and Hb overlap. Then $h_1 a = h_2 b$ so that $a = h_1^{-1} h_2 b \in Hb$. Thus $Ha \subset Hb$, and conversely by symmetry.
- (Lagrange) If H is a subgroup of G, and G has a finite number of elements (its order, denoted $|G|$), then$|H|$ divides $|G|$. To prove this just exhaust G by disjoint cosets of H. The number of disjoint cosets, the index of H in G, is denoted $[G : H]$. Thus we find that, for a finite group G, $|G| = |H|[G : H]$
- Lagrange implies that, for example, a group of order 60 cannot have a subgroup of order 24. But just because a number divides the order of a group it does not guarantee that a subgroup of that order exists.

Cosets and Lagrange's Theorem

- Any 2 (right) cosets of a subgroup are either disjoint or identical. For suppose that Ha and Hb overlap. Then $h_1 a = h_2 b$ so that $a = h_1^{-1} h_2 b \in Hb$. Thus $Ha \subset Hb$, and conversely by symmetry.
- (Lagrange) If H is a subgroup of G, and G has a finite number of elements (its order, denoted $|G|$), then $|H|$ divides $|G|$. To prove this just exhaust G by disjoint cosets of H. The number of disjoint cosets, the index of H in G, is denoted $[G : H]$. Thus we find that, for a finite group G, $|G| = |H|[G : H]$
- Lagrange implies that, for example, a group of order 60 cannot have a subgroup of order 24. But just because a number divides the order of a group it does not guarantee that a subgroup of that order exists.
- Note that if $H \lhd G$ then the left and right cosets of H are identical. (Easy check)

Isomorphism

- If $(G, \circledcirc)$ and $(H, \blacklozenge)$ are both groups, then we say they are isomorphic is there is a mapping between them that is 1-1 and onto, and preserves the group structure.

Isomorphism

- If $(G, \circledcirc)$ and $(H, \blacklozenge)$ are both groups, then we say they are isomorphic is there is a mapping between them that is 1-1 and onto, and preserves the group structure.
- Explicitly, G and H are isomorphic, written $G \approx H$, when there is a function $\varphi : G \to H$ which is one-to one, onto, and satisfies $\varphi(a \circledcirc b) = \varphi(a) \blacklozenge \varphi(b) \quad \forall a, b \in G$.

Isomorphism

- If $(G, \circledcirc)$ and $(H, \blacklozenge)$ are both groups, then we say they are isomorphic is there is a mapping between them that is 1-1 and onto, and preserves the group structure.
- Explicitly, G and H are isomorphic, written $G \approx H$, when there is a function $\varphi : G \to H$ which is one-to one, onto, and satisfies $\varphi(a \circledcirc b) = \varphi(a) \blacklozenge \varphi(b) \quad \forall a, b \in G$.
- Ex: Let G be the subgroup of GL_2 of elements of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. As $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$, we see that G is isomorphic to $(\mathbb{R}, +)$ via the obvious φ.

Isomorphism

- If $(G, \circledcirc)$ and $(H, \blacklozenge)$ are both groups, then we say they are <u>isomorphic</u> is there is a mapping between them that is 1-1 and onto, and preserves the group structure.
- Explicitly, G and H are isomorphic, written $G \approx H$, when there is a function $\varphi : G \to H$ which is one-to one, onto, and satisfies $\varphi(a \circledcirc b) = \varphi(a) \blacklozenge \varphi(b) \quad \forall a, b \in G$.
- Ex: Let G be the subgroup of GL_2 of elements of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. As $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$, we see that G is isomorphic to $(\mathbb{R}, +)$ via the obvious φ.
- Ex: Let $G = (\mathbb{R}^+, \times), H = (\mathbb{R}, +)$. Then $\varphi = \log$ is an isomorphism from G to H.

