Subgroups and cosets

Daniel H. Luecking
MASC

November 1, 2023

Computing in our example groups

I hope everyone can now recognize, and compute in, the example groups covered in the last lecture.

Computing in our example groups

I hope everyone can now recognize, and compute in, the example groups covered in the last lecture. If I say, "in the group $\mathbb{Z}_9$ with addition mod 9, find $6+6$ and $6+6+6$." You should respond "$6+6=3$ and $(6+6)+6=3+6=0$."

Computing in our example groups

I hope everyone can now recognize, and compute in, the example groups covered in the last lecture. If I say, "in the group $\mathbb{Z}_9$ with addition mod 9, find $6+6$ and $6+6+6$." You should respond "$6+6=3$ and $(6+6)+6=3+6=0$."

Similarly, for $u(\mathbb{Z}_9)$ with multiplication mod 9 if asked for $4 \cdot 4$ and $4 \cdot 4 \cdot 4$ you should be able to find $4 \cdot 4 = 16 \bmod 9 = 7$ and $(4 \cdot 4) \cdot 4 = 7 \cdot 4 = 28 \bmod 9 = 1$.

Computing in our example groups

I hope everyone can now recognize, and compute in, the example groups covered in the last lecture. If I say, "in the group $\mathbb{Z}_9$ with addition mod 9, find $6+6$ and $6+6+6$." You should respond "$6+6=3$ and $(6+6)+6=3+6=0$."

Similarly, for $u(\mathbb{Z}_9)$ with multiplication mod 9 if asked for $4\cdot 4$ and $4\cdot 4\cdot 4$ you should be able to find $4\cdot 4 = 16 \bmod 9 = 7$ and $(4\cdot 4)\cdot 4 = 7\cdot 4 = 28 \bmod 9 = 1$.

Finally, for the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ you should be able to find

$$\alpha\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \text{ and } \alpha\alpha\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Computing in our example groups

I hope everyone can now recognize, and compute in, the example groups covered in the last lecture. If I say, "in the group $\mathbb{Z}_9$ with addition mod 9, find $6+6$ and $6+6+6$." You should respond "$6+6=3$ and $(6+6)+6=3+6=0$."

Similarly, for $u(\mathbb{Z}_9)$ with multiplication mod 9 if asked for $4\cdot 4$ and $4\cdot 4\cdot 4$ you should be able to find $4\cdot 4=16 \bmod 9=7$ and $(4\cdot 4)\cdot 4=7\cdot 4=28 \bmod 9=1$.

Finally, for the permutation $\alpha=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$ you should be able to find

$$\alpha\alpha=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} \text{ and } \alpha\alpha\alpha=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

Note that in all these cases, repeating the operation on a single element eventually produced the identity of that group.

Computing in our example groups

I hope everyone can now recognize, and compute in, the example groups covered in the last lecture. If I say, "in the group $\mathbb{Z}_9$ with addition mod 9, find $6+6$ and $6+6+6$." You should respond "$6+6=3$ and $(6+6)+6=3+6=0$."

Similarly, for $u(\mathbb{Z}_9)$ with multiplication mod 9 if asked for $4 \cdot 4$ and $4 \cdot 4 \cdot 4$ you should be able to find $4 \cdot 4 = 16 \bmod 9 = 7$ and $(4 \cdot 4) \cdot 4 = 7 \cdot 4 = 28 \bmod 9 = 1$.

Finally, for the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ you should be able to find

$$\alpha\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \text{ and } \alpha\alpha\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Note that in all these cases, repeating the operation on a single element eventually produced the identity of that group. This is not an accident.

Subgroups

When we speak of a group G with an operation $*$, we may write "the group $(G, *)$". The point is that you need both the set and the operation and this notation tells you both.

Subgroups

When we speak of a group G with an operation $*$, we may write "the group $(G, *)$". The point is that you need both the set and the operation and this notation tells you both. Thus the groups $(\mathbb{Z}_9, +)$ and $(u(\mathbb{Z}_9), \cdot)$ were discussed on the previous page.

Subgroups

When we speak of a group G with an operation $*$, we may write "the group $(G, *)$". The point is that you need both the set and the operation and this notation tells you both. Thus the groups $(\mathbb{Z}_9, +)$ and $(u(\mathbb{Z}_9), \cdot)$ were discussed on the previous page. If the operation has already been specified or is understood from context, we just say "the group G."

Subgroups

When we speak of a group G with an operation $*$, we may write "the group $(G, *)$". The point is that you need both the set and the operation and this notation tells you both. Thus the groups $(\mathbb{Z}_9, +)$ and $(u(\mathbb{Z}_9), \cdot)$ were discussed on the previous page. If the operation has already been specified or is understood from context, we just say "the group G."

We define a *subgroup* of a group $(G, *)$ to be a nonempty subset H of G which is a group using the same operation $*$.

Subgroups

When we speak of a group G with an operation $*$, we may write "the group $(G, *)$". The point is that you need both the set and the operation and this notation tells you both. Thus the groups $(\mathbb{Z}_9, +)$ and $(u(\mathbb{Z}_9), \cdot)$ were discussed on the previous page. If the operation has already been specified or is understood from context, we just say "the group G."

