10/22/15

HW3 due next Tues.
Midterm Exam next Thurs.

HW2 Stats:

Total	35
Average	29
Median	28.5
St. Dev.	3.7

Having proved the Abel-Ruffini Theorem, we will now shift gears. Recall that I originally gave two definitions of a group.

(1) A structure $(G, \circ, 1)$ where

- G is a set
- $\circ : G \times G \to G$ is a function
- $1 \in G$ is a special element

satisfying three axioms [omitted].

② A set G of automorphisms of some object X in a category $\mathcal{C}$ satisfying

$$\forall \alpha, \beta \in G, \quad \alpha \circ \beta^{-1} \in G.$$

All groups that we care about are of Type ②. Definition ① is just a convenient device that allows us to see patterns and to prove general theorems.

It is clear how to go from type ② to type ①, i.e., just "forget" about the object X and the category $\mathcal{C}$. It is less clear how to go from ① to ②. Today I'll show you how to do this.

But first, please let me test your patience with some more abstract nonsense.

☆ Definition: Let $\mathcal{C}$ & $\mathcal{D}$ be categories. A (covariant) <u>functor</u>

$$F : \mathcal{C} \to \mathcal{D}$$

assigns to each object X in $\mathcal{C}$ an object $F(X)$ in $\mathcal{D}$, and assigns to each morphism $\alpha \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ a morphism $F(\alpha) \in \mathrm{Hom}_{\mathcal{D}}(F(X),F(Y))$ such that

- For all objects X in $\mathcal{C}$, $F(id_X) = id_{F(X)}$.
- For all $\alpha \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ & $\beta \in \mathrm{Hom}_{\mathcal{C}}(Y,Z)$, we have

$$\begin{tikzcd}
X \arrow[r, "\alpha"] \arrow[rr, bend right, "\beta\circ\alpha"'] & Y \arrow[r, "\beta"] & Z \arrow[r, phantom, "\Longrightarrow"] & F(X) \arrow[r, "F(\alpha)"] \arrow[rr, bend right, "F(\beta\circ\alpha)"'] & F(Y) \arrow[r, "F(\beta)"] & F(Z)
\end{tikzcd}$$

It follows that F sends commutative diagrams in $\mathcal{C}$ to commutative diagrams in $\mathcal{D}$.

A contravariant functor $F : \mathcal{C} \to \mathcal{D}$ is the same thing as a covariant functor $F : \mathcal{C}^{op} \to \mathcal{D}$, where $\mathcal{C}^{op}$ is the ↓

opposite category of $\mathcal{C}$ (with the same objects, and reversed arrows). That is, if F is contravariant then we have

$$\begin{tikzcd}
X \arrow[r, "\alpha"] \arrow[rr, bend right, "\beta\circ\alpha"'] & Y \arrow[r, "\beta"] & Z \arrow[r, phantom, "\Longrightarrow"] & F(X) & F(Y) \arrow[l, "F(\alpha)"'] & F(Z) \arrow[l, "F(\beta)"'] \arrow[ll, bend left, "F(\beta\circ\alpha)"]
\end{tikzcd}$$

///

We have already seen several examples of functors:

- If $\mathcal{C}$ & $\mathcal{D}$ are posets (i.e. with $|\mathrm{Hom}(X,Y)| \in \{0,1\}\ \forall X, Y$), then a functor $F : \mathcal{D} \to \mathcal{C}$ is just a morphism of posets. A contravariant Galois connection [the kind I originally defined] is a pair of contravariant functors

$$F : \mathcal{D} \rightleftarrows \mathcal{C} : G$$

such that for all objects X in $\mathcal{D}$ and Y in $\mathcal{C}$ there exists a bijection of hom sets

↓

$$\mathrm{Hom}_{\mathcal{D}}(X, G(Y)) \leftrightarrow \mathrm{Hom}_{\mathcal{C}}(Y, F(X)).$$

If we replace $\mathcal{C}$ by $\mathcal{C}^{op}$ then this becomes a covariant Galois connection

$$F : \mathcal{D} \rightleftarrows \mathcal{C}^{op} : G.$$

[Note that a functor $F : \mathcal{D} \to \mathcal{C}^{op}$ is the same thing as a functor $F : \mathcal{D}^{op} \to \mathcal{C}$.]

- We have seen functors that forget structure. The functor

$$\text{set} : \text{Grp} \to \text{Set}$$

forgets the identity element and product function of a group. The functor

$$\text{ab} : K\text{-Vec} \to \text{Ab}$$

forgets how to do scalar multiplication. The technical name for these is "forgetful functors".