Isomorphism

- If $(G, \circledcirc)$ and $(H, \blacklozenge)$ are both groups, then we say they are <u>isomorphic</u> is there is a mapping between them that is 1-1 and onto, and preserves the group structure.
- Explicitly, G and H are isomorphic, written $G \approx H$, when there is a function $\varphi : G \to H$ which is one-to one, onto, and satisfies $\varphi(a \circledcirc b) = \varphi(a) \blacklozenge \varphi(b) \quad \forall a, b \in G$.
- Ex: Let G be the subgroup of GL_2 of elements of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. As $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$, we see that G is isomorphic to $(\mathbb{R}, +)$ via the obvious φ.
- Ex: Let $G = (\mathbb{R}^+, \times), H = (\mathbb{R}, +)$. Then $\varphi = \log$ is an isomorphism from G to H.
- Ex: D_3 is isomorphic to S_3, but D_4 is not isomorphic to S_4.

Automorphisms

- Sometimes the two groups that are isomorphic are the same group. In this case we call the isomorphism an automorphism.

Automorphisms

- Sometimes the two groups that are isomorphic are the same group. In this case we call the isomorphism an automorphism.
- Ex: Let $G = \{0, 1, 2\}$, with addition performed modulo 3. Then the mapping from G to itself defined by: $\varphi(0) = 0, \varphi(1) = 2, \varphi(2) = 1$ is an automorphism. Note that the identity must be carried to the identity.

Automorphisms

- Sometimes the two groups that are isomorphic are the same group. In this case we call the isomorphism an automorphism.
- Ex: Let $G = \{0, 1, 2\}$, with addition performed modulo 3. Then the mapping from G to itself defined by: $\varphi(0) = 0, \varphi(1) = 2, \varphi(2) = 1$ is an automorphism. Note that the identity must be carried to the identity.
- Sending x to -x is an automorphism of $(\mathbb{Z}, +)$

Automorphisms

- Sometimes the two groups that are isomorphic are the same group. In this case we call the isomorphism an automorphism.
- Ex: Let $G = \{0, 1, 2\}$, with addition performed modulo 3. Then the mapping from G to itself defined by: $\varphi(0) = 0, \varphi(1) = 2, \varphi(2) = 1$ is an automorphism. Note that the identity must be carried to the identity.
- Sending x to -x is an automorphism of $(\mathbb{Z}, +)$
- Given any fixed element $a \in G$, define $\varphi(x) = axa^{-1}$. This is always an automorphism, known as an inner automorphism. The product axa^{-1} is called the conjugate of x by a, and the method is called conjugation. Note: for GL_n, this is the change of basis formula.

Automorphisms

- Sometimes the two groups that are isomorphic are the same group. In this case we call the isomorphism an automorphism.
- Ex: Let $G = \{0, 1, 2\}$, with addition performed modulo 3. Then the mapping from G to itself defined by: $\varphi(0) = 0, \varphi(1) = 2, \varphi(2) = 1$ is an automorphism. Note that the identity must be carried to the identity.
- Sending x to -x is an automorphism of $(\mathbb{Z}, +)$
- Given any fixed element $a \in G$, define $\varphi(x) = axa^{-1}$. This is always an automorphism, known as an inner automorphism. The product axa^{-1} is called the conjugate of x by a, and the method is called conjugation. Note: for GL_n, this is the change of basis formula.
- A subgroup of a group is normal if it is fixed by all the inner automorphisms from the parent group.

Homomorphisms

- If we drop the 1-1 and onto requirements of an isomorphism, then φ is called a homomorphism. In short, we only require that $\varphi(xy) = \varphi(x)\varphi(y)$. (Note: we are denoting the group operation by multiplication, and will write 1 for the identity.)

Homomorphisms

- If we drop the 1-1 and onto requirements of an isomorphism, then φ is called a homomorphism. In short, we only require that $\varphi(xy) = \varphi(x)\varphi(y)$. (Note: we are denoting the group operation by multiplication, and will write 1 for the identity.)
- Homomorphisms take the identity to the identity, and inverses to inverses (easy homework problem).