We define a *subgroup* of a group $(G, *)$ to be a nonempty subset H of G which is a group using the same operation $*$. Notice that in G we already have an identity element as well as inverses. For H to be a subgroup the identity must be in H and the inverse of any element in H must be in H.

Subgroups

When we speak of a group G with an operation $*$, we may write "the group $(G, *)$". The point is that you need both the set and the operation and this notation tells you both. Thus the groups $(\mathbb{Z}_9, +)$ and $(u(\mathbb{Z}_9), \cdot)$ were discussed on the previous page. If the operation has already been specified or is understood from context, we just say "the group G."

We define a *subgroup* of a group $(G, *)$ to be a nonempty subset H of G which is a group using the same operation $*$. Notice that in G we already have an identity element as well as inverses. For H to be a subgroup the identity must be in H and the inverse of any element in H must be in H. But the most important condition is the first one in the definition of a group: if a and b are in H then $a * b$ must be in H.

Subgroups

When we speak of a group G with an operation $*$, we may write "the group $(G, *)$". The point is that you need both the set and the operation and this notation tells you both. Thus the groups $(\mathbb{Z}_9, +)$ and $(u(\mathbb{Z}_9), \cdot)$ were discussed on the previous page. If the operation has already been specified or is understood from context, we just say "the group G."

We define a *subgroup* of a group $(G, *)$ to be a nonempty subset H of G which is a group using the same operation $*$. Notice that in G we already have an identity element as well as inverses. For H to be a subgroup the identity must be in H and the inverse of any element in H must be in H. But the most important condition is the first one in the definition of a group: if a and b are in H then $a * b$ must be in H.

The second condition in the definition of group (associativity) will automatically be satisfied for H since it is purely a property of the operation and doesn't care whether the elements come are in the subset H.

Conditions for a subset to be a subgroup

We only have to check two conditions to see if a subset H of a group $(G, *)$ is a subgroup:

Theorem

If $(G, *)$ is a group and H is a nonempty subset, then H is a subgroup if and only if H satisfies the two conditions:

Conditions for a subset to be a subgroup

We only have to check two conditions to see if a subset H of a group $(G, *)$ is a subgroup:

Theorem

If $(G, *)$ is a group and H is a nonempty subset, then H is a subgroup if and only if H satisfies the two conditions:

- *For any a, b in H, $a * b$ is in H*

Conditions for a subset to be a subgroup

We only have to check two conditions to see if a subset H of a group $(G, *)$ is a subgroup:

Theorem

If $(G, *)$ is a group and H is a nonempty subset, then H is a subgroup if and only if H satisfies the two conditions:

- *For any a, b in H, $a * b$ is in H*
- *For any a in H, the inverse of a is in H.*

Moreover, if H is finite, the second condition follows from the first, so we only have to check closure.

Conditions for a subset to be a subgroup

We only have to check two conditions to see if a subset H of a group $(G, *)$ is a subgroup:

Theorem

If $(G, *)$ is a group and H is a nonempty subset, then H is a subgroup if and only if H satisfies the two conditions:

- *For any a, b in H, $a * b$ is in H*
- *For any a in H, the inverse of a is in H.*

Moreover, if H is finite, the second condition follows from the first, so we only have to check closure.

These are the first and last of the four parts of the definition of a group. The middle two parts of the definition (associativity and existence of an identity) follow from G being a group and the above conditions.

Conditions for a subset to be a subgroup

We only have to check two conditions to see if a subset H of a group $(G, *)$ is a subgroup:

Theorem

If $(G, *)$ is a group and H is a nonempty subset, then H is a subgroup if and only if H satisfies the two conditions:

- *For any a, b in H, $a * b$ is in H*
- *For any a in H, the inverse of a is in H.*

Moreover, if H is finite, the second condition follows from the first, so we only have to check closure.

These are the first and last of the four parts of the definition of a group. The middle two parts of the definition (associativity and existence of an identity) follow from G being a group and the above conditions. The identity is $a * a^{-1}$ which must belong to H if the above two conditions hold.

Examples of subgroups

- $\{1, 4, 7\}$ is a subgroup of $u(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$

Examples of subgroups

- $\{1, 4, 7\}$ is a subgroup of $u(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$
- $\{0, 3, 6\}$ is a subgroup of $\mathbb{Z}_9$.

Examples of subgroups

- $\{1, 4, 7\}$ is a subgroup of $u(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$
- $\{0, 3, 6\}$ is a subgroup of $\mathbb{Z}_9$.
- $\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\}$ is a subgroup of S_4.

Examples of subgroups

- $\{1, 4, 7\}$ is a subgroup of $u(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$
- $\{0, 3, 6\}$ is a subgroup of $\mathbb{Z}_9$.
- $\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\}$ is a subgroup of S_4.

For the first of these we need to check six possible products: $4 \cdot 4 = 7$, $4 \cdot 7 = 1$, $7 \cdot 7 = 4$ (plus three more).