Remark: Many forgetful functors $\mathcal{C} \to \mathcal{D}$ have an associated "free functor"

$$\text{free} : \mathcal{D} \rightleftarrows \mathcal{C} : \text{forget}$$

which sends an object X of $\mathcal{D}$ to the object $\text{free}(X)$ of $\mathcal{C}$ that is "freely generated" by X. In our first example

$$\text{free} : \text{Set} \rightleftarrows \text{Grp} : \text{forget} ,$$

$\text{free}(X)$ is called the free group generated by the set X. It satisfies the following universal property: For all sets X and groups G there is a "natural" bijection of hom sets

$$\text{Hom}_{\text{Set}}(X, \text{forget}(G)) \cong \text{Hom}_{\text{Grp}}(\text{free}(X), G) .$$

This probably seems intuitive: a set function $X \to \text{forget}(G)$ is the same thing as a group hom $\text{free}(X) \to G$. But what is the word "natural" supposed to mean?

"I didn't invent categories to study functors; I invented them to study natural transformations."

— Saunders Mac Lane.

☆ Definition: Let $\mathcal{C}$ & $\mathcal{D}$ be categories and let F & G be functors $\mathcal{C} \to \mathcal{D}$.
A natural transformation

$$\nu : F \to G$$

assigns to each object X of $\mathcal{C}$ a morphism $\nu_X \in \mathrm{Hom}_{\mathcal{C}}(F(X), G(X))$ such that for all morphisms $\alpha \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ the following diagram commutes

$$\begin{tikzcd}
F(X) \arrow[r, "F(\alpha)"] \arrow[d, "\nu_X"'] & F(Y) \arrow[d, "\nu_Y"] \\
G(X) \arrow[r, "G(\alpha)"] & G(Y)
\end{tikzcd}$$

We call ν a natural isomorphism if each ν_X is on isomorphism in $\mathcal{D}$.

Q: Isn't this an unnecessary level of abstraction?

A: Not according to Mac Lane.
More seriously, we will see that the notion of natural transformation will help us better understand even mundane situations.

The mother of all natural transformations is the following construction.

☆ Definition: Let $\mathcal{C}$ & $\mathcal{D}$ be categories and consider a pair of functors

$$F : \mathcal{D} \rightleftarrows \mathcal{C} : G.$$

We can use this to define a pair of functors

$$\mathrm{Hom}_{\mathcal{C}}(F-,-) : \mathcal{D}^{op} \times \mathcal{C} \to \mathrm{Set}$$

$$\mathrm{Hom}_{\mathcal{D}}(-,G-) : \mathcal{D}^{op} \times \mathcal{C} \to \mathrm{Set},$$

where the product category $\mathcal{D}^{op} \times \mathcal{C}$ is defined in the obvious way.

$\downarrow$

Now suppose that there exists a natural isomorphism

$$\Phi : \mathrm{Hom}_{\mathcal{C}}(F-,-) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}}(-,G-).$$

In this case we will say that

- F is left adjoint to G.
- G is right adjoint to F.
- (F,G) is an adjoint pair.
- $F : \mathcal{D} \rightleftarrows \mathcal{C} : G$ is an adjunction.

Examples:

- A Galois connection is nothing but an adjunction of posets.

- If forget $: \mathcal{D} \to \mathcal{C}$ is a forgetful functor, then we say free $: \mathcal{C} \to \mathcal{D}$ is the associated free functor if

$$(\text{free}, \text{forget})$$

is an adjoint pair.

Okay; I think that's enough abstract nonsense for now. I promised that I would tell you how to go from Definition ① to Definition ② of groups.

Let G be a group. Recall that we can think of G as a category with one object (call it $*$) and such that every morphism is an isomorphism. In this case we can identify

$$G = \mathrm{Aut}_G(*) = \mathrm{End}_G(*)$$

But what *is* this mysterious object $*$? Well, it could be anything. To turn $*$ into something interesting, choose a nice category $\mathcal{C}$ and consider a functor

$$F : G \to \mathcal{C}.$$

In other words, choose an object X in $\mathcal{C}$ and for every element $\alpha \in G = \mathrm{End}_G(*)$ consider an element $F(\alpha) \in \mathrm{End}_{\mathcal{C}}(X)$ such that

↓

- $F(id_*) = id_{F(*)} = id_X$

- $\forall \alpha, \beta \in G$ we have

$$F(\alpha \circ \beta) = F(\alpha) \circ F(\beta).$$

Since every $\alpha \in G$ is invertible we have

$$\begin{aligned} F(\alpha) \circ F(\alpha^{-1}) &= F(\alpha \circ \alpha^{-1}) \\ &= F(id_*) \\ &= id_X \end{aligned}$$

and similarly $F(\alpha^{-1}) \circ F(\alpha) = id_X$. It follows that $F(\alpha) \in End_{\mathcal{C}}(X)$ is actually an auto<u>morphism</u>, so we obtain a homomorphism of groups

$$F : G \longrightarrow Aut_{\mathcal{C}}(X),$$

which by abuse of notation we will also call F. [You might also like to force this F to be injective, but we will get a better theory if we don't require this.]

Jargon: Let G be a group and let $\mathcal{C}$ be a category. A functor

$$F : G \longrightarrow \mathcal{C}$$

is called a representation of G in the category $\mathcal{C}$. The flavor of representation theory depends on the choice of category.

We will begin next time by choosing $\mathcal{C} = \mathrm{Set}$, in which case the representations are called "G-sets".