Homomorphisms

- If we drop the 1-1 and onto requirements of an isomorphism, then φ is called a homomorphism. In short, we only require that $\varphi(xy) = \varphi(x)\varphi(y)$. (Note: we are denoting the group operation by multiplication, and will write 1 for the identity.)
- Homomorphisms take the identity to the identity, and inverses to inverses (easy homework problem).
- The kernel of a homomorphism, $ker(\varphi)$, is the set of elements taken to the identity in the range group.

Homomorphisms

- If we drop the 1-1 and onto requirements of an isomorphism, then φ is called a homomorphism. In short, we only require that $\varphi(xy) = \varphi(x)\varphi(y)$. (Note: we are denoting the group operation by multiplication, and will write 1 for the identity.)
- Homomorphisms take the identity to the identity, and inverses to inverses (easy homework problem).
- The kernel of a homomorphism, $ker(\varphi)$, is the set of elements taken to the identity in the range group.
- Theorem: $ker(\varphi)$ is always a normal subgroup of its domain. Conversely, if $H \lhd G$ then there is a homomorphism from G onto G/H whose kernel is H.

Homomorphisms

- If we drop the 1-1 and onto requirements of an isomorphism, then φ is called a homomorphism. In short, we only require that $\varphi(xy) = \varphi(x)\varphi(y)$. (Note: we are denoting the group operation by multiplication, and will write 1 for the identity.)
- Homomorphisms take the identity to the identity, and inverses to inverses (easy homework problem).
- The kernel of a homomorphism, $ker(\varphi)$, is the set of elements taken to the identity in the range group.
- Theorem: $ker(\varphi)$ is always a normal subgroup of its domain. Conversely, if $H \triangleleft G$ then there is a homomorphism from G onto G/H whose kernel is H.
- Proof: Normality is immediate. Conversely, given a normal subgroup we map each element, a, to its coset, Ha. This was shown above to carry G to G/H, and is a homomorphism with H as its kernel.

Cyclic Groups

- Consider the clock group, $\mathbb{Z}/12\mathbb{Z}$. In essence it consists of the numbers 0..11, where addition is performed modulo 12. This group is generated by the number(coset) 1, because repeatedly adding 1 will generate everything. It is called a cyclic group.

Cyclic Groups

- Consider the clock group, $\mathbb{Z}/12\mathbb{Z}$. In essence it consists of the numbers 0..11, where addition is performed modulo 12. This group is generated by the number(coset) 1, because repeatedly adding 1 will generate everything. It is called a cyclic group.
- Generally, denoting the group operation by multiplication, if every element is of the form a^k then the group is called cyclic. In the case of a finite group, the group consists of $\{1, a, \ldots, a^{n-1}\}$. It is analogous to a clock with n hours. It is written $\mathbb{Z}_n$.

Cyclic Groups

- Consider the clock group, $\mathbb{Z}/12\mathbb{Z}$. In essence it consists of the numbers 0..11, where addition is performed modulo 12. This group is generated by the number(coset) 1, because repeatedly adding 1 will generate everything. It is called a cyclic group.
- Generally, denoting the group operation by multiplication, if every element is of the form a^k then the group is called cyclic. In the case of a finite group, the group consists of $\{1, a, \ldots, a^{n-1}\}$. It is analogous to a clock with n hours. It is written $\mathbb{Z}_n$.
- If $|G| = p$, a prime number, then it must be the cyclic group $\mathbb{Z}_p$. This follows from Lagrange, for taking powers of some element other than the identity, we will generate a subgroup, whose order must divide p, hence must be all of G. A cyclic group is always Abelian.

Simplicity

- Considering $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 10, 11\}$, under addition modulo 12, there is a subgroup within it, namely $\{0, 4, 8\}$ under the same operation. This subgroup is normal in $\mathbb{Z}_{12}$, and the image of the homomorphism: $(0, 3, 6, 9) \to 0$, $(1, 4, 7, 10) \to 4$, and $(2, 5, 8, 11) \to 8$. The subgroup is isomorphic to $\mathbb{Z}_3$

Simplicity

- Considering $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 10, 11\}$, under addition modulo 12, there is a subgroup within it, namely $\{0, 4, 8\}$ under the same operation. This subgroup is normal in $\mathbb{Z}_{12}$, and the image of the homomorphism: $(0, 3, 6, 9) \to 0$, $(1, 4, 7, 10) \to 4$, and $(2, 5, 8, 11) \to 8$. The subgroup is isomorphic to $\mathbb{Z}_3$
- The prime order groups, $\mathbb{Z}_p$ have no such normal subgroups.