Examples of subgroups

- $\{1, 4, 7\}$ is a subgroup of $u(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$
- $\{0, 3, 6\}$ is a subgroup of $\mathbb{Z}_9$.
- $\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\}$ is a subgroup of S_4.

For the first of these we need to check six possible products: $4 \cdot 4 = 7$, $4 \cdot 7 = 1$, $7 \cdot 7 = 4$ (plus three more).

For the second one: $3 + 3 = 6$, $3 + 6 = 0$, $6 + 6 = 3$ (plus three more).

Examples of subgroups

- $\{1, 4, 7\}$ is a subgroup of $u(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$
- $\{0, 3, 6\}$ is a subgroup of $\mathbb{Z}_9$.
- $\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\}$ is a subgroup of S_4.

For the first of these we need to check six possible products: $4 \cdot 4 = 7$, $4 \cdot 7 = 1$, $7 \cdot 7 = 4$ (plus three more).

For the second one: $3 + 3 = 6$, $3 + 6 = 0$, $6 + 6 = 3$ (plus three more).

For the third example, these are the identity permutation id, plus α and $\alpha\alpha$ from earlier. We have already computed $\alpha(\alpha\alpha) = \mathrm{id}$. Moreover, $(\alpha\alpha)(\alpha\alpha) = (\alpha(\alpha\alpha))\alpha = \mathrm{id}\,\alpha = \alpha$, etc.

Powers in groups

If we have any group $(G, \cdot)$ (I'll use multiplication notation for simplicity) and any element a in G, we can abbreviate $a \cdot a$ by a^2 and $a \cdot a \cdot a$ by a^3, etc.

Powers in groups

If we have any group $(G, \cdot)$ (I'll use multiplication notation for simplicity) and any element a in G, we can abbreviate $a \cdot a$ by a^2 and $a \cdot a \cdot a$ by a^3, etc. Similarly, a^{-1} is the inverse of a, $a^{-2} = a^{-1} \cdot a^{-1}$ is the inverse of a^2 and $a^{-3} = a^{-1} \cdot a^{-1} \cdot a^{-1}$ is the inverse of a^3, etc.

Powers in groups

If we have any group $(G, \cdot)$ (I'll use multiplication notation for simplicity) and any element a in G, we can abbreviate $a \cdot a$ by a^2 and $a \cdot a \cdot a$ by a^3, etc. Similarly, a^{-1} is the inverse of a, $a^{-2} = a^{-1} \cdot a^{-1}$ is the inverse of a^2 and $a^{-3} = a^{-1} \cdot a^{-1} \cdot a^{-1}$ is the inverse of a^3, etc.

[If the operation is '$+$', it is more traditional to write repeated operations as follows: $a + a = 2a$, $a + a + a = 3a$.

Powers in groups

If we have any group $(G, \cdot)$ (I'll use multiplication notation for simplicity) and any element a in G, we can abbreviate $a \cdot a$ by a^2 and $a \cdot a \cdot a$ by a^3, etc. Similarly, a^{-1} is the inverse of a, $a^{-2} = a^{-1} \cdot a^{-1}$ is the inverse of a^2 and $a^{-3} = a^{-1} \cdot a^{-1} \cdot a^{-1}$ is the inverse of a^3, etc.

[If the operation is '$+$', it is more traditional to write repeated operations as follows: $a + a = 2a$, $a + a + a = 3a$. In this case the inverse of a would be written $-a$. Then $-3a$, for example, would mean $-a + -a + -a$ which is also the inverse of $3a$.]

Powers in groups

If we have any group $(G, \cdot)$ (I'll use multiplication notation for simplicity) and any element a in G, we can abbreviate $a \cdot a$ by a^2 and $a \cdot a \cdot a$ by a^3, etc. Similarly, a^{-1} is the inverse of a, $a^{-2} = a^{-1} \cdot a^{-1}$ is the inverse of a^2 and $a^{-3} = a^{-1} \cdot a^{-1} \cdot a^{-1}$ is the inverse of a^3, etc.

[If the operation is '$+$', it is more traditional to write repeated operations as follows: $a + a = 2a$, $a + a + a = 3a$. In this case the inverse of a would be written $-a$. Then $-3a$, for example, would mean $-a + -a + -a$ which is also the inverse of $3a$.]

Because of the regrouping property, $a \cdot a \cdot a$ is not ambiguous because both possible interpretations $(a \cdot a) \cdot a$ and $a \cdot (a \cdot a)$ must be equal. The same is true of all powers.

Cyclic groups and subgroups

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k.

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k. For this to be consistent, we have to define a^0 to be the identity element e and $a^1 = a$.

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k. For this to be consistent, we have to define a^0 to be the identity element e and $a^1 = a$. [For additive groups we have $na + ka = (n+k)a$, $0a$ is the identity (usually called 0) and $1a = a$.]

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k. For this to be consistent, we have to define a^0 to be the identity element e and $a^1 = a$. [For additive groups we have $na + ka = (n+k)a$, $0a$ is the identity (usually called 0) and $1a = a$.]

If $(G, \cdot)$ is a finite group with n elements, and we start with an element a, then the $n+1$ elements $a^0, a^1, a^2, a^3, \cdots, a^n$ cannot all be different.

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k. For this to be consistent, we have to define a^0 to be the identity element e and $a^1 = a$. [For additive groups we have $na + ka = (n+k)a$, $0a$ is the identity (usually called 0) and $1a = a$.]

If $(G, \cdot)$ is a finite group with n elements, and we start with an element a, then the $n+1$ elements $a^0, a^1, a^2, a^3, \cdots, a^n$ cannot all be different. So at some point a^m equals some previous element a^j. Then we can operate by a^{-j} on both sides of $a^m = a^j$ to get $a^{m-j} = e = a^0$.

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k. For this to be consistent, we have to define a^0 to be the identity element e and $a^1 = a$. [For additive groups we have $na + ka = (n+k)a$, $0a$ is the identity (usually called 0) and $1a = a$.]

If $(G, \cdot)$ is a finite group with n elements, and we start with an element a, then the $n+1$ elements $a^0, a^1, a^2, a^3, \cdots, a^n$ cannot all be different. So at some point a^m equals some previous element a^j. Then we can operate by a^{-j} on both sides of $a^m = a^j$ to get $a^{m-j} = e = a^0$.

We conclude that if G is finite then successive powers of any element a eventually produce the identity, say $a^k = e$, and after that, previous powers are repeated.

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k. For this to be consistent, we have to define a^0 to be the identity element e and $a^1 = a$. [For additive groups we have $na + ka = (n+k)a$, $0a$ is the identity (usually called 0) and $1a = a$.]

If $(G, \cdot)$ is a finite group with n elements, and we start with an element a, then the $n+1$ elements $a^0, a^1, a^2, a^3, \cdots, a^n$ cannot all be different. So at some point a^m equals some previous element a^j. Then we can operate by a^{-j} on both sides of $a^m = a^j$ to get $a^{m-j} = e = a^0$.

We conclude that if G is finite then successive powers of any element a eventually produce the identity, say $a^k = e$, and after that, previous powers are repeated. That is, $a^{k+1} = a^k \cdot a = ea = a$. We'll see in a minute that $\{a, a^2, \ldots, a^k = e\}$ is a group.

Cyclic groups and subgroups

The basic property of this notation is that $a^n \cdot a^k = a^{n+k}$ and this holds regardless of the signs of the integers n and k. For this to be consistent, we have to define a^0 to be the identity element e and $a^1 = a$. [For additive groups we have $na + ka = (n+k)a$, $0a$ is the identity (usually called 0) and $1a = a$.]

If $(G, \cdot)$ is a finite group with n elements, and we start with an element a, then the $n+1$ elements $a^0, a^1, a^2, a^3, \cdots, a^n$ cannot all be different. So at some point a^m equals some previous element a^j. Then we can operate by a^{-j} on both sides of $a^m = a^j$ to get $a^{m-j} = e = a^0$.

We conclude that if G is finite then successive powers of any element a eventually produce the identity, say $a^k = e$, and after that, previous powers are repeated. That is, $a^{k+1} = a^k \cdot a = ea = a$. We'll see in a minute that $\{a, a^2, \ldots, a^k = e\}$ is a group. It is called the *cyclic subgroup generated by a* and is denoted $\langle a \rangle$.

Why is $\langle a \rangle$ a subgroup?

The first integer k for which $a^k = e$ is called the *order of a*. It also happens to be the order (i.e. size) of $\langle a \rangle$.

Why is $\langle a \rangle$ a subgroup?

The first integer k for which $a^k = e$ is called the *order of a*. It also happens to be the order (i.e. size) of $\langle a \rangle$.

Note that if $m = qk$ then a^{qk} is a product of qk a's. These can be grouped into a product of q repetitions of a^k.

Why is $\langle a \rangle$ a subgroup?

The first integer k for which $a^k = e$ is called the *order of a*. It also happens to be the order (i.e. size) of $\langle a \rangle$.

Note that if $m = qk$ then a^{qk} is a product of qk a's. These can be grouped into a product of q repetitions of a^k. That is, $a^{qk} = (a^k)^q$. If $a^k = e$ then $a^{qk} = e^q = e$. Therefore, if $m = qk + r$ then $a^m = a^{qk}a^r = ea^r = a^r$.

Why is $\langle a \rangle$ a subgroup?

The first integer k for which $a^k = e$ is called the *order of a*. It also happens to be the order (i.e. size) of $\langle a \rangle$.

Note that if $m = qk$ then a^{qk} is a product of qk a's. These can be grouped into a product of q repetitions of a^k. That is, $a^{qk} = (a^k)^q$. If $a^k = e$ then $a^{qk} = e^q = e$. Therefore, if $m = qk + r$ then $a^m = a^{qk}a^r = ea^r = a^r$. That is, if k is the order of a, then $a^m = a^{m \bmod k}$.

To see that $\langle a \rangle$ is a group we only have to show every element has an inverse and that it is closed under the operation.

Why is $\langle a \rangle$ a subgroup?

The first integer k for which $a^k = e$ is called the *order of a*. It also happens to be the order (i.e. size) of $\langle a \rangle$.