Simplicity

- Considering $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 10, 11\}$, under addition modulo 12, there is a subgroup within it, namely $\{0, 4, 8\}$ under the same operation. This subgroup is normal in $\mathbb{Z}_{12}$, and the image of the homomorphism: $(0, 3, 6, 9) \rightarrow 0$, $(1, 4, 7, 10) \rightarrow 4$, and $(2, 5, 8, 11) \rightarrow 8$. The subgroup is isomorphic to $\mathbb{Z}_3$
- The prime order groups, $\mathbb{Z}_p$ have no such normal subgroups.
- A group with no non-trivial normal subgroups is called <u>simple</u>. In a rough sense, simple groups are like prime numbers, they have no similar structure within them.

Simplicity

- Considering $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 10, 11\}$, under addition modulo 12, there is a subgroup within it, namely $\{0, 4, 8\}$ under the same operation. This subgroup is normal in $\mathbb{Z}_{12}$, and the image of the homomorphism: $(0, 3, 6, 9) \rightarrow 0$, $(1, 4, 7, 10) \rightarrow 4$, and $(2, 5, 8, 11) \rightarrow 8$. The subgroup is isomorphic to $\mathbb{Z}_3$
- The prime order groups, $\mathbb{Z}_p$ have no such normal subgroups.
- A group with no non-trivial normal subgroups is called simple. In a rough sense, simple groups are like prime numbers, they have no similar structure within them.
- Around 1980, a 30+ year effort involving many thousands of publication pages produced a complete list of all finite simple groups. The theorem is sometimes called The Enormous Theorem, and the effort The Thirty Years War.

Simplicity

- Considering $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 10, 11\}$, under addition modulo 12, there is a subgroup within it, namely $\{0, 4, 8\}$ under the same operation. This subgroup is normal in $\mathbb{Z}_{12}$, and the image of the homomorphism: $(0, 3, 6, 9) \to 0$, $(1, 4, 7, 10) \to 4$, and $(2, 5, 8, 11) \to 8$. The subgroup is isomorphic to $\mathbb{Z}_3$
- The prime order groups, $\mathbb{Z}_p$ have no such normal subgroups.
- A group with no non-trivial normal subgroups is called simple. In a rough sense, simple groups are like prime numbers, they have no similar structure within them.
- Around 1980, a 30+ year effort involving many thousands of publication pages produced a complete list of all finite simple groups. The theorem is sometimes called The Enormous Theorem, and the effort The Thirty Years War.
- Simple groups play a key role in the problem of the quintic.

S_n and A_n

- The symmetric groups, S_n, are those whose elements are the permutations of the numbers 1 to n. Equivalently, they are the permutations of any n distinct objects, numbers just being one convenient way to represent their action. The group operation is concatenation, i.e. one permutation followed by another.

S_n and A_n

- The symmetric groups, S_n, are those whose elements are the permutations of the numbers 1 to n. Equivalently, they are the permutations of any n distinct objects, numbers just being one convenient way to represent their action. The group operation is concatenation, i.e. one permutation followed by another.
- The obvious way to describe such a permutation is to list what happens to each number, for example: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

S_n and A_n

- The symmetric groups, S_n, are those whose elements are the permutations of the numbers 1 to n. Equivalently, they are the permutations of any n distinct objects, numbers just being one convenient way to represent their action. The group operation is concatenation, i.e. one permutation followed by another.
- The obvious way to describe such a permutation is to list what happens to each number, for example: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$
- To shorten the notation, we can write this example as: (123)(45), with the understanding that a list like (1 2 3) means that $(1 \to 2, 2 \to 3, 3 \to 1)$. Obviously a full permutation can be written as a product of independent cyclic permutations.