Note that if $m = qk$ then a^{qk} is a product of qk a's. These can be grouped into a product of q repetitions of a^k. That is, $a^{qk} = (a^k)^q$. If $a^k = e$ then $a^{qk} = e^q = e$. Therefore, if $m = qk + r$ then $a^m = a^{qk}a^r = ea^r = a^r$. That is, if k is the order of a, then $a^m = a^{m \bmod k}$.

To see that $\langle a \rangle$ is a group we only have to show every element has an inverse and that it is closed under the operation. To see the first note that $a^j \cdot a^{k-j} = a^k = e$ if k is the order of a. Thus every a^j has an inverse which is also in $\langle a \rangle$.

Why is $\langle a \rangle$ a subgroup?

The first integer k for which $a^k = e$ is called the *order of a*. It also happens to be the order (i.e. size) of $\langle a \rangle$.

Note that if $m = qk$ then a^{qk} is a product of qk a's. These can be grouped into a product of q repetitions of a^k. That is, $a^{qk} = (a^k)^q$. If $a^k = e$ then $a^{qk} = e^q = e$. Therefore, if $m = qk + r$ then $a^m = a^{qk}a^r = ea^r = a^r$. That is, if k is the order of a, then $a^m = a^{m \bmod k}$.

To see that $\langle a \rangle$ is a group we only have to show every element has an inverse and that it is closed under the operation. To see the first note that $a^j \cdot a^{k-j} = a^k = e$ if k is the order of a. Thus every a^j has an inverse which is also in $\langle a \rangle$. To see closure, note that $a^j \cdot a^m = a^{(j+m) \bmod k}$, which is also in $\langle a \rangle$.

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6 \rangle = \{6, 6+6=3, 3+6=0\}$.

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6 \rangle = \{6, 6+6=3, 3+6=0\}$. Note that $\mathbb{Z}_9$ is itself cyclic, being equal to $\langle 1 \rangle$. This happens for every $(\mathbb{Z}_n, +)$.

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6 \rangle = \{6, 6+6=3, 3+6=0\}$. Note that $\mathbb{Z}_9$ is itself cyclic, being equal to $\langle 1 \rangle$. This happens for every $(\mathbb{Z}_n, +)$.

For $u(Z_9)$, 4 has order 3 and $\langle 4 \rangle = \{4, 4 \cdot 4 = 7, 7 \cdot 4 = 1\}$.

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6 \rangle = \{6, 6+6=3, 3+6=0\}$. Note that $\mathbb{Z}_9$ is itself cyclic, being equal to $\langle 1 \rangle$. This happens for every $(\mathbb{Z}_n, +)$.

For $u(Z_9)$, 4 has order 3 and $\langle 4 \rangle = \{4, 4 \cdot 4 = 7, 7 \cdot 4 = 1\}$. The element 2 has order 6. The element 8 has order 2.

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6 \rangle = \{6, 6+6=3, 3+6=0\}$. Note that $\mathbb{Z}_9$ is itself cyclic, being equal to $\langle 1 \rangle$. This happens for every $(\mathbb{Z}_n, +)$.

For $u(Z_9)$, 4 has order 3 and $\langle 4 \rangle = \{4, 4 \cdot 4 = 7, 7 \cdot 4 = 1\}$. The element 2 has order 6. The element 8 has order 2.

For S_4, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ has order 3 and

$$\langle \alpha \rangle = \left\{ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}$$

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6\rangle = \{6, 6+6=3, 3+6=0\}$. Note that $\mathbb{Z}_9$ is itself cyclic, being equal to $\langle 1\rangle$. This happens for every $(\mathbb{Z}_n, +)$.

For $u(Z_9)$, 4 has order 3 and $\langle 4\rangle = \{4, 4\cdot 4 = 7, 7\cdot 4 = 1\}$. The element 2 has order 6. The element 8 has order 2.

For S_4, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ has order 3 and

$$\langle \alpha \rangle = \left\{ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}$$

Some more examples along the same lines:
In $(\mathbb{Z}_{15}, +)$, 3 has order 5 and $\langle 3\rangle = \{3, 6, 9, 12, 0\}$.

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6 \rangle = \{6, 6+6=3, 3+6=0\}$. Note that $\mathbb{Z}_9$ is itself cyclic, being equal to $\langle 1 \rangle$. This happens for every $(\mathbb{Z}_n, +)$.

For $u(Z_9)$, 4 has order 3 and $\langle 4 \rangle = \{4, 4 \cdot 4 = 7, 7 \cdot 4 = 1\}$. The element 2 has order 6. The element 8 has order 2.

For S_4, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ has order 3 and

$$\langle \alpha \rangle = \left\{ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}$$

Some more examples along the same lines:
In $(\mathbb{Z}_{15}, +)$, 3 has order 5 and $\langle 3 \rangle = \{3, 6, 9, 12, 0\}$.

In $(u(\mathbb{Z}_{16}), \cdot)$, 5 has order 4 and $\langle 5 \rangle = \{5, 9, 13, 1\}$.