S_n and A_n

- The symmetric groups, S_n, are those whose elements are the permutations of the numbers 1 to n. Equivalently, they are the permutations of any n distinct objects, numbers just being one convenient way to represent their action. The group operation is concatenation, i.e. one permutation followed by another.
- The obvious way to describe such a permutation is to list what happens to each number, for example: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$
- To shorten the notation, we can write this example as: (123)(45), with the understanding that a list like (1 2 3) means that $(1 \to 2, 2 \to 3, 3 \to 1)$. Obviously a full permutation can be written as a product of independent cyclic permutations.
- In general, we apply the action of permutations from right to left. Thus, for example, we interpret (1 2)(1 3) as (1 3 2).

S_n and A_n

- A special permutation, a transposition, is one that swaps exactly two numbers, leaving the others unchanged. For example (1 3).

S_n and A_n

- A special permutation, a transposition, is one that swaps exactly two numbers, leaving the others unchanged. For example $(1\ 3)$.
- Every permutation is a product of transpositions because, for example, $(12345) = (15)(14)(13)(12)$

S_n and A_n

- A special permutation, a transposition, is one that swaps exactly two numbers, leaving the others unchanged. For example (1 3).
- Every permutation is a product of transpositions because, for example, $(12345) = (15)(14)(13)(12)$
- When a permutation is written as a product of transpositions, the number of transpositions is not unique. What is unique, however, is the parity of the number. That is:

S_n and A_n

- A special permutation, a transposition, is one that swaps exactly two numbers, leaving the others unchanged. For example (1 3).
- Every permutation is a product of transpositions because, for example, $(12345) = (15)(14)(13)(12)$
- When a permutation is written as a product of transpositions, the number of transpositions is not unique. What is unique, however, is the parity of the number. That is:
- Theorem: If a permutation is written as a product of transpositions in two different ways, then both ways involve either an even number of transpositions or an odd number of transpositions.

S_n and A_n

- Proof: Instead of the permutations acting on 1 through n, consider it to be acting on the n standard basis vectors of $\mathbb{R}^n$.

S_n and A_n

- Proof: Instead of the permutations acting on 1 through n, consider it to be acting on the n standard basis vectors of $\mathbb{R}^n$.
- The identity permutation corresponds to the $n \times n$ identity matrix. Every transposition interchanges two columns of the matrix, changing the sign of the determinant. If one expression used an odd number of transpositions and another used an even number, then the determinant would be either -1 or $+1$ for the same resulting matrix. Impossible if you believe the properties of determinants. QED

S_n and A_n

- Proof: Instead of the permutations acting on 1 through n, consider it to be acting on the n standard basis vectors of $\mathbb{R}^n$.
- The identity permutation corresponds to the $n \times n$ identity matrix. Every transposition interchanges two columns of the matrix, changing the sign of the determinant. If one expression used an odd number of transpositions and another used an even number, then the determinant would be either -1 or $+1$ for the same resulting matrix. Impossible if you believe the properties of determinants. QED
- Another way of saying this: the determinant function is a homomorphism from the set of permutation matrices to the group ($+1$, -1). The kernel of the determinant is the set sent to $+1$.

A_5 is Simple

- The set of permutations built from an even number of transpositions is the kernel of the determinant, hence is a normal subgroup of S_n. It is called the Alternating Group on n elements, written A_n. In short, $A_n \lhd S_n$.

A_5 is Simple

- The set of permutations built from an even number of transpositions is the kernel of the determinant, hence is a normal subgroup of S_n. It is called the Alternating Group on n elements, written A_n. In short, $A_n \lhd S_n$.
- A key step in showing the quintic unsolvable will be to show that A_5 is simple. There are many ways to do this, none entirely simple.