Examples of cyclic subgroups

For the group $\mathbb{Z}_9$, 6 has order 3 and $\langle 6 \rangle = \{6, 6+6=3, 3+6=0\}$. Note that $\mathbb{Z}_9$ is itself cyclic, being equal to $\langle 1 \rangle$. This happens for every $(\mathbb{Z}_n, +)$.

For $u(Z_9)$, 4 has order 3 and $\langle 4 \rangle = \{4, 4 \cdot 4 = 7, 7 \cdot 4 = 1\}$. The element 2 has order 6. The element 8 has order 2.

For S_4, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ has order 3 and

$$\langle \alpha \rangle = \left\{ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}$$

Some more examples along the same lines:
In $(\mathbb{Z}_{15}, +)$, 3 has order 5 and $\langle 3 \rangle = \{3, 6, 9, 12, 0\}$.

In $(u(\mathbb{Z}_{16}), \cdot)$, 5 has order 4 and $\langle 5 \rangle = \{5, 9, 13, 1\}$.

In S_5, $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ has order 4 and

$$\langle \gamma \rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\}$$

Cosets of a subgroup

Definition: If $(G, \cdot)$ is a group and H is any subgroup of G, and a is any element of G then $a \cdot H$ means the set of all products $a \cdot h$ for $h \in H$.

Cosets of a subgroup

Definition: If $(G, \cdot)$ is a group and H is any subgroup of G, and a is any element of G then $a \cdot H$ means the set of all products $a \cdot h$ for $h \in H$. This set $a \cdot H$ is called a *left coset of H*.

Cosets of a subgroup

Definition: If $(G, \cdot)$ is a group and H is any subgroup of G, and a is any element of G then $a \cdot H$ means the set of all products $a \cdot h$ for $h \in H$. This set $a \cdot H$ is called a *left coset of H*.

$H \cdot a$ would be defined similarly and called a *right coset of H*. If the operation is addition, cosets would be written $a + H$.

Cosets of a subgroup

Definition: If $(G, \cdot)$ is a group and H is any subgroup of G, and a is any element of G then $a \cdot H$ means the set of all products $a \cdot h$ for $h \in H$. This set $a \cdot H$ is called a *left coset of H*.

$H \cdot a$ would be defined similarly and called a *right coset of H*. If the operation is addition, cosets would be written $a + H$. The properties of left and right cosets are essentially the same, so I will deal only with left cosets and just say "cosets".

Consider the group $(\mathbb{Z}_{12}, +)$ and the subgroup $H = \langle 3 \rangle = \{0, 3, 6, 9\}$.

Cosets of a subgroup

Definition: If $(G, \cdot)$ is a group and H is any subgroup of G, and a is any element of G then $a \cdot H$ means the set of all products $a \cdot h$ for $h \in H$. This set $a \cdot H$ is called a *left coset of H*.

$H \cdot a$ would be defined similarly and called a *right coset of H*. If the operation is addition, cosets would be written $a + H$. The properties of left and right cosets are essentially the same, so I will deal only with left cosets and just say "cosets".

Consider the group $(\mathbb{Z}_{12}, +)$ and the subgroup $H = \langle 3 \rangle = \{0, 3, 6, 9\}$. Then $2 + H = \{2, 5, 8, 11\}$ is one of the cosets of H. Note that $2 + H$ is the same set as $5 + H$ (check this).

Cosets of a subgroup

Definition: If $(G, \cdot)$ is a group and H is any subgroup of G, and a is any element of G then $a \cdot H$ means the set of all products $a \cdot h$ for $h \in H$. This set $a \cdot H$ is called a *left coset of H*.

$H \cdot a$ would be defined similarly and called a *right coset of H*. If the operation is addition, cosets would be written $a + H$. The properties of left and right cosets are essentially the same, so I will deal only with left cosets and just say "cosets".

Consider the group $(\mathbb{Z}_{12}, +)$ and the subgroup $H = \langle 3 \rangle = \{0, 3, 6, 9\}$. Then $2 + H = \{2, 5, 8, 11\}$ is one of the cosets of H. Note that $2 + H$ is the same set as $5 + H$ (check this). In the table on the next page, all possible distinct cosets of H are shown

Properties of cosets

Cosets of the subgroup $H = \{0, 3, 6, 9\}$ in $\mathbb{Z}_{12}$:

$$\begin{aligned} H = 0 + H &= \{0, 3, 6, 9\} \\ 1 + H &= \{1, 4, 7, 10\} \\ 2 + H &= \{2, 5, 8, 11\} \end{aligned}$$

Properties of cosets

Cosets of the subgroup $H = \{0, 3, 6, 9\}$ in $\mathbb{Z}_{12}$:

$$\begin{aligned} H = 0 + H &= \{0, 3, 6, 9\} \\ 1 + H &= \{1, 4, 7, 10\} \\ 2 + H &= \{2, 5, 8, 11\} \end{aligned}$$

These repeat for other additions: $3 + H = 0 + H$, $4 + H = 1 + H$, and so on. This sort of thing happens for every subgroup of any group.