A_5 is Simple

- The set of permutations built from an even number of transpositions is the kernel of the determinant, hence is a normal subgroup of S_n. It is called the Alternating Group on n elements, written A_n. In short, $A_n \lhd S_n$.
- A key step in showing the quintic unsolvable will be to show that A_5 is simple. There are many ways to do this, none entirely simple.
- Our proof, adapted from Rotman's book, will count various sets of even permutations, and then show that only two possibilities, corresponding to trivial subgroups can possibly be normal.

A_5 is Simple

- The set of permutations built from an even number of transpositions is the kernel of the determinant, hence is a normal subgroup of S_n. It is called the Alternating Group on n elements, written A_n. In short, $A_n \lhd S_n$.
- A key step in showing the quintic unsolvable will be to show that A_5 is simple. There are many ways to do this, none entirely simple.
- Our proof, adapted from Rotman's book, will count various sets of even permutations, and then show that only two possibilities, corresponding to trivial subgroups can possibly be normal.
- To begin, note that the determinant map splits S_5 into 2 cosets of equal size. Because S_5 has order 5!, A_5 will be half that, namely 60.

A_5 is Simple

- The 60 members of A_5, all even, can be organized as follows:

Cycle Structure	Number of Them	Type
(1)	1	Identity
(123)	20=(5x4x3)/3	3-cycle
(12)(34)	$15 = \frac{1}{2}(\frac{5x4}{2} X \frac{3x2}{2})$	pair of 2-cycles
(12345)	$24 = 5!/5$	5-cycle

A_5 is Simple

- The 60 members of A_5, all even, can be organized as follows:

Cycle Structure	Number of Them	Type
(1)	1	Identity
(123)	20=(5x4x3)/3	3-cycle
(12)(34)	$15 = \frac{1}{2}\left(\frac{5x4}{2} X \frac{3x2}{2}\right)$	pair of 2-cycles
(12345)	$24 = 5!/5$	5-cycle

- Step 1: Any normal subgroup of A_5 containing a single 3-cycle must contain all of the 3-cycles.
  Proof: Suppose $H \lhd A_5, (123) \in H$. Then its inverse, $(321) \in H$, because H is a group, and $(432)(321)(234) = (124) \in H$. Generalizing, any 3-cycle can have one of its numbers replaced by any other number via conjugating with a member of A_5. So if one 3-cycle is in H then all 20 of them are. QED.

A_5 is Simple

- Step 2: Any normal subgroup of A_5 containing a single pair of 2-cycles must contain all of the pairs of 2-cycles.

A_5 is Simple

- Step 2: Any normal subgroup of A_5 containing a single pair of 2-cycles must contain all of the pairs of 2-cycles.
- Proof: Suppose $H \triangleleft A_5, (12)(34) \in H$. Let $\alpha = (435) \in H$. A direct calculation shows that $\alpha(12)(34)\alpha^{-1} = (12)(54) \in H$. Generalizing, any pair of 2-cycles can have one of its numbers replaced by any other number by conjugation with a member of A_5. So if one pair of 2-cycles is in H then all 15 of them are. QED.

A_5 is Simple

- Step 2: Any normal subgroup of A_5 containing a single pair of 2-cycles must contain all of the pairs of 2-cycles.
- Proof: Suppose $H \lhd A_5, (12)(34) \in H$. Let $\alpha = (435) \in H$. A direct calculation shows that $\alpha(12)(34)\alpha^{-1} = (12)(54) \in H$. Generalizing, any pair of 2-cycles can have one of its numbers replaced by any other number by conjugation with a member of A_5. So if one pair of 2-cycles is in H then all 15 of them are. QED.
- Step 3: If any given 5-cycle is in $H \lhd A_5$, then half of the 5-cycles, a total of 12, or 24 of all of them, must also be in H.

A_5 is Simple

- Step 2: Any normal subgroup of A_5 containing a single pair of 2-cycles must contain all of the pairs of 2-cycles.
- Proof: Suppose $H \lhd A_5, (12)(34) \in H$. Let $\alpha = (435) \in H$. A direct calculation shows that $\alpha(12)(34)\alpha^{-1} = (12)(54) \in H$. Generalizing, any pair of 2-cycles can have one of its numbers replaced by any other number by conjugation with a member of A_5. So if one pair of 2-cycles is in H then all 15 of them are. QED.
- Step 3: If any given 5-cycle is in $H \lhd A_5$, then half of the 5-cycles, a total of 12, or 24 of all of them, must also be in H.
- Proof: We will show that the set of all 24 5-cycles splits into 2 equal sized sets, and that all the elements in each set are conjugates of one another.

A_5 is Simple

- Consider first (1 2 3 4 5), and let $\alpha = (123)$. We compute $\alpha(12345)\alpha^{-1} = (23145)$. In short, the first 3 entries of the permutation have been permuted, leaving the final 2 entries unchanged.

A_5 is Simple

- Consider first (1 2 3 4 5), and let $\alpha = (123)$. We compute $\alpha(12345)\alpha^{-1} = (23145)$. In short, the first 3 entries of the permutation have been permuted, leaving the final 2 entries unchanged.
- More generally, by applying this method to (1 2 3 4 5) and then to its inverse (5 4 3 2 1), we can generate all of these conjugates: (1 2 3 4 5), (2 3 1 4 5), (3 1 2 4 5), (1 3 4 2 5), (1 2 5 3 4), (5 4 3 2 1), (4 3 5 2 1), (3 5 4 2 1), (5 4 2 3 1), (5 2 4 3 1) and (5 4 1 3 2). We have a total of 12 members of A_5, all conjugate to one another.

A_5 is Simple

- Consider first (1 2 3 4 5), and let $\alpha = (123)$. We compute $\alpha(12345)\alpha^{-1} = (23145)$. In short, the first 3 entries of the permutation have been permuted, leaving the final 2 entries unchanged.
- More generally, by applying this method to (1 2 3 4 5) and then to its inverse (5 4 3 2 1), we can generate all of these conjugates: (1 2 3 4 5), (2 3 1 4 5), (3 1 2 4 5), (1 3 4 2 5), (1 2 5 3 4), (5 4 3 2 1), (4 3 5 2 1), (3 5 4 2 1), (5 4 2 3 1), (5 2 4 3 1) and (5 4 1 3 2). We have a total of 12 members of A_5, all conjugate to one another.
- We are still missing (1 2 3 5 4), but if we apply the same methods to it and its inverse we will get the other 12 of the 5-cycles in A_5.

A_5 is Simple

- Now we can complete the simplicity proof. A_5 has been broken into 5 disjoint sets, of sizes 1, 20, 15, 12 and 12. Each of these sets, if it is to be in a normal subgroup of A_5 must be wholly in it. The self conjugate nature of each set says that no partial membership is allowed. But if a subgroup is to be assembled from these sets, it must have order that divides 60 (Lagrange). In addition, it will always include the subgroup of size 1, for it contains the identity.

A_5 is Simple

- Now we can complete the simplicity proof. A_5 has been broken into 5 disjoint sets, of sizes 1, 20, 15, 12 and 12. Each of these sets, if it is to be in a normal subgroup of A_5 must be wholly in it. The self conjugate nature of each set says that no partial membership is allowed. But if a subgroup is to be assembled from these sets, it must have order that divides 60 (Lagrange). In addition, it will always include the subgroup of size 1, for it contains the identity.
- The only way to added the requisite numbers and have a size dividing 60 is to take only the first, or to take all. This means the only normal subgroups are the trivial ones.

A_5 is Simple

- Now we can complete the simplicity proof. A_5 has been broken into 5 disjoint sets, of sizes 1, 20, 15, 12 and 12. Each of these sets, if it is to be in a normal subgroup of A_5 must be wholly in it. The self conjugate nature of each set says that no partial membership is allowed. But if a subgroup is to be assembled from these sets, it must have order that divides 60 (Lagrange). In addition, it will always include the subgroup of size 1, for it contains the identity.
- The only way to added the requisite numbers and have a size dividing 60 is to take only the first, or to take all. This means the only normal subgroups are the trivial ones.
- A_5 **is simple.**