Properties of cosets

Cosets of the subgroup $H = \{0, 3, 6, 9\}$ in $\mathbb{Z}_{12}$:

$$\begin{aligned} H = 0 + H &= \{0, 3, 6, 9\} \\ 1 + H &= \{1, 4, 7, 10\} \\ 2 + H &= \{2, 5, 8, 11\} \end{aligned}$$

These repeat for other additions: $3 + H = 0 + H$, $4 + H = 1 + H$, and so on. This sort of thing happens for every subgroup of any group.

Theorem

- *Two cosets $a \cdot H$ and $b \cdot H$ are equal if $b^{-1} \cdot a$ belongs to H and otherwise are disjoint.*

Properties of cosets

Cosets of the subgroup $H = \{0, 3, 6, 9\}$ in $\mathbb{Z}_{12}$:

$$\begin{aligned} H = 0 + H &= \{0, 3, 6, 9\} \\ 1 + H &= \{1, 4, 7, 10\} \\ 2 + H &= \{2, 5, 8, 11\} \end{aligned}$$

These repeat for other additions: $3 + H = 0 + H$, $4 + H = 1 + H$, and so on. This sort of thing happens for every subgroup of any group.

Theorem

- *Two cosets $a \cdot H$ and $b \cdot H$ are equal if $b^{-1} \cdot a$ belongs to H and otherwise are disjoint.*
- *The size of each coset is the same as the size of H: $|a \cdot H| = |H|$*

Properties of cosets

Cosets of the subgroup $H = \{0, 3, 6, 9\}$ in $\mathbb{Z}_{12}$:

$$\begin{aligned} H = 0 + H &= \{0, 3, 6, 9\} \\ 1 + H &= \{1, 4, 7, 10\} \\ 2 + H &= \{2, 5, 8, 11\} \end{aligned}$$

These repeat for other additions: $3 + H = 0 + H$, $4 + H = 1 + H$, and so on. This sort of thing happens for every subgroup of any group.

Theorem

- *Two cosets $a \cdot H$ and $b \cdot H$ are equal if $b^{-1} \cdot a$ belongs to H and otherwise are disjoint.*
- *The size of each coset is the same as the size of H: $|a \cdot H| = |H|$*
- *Every element of G is in one of the cosets of H. In fact a belongs to $a \cdot H$ because H contains the identity e, and so $a \cdot e$ belongs to $a \cdot H$.*

Lagrange's Theorem

The since all cosets are disjoint, and together make up all of G it follows that $|G|$ is the sum of the sizes of the cosets.

Lagrange's Theorem

The since all cosets are disjoint, and together make up all of G it follows that $|G|$ is the sum of the sizes of the cosets. Since the cosets are all the size of H, that sum is just the product of the number of cosets times the size of H.

Lagrange's Theorem

The since all cosets are disjoint, and together make up all of G it follows that $|G|$ is the sum of the sizes of the cosets. Since the cosets are all the size of H, that sum is just the product of the number of cosets times the size of H. For example, we considered $\mathbb{Z}_{12}$ earlier. A certain subgroup had 3 cosets, each of size 4.

Lagrange's Theorem

The since all cosets are disjoint, and together make up all of G it follows that $|G|$ is the sum of the sizes of the cosets. Since the cosets are all the size of H, that sum is just the product of the number of cosets times the size of H. For example, we considered $\mathbb{Z}_{12}$ earlier. A certain subgroup had 3 cosets, each of size 4.

These ideas lead to the following theorem:

Theorem (Lagrange's Theorem)

If H is a subgroup of G, then $|H|$ evenly divides $|G|$ and the number of cosets of H is $|G|/|H|$.

Lagrange's Theorem

The since all cosets are disjoint, and together make up all of G it follows that $|G|$ is the sum of the sizes of the cosets. Since the cosets are all the size of H, that sum is just the product of the number of cosets times the size of H. For example, we considered $\mathbb{Z}_{12}$ earlier. A certain subgroup had 3 cosets, each of size 4.

These ideas lead to the following theorem:

Theorem (Lagrange's Theorem)

If H is a subgroup of G, then $|H|$ evenly divides $|G|$ and the number of cosets of H is $|G|/|H|$.

We can apply Lagrange's Theorem to the subgroup $H = \langle a \rangle$.

Lagrange's Theorem

The since all cosets are disjoint, and together make up all of G it follows that $|G|$ is the sum of the sizes of the cosets. Since the cosets are all the size of H, that sum is just the product of the number of cosets times the size of H. For example, we considered $\mathbb{Z}_{12}$ earlier. A certain subgroup had 3 cosets, each of size 4.

These ideas lead to the following theorem:

Theorem (Lagrange's Theorem)

If H is a subgroup of G, then $|H|$ evenly divides $|G|$ and the number of cosets of H is $|G|/|H|$.

We can apply Lagrange's Theorem to the subgroup $H = \langle a \rangle$. Suppose $|H| = k$ and $|G| = n$, then $n/k = q$ is an integer. Since $a^k = e$ it follows from earlier that $a^n = a^{qk} = e$.

Lagrange's Theorem

The since all cosets are disjoint, and together make up all of G it follows that $|G|$ is the sum of the sizes of the cosets. Since the cosets are all the size of H, that sum is just the product of the number of cosets times the size of H. For example, we considered $\mathbb{Z}_{12}$ earlier. A certain subgroup had 3 cosets, each of size 4.

These ideas lead to the following theorem:

Theorem (Lagrange's Theorem)

If H is a subgroup of G, then $|H|$ evenly divides $|G|$ and the number of cosets of H is $|G|/|H|$.

We can apply Lagrange's Theorem to the subgroup $H = \langle a \rangle$. Suppose $|H| = k$ and $|G| = n$, then $n/k = q$ is an integer. Since $a^k = e$ it follows from earlier that $a^n = a^{qk} = e$. That is,

$$\text{for any } a \text{ in } G,\ a^{|G|} = e$$

Examples

We can check Lagrange's Theorem against our previous examples. The group $(\mathbb{Z}_9, +)$ has order 9 and the subgroup $H = \langle 6 \rangle$ has order 3, so the number of cosets will be $9/3 = 3$.

Examples

We can check Lagrange's Theorem against our previous examples. The group $(\mathbb{Z}_9, +)$ has order 9 and the subgroup $H = \langle 6 \rangle$ has order 3, so the number of cosets will be $9/3 = 3$.

The group $(u(\mathbb{Z}_9), \cdot)$ has order $\phi(9) = 6$ and the subgroup $H = \langle 4 \rangle$ has order 3, so the number of cosets will be $6/3 = 2$.

Examples

We can check Lagrange's Theorem against our previous examples. The group $(\mathbb{Z}_9, +)$ has order 9 and the subgroup $H = \langle 6 \rangle$ has order 3, so the number of cosets will be $9/3 = 3$.

The group $(u(\mathbb{Z}_9), \cdot)$ has order $\phi(9) = 6$ and the subgroup $H = \langle 4 \rangle$ has order 3, so the number of cosets will be $6/3 = 2$.

The group S_4 has order $4! = 24$ and the subgroup $\langle \alpha \rangle$, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ from before, has order 3, so it has $24/3 = 8$ cosets.

Examples

We can check Lagrange's Theorem against our previous examples. The group $(\mathbb{Z}_9, +)$ has order 9 and the subgroup $H = \langle 6 \rangle$ has order 3, so the number of cosets will be $9/3 = 3$.

The group $(u(\mathbb{Z}_9), \cdot)$ has order $\phi(9) = 6$ and the subgroup $H = \langle 4 \rangle$ has order 3, so the number of cosets will be $6/3 = 2$.

The group S_4 has order $4! = 24$ and the subgroup $\langle \alpha \rangle$, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ from before, has order 3, so it has $24/3 = 8$ cosets.

The group $(\mathbb{Z}_{15}, +)$ has order 15 and the subgroup $\langle 3 \rangle$ has order 5, so there are $15/5 = 3$ cosets.

Examples

We can check Lagrange's Theorem against our previous examples. The group $(\mathbb{Z}_9, +)$ has order 9 and the subgroup $H = \langle 6 \rangle$ has order 3, so the number of cosets will be $9/3 = 3$.

The group $(u(\mathbb{Z}_9), \cdot)$ has order $\phi(9) = 6$ and the subgroup $H = \langle 4 \rangle$ has order 3, so the number of cosets will be $6/3 = 2$.

The group S_4 has order $4! = 24$ and the subgroup $\langle \alpha \rangle$, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ from before, has order 3, so it has $24/3 = 8$ cosets.

The group $(\mathbb{Z}_{15}, +)$ has order 15 and the subgroup $\langle 3 \rangle$ has order 5, so there are $15/5 = 3$ cosets.

The group $(u(\mathbb{Z}_{16}), \cdot)$ has order $\phi(16) = 8$ and the subgroup $\langle 5 \rangle$ has order 4, so there are $8/4 = 2$ cosets.

Examples

We can check Lagrange's Theorem against our previous examples. The group $(\mathbb{Z}_9, +)$ has order 9 and the subgroup $H = \langle 6 \rangle$ has order 3, so the number of cosets will be $9/3 = 3$.

The group $(u(\mathbb{Z}_9), \cdot)$ has order $\phi(9) = 6$ and the subgroup $H = \langle 4 \rangle$ has order 3, so the number of cosets will be $6/3 = 2$.

The group S_4 has order $4! = 24$ and the subgroup $\langle \alpha \rangle$, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ from before, has order 3, so it has $24/3 = 8$ cosets.

The group $(\mathbb{Z}_{15}, +)$ has order 15 and the subgroup $\langle 3 \rangle$ has order 5, so there are $15/5 = 3$ cosets.

The group $(u(\mathbb{Z}_{16}), \cdot)$ has order $\phi(16) = 8$ and the subgroup $\langle 5 \rangle$ has order 4, so there are $8/4 = 2$ cosets.

Lagrange's Theorem puts limits on the possible subgroups. For example, $(u(\mathbb{Z}_{16}), \cdot)$ cannot have any subgroups with size 3 or 5. The only possible sizes are factors of 8: $1, 2, 4, 8$.