11/3/15

I'll return the Midterm on Thursday.
HW4 : TBA.

Having finished the abstract structure theory of groups, our next topic will be the "representation theory" of groups.

This will require some new categorical ideas, so let me recall the definitions from last time.

☆ Definition : A covariant functor of categories

$$F : \mathcal{C} \to \mathcal{D}$$

sends objects to objects and arrows to arrows such that

- $F(id_X) = id_{F(X)}$ for all $X \in \mathcal{C}$
- $F(\alpha \circ \beta) = F(\alpha) \circ F(\beta)$ for all objects $X, Y, Z \in \mathcal{C}$ and morphisms $\beta : X \to Y$, $\alpha : Y \to Z$.

///

A contravariant functor $F : \mathcal{C} \to \mathcal{D}$ is the same thing as a covariant functor $F : \mathcal{C} \to \mathcal{D}^{op}$ [equivalently, $F : \mathcal{C}^{op} \to \mathcal{D}$], i.e., for all compositions $\alpha \circ \beta$ we have

$$F(\alpha \circ \beta) = F(\beta) \circ F(\alpha) .$$

One can check that categories are the objects of a category (called "Cat") with functors as arrows. The identity arrows are given by the identity functor

$$\mathrm{id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$$

that sends each object and arrow in $\mathcal{C}$ to itself. Then by definition we say that categories $\mathcal{C}$ & $\mathcal{D}$ are isomorphic if there exist functors

$$F : \mathcal{C} \rightleftarrows \mathcal{D} : G$$

such that $G \circ F = \mathrm{id}_{\mathcal{C}}$ & $F \circ G = \mathrm{id}_{\mathcal{D}}$.

However, isomorphism of categories is usually too strong to be useful. Since we really only care about objects up to isomorphism we should look for a notion of "equivalence" for categories that matches up isomorphism classes of objects.

For this we need another definition

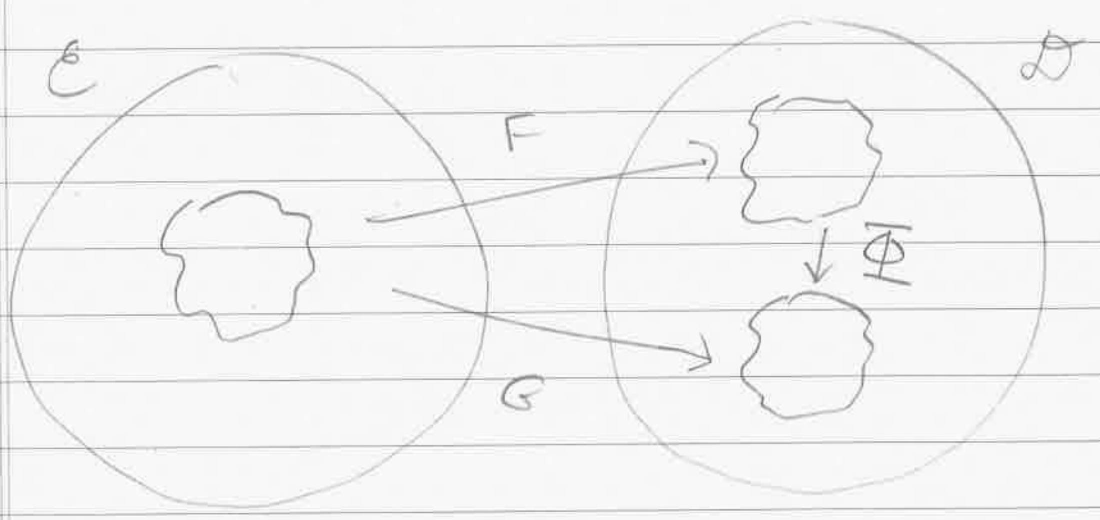
☆ Definition: Given two functors F & G from $\mathcal{C}$ to $\mathcal{D}$, a natural transformation

$$\Phi : F \to G$$

assigns to each object $X \in \mathcal{C}$ an arrow $\Phi(X) : F(X) \longrightarrow G(X)$ in $\mathcal{D}$ such that for all objects $X, Y \in \mathcal{C}$ and arrows $\alpha \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ the following diagram commutes

$$\begin{tikzcd}
F(X) \arrow[r, "F(\alpha)"] \arrow[d, "\Phi(X)"'] & F(Y) \arrow[d, "\Phi(Y)"] \\
G(X) \arrow[r, "G(\alpha)"'] & G(Y)
\end{tikzcd}$$

Intuition: Given a commutative diagram in $\mathcal{C}$, F & G produce two commutative diagrams in $\mathcal{D}$ and Φ produces a "morphism" of commutative diagrams



We will say that $\Phi : F \to G$ is a natural isomorphism if the arrow $\Phi(X) : F(X) \to G(X)$ is an isomorphism in $\mathcal{D}$ for all $X \in \mathcal{C}$. [Thus F & G are "equivalent up to isomorphism".]

Now we can state the correct definition for equivalence of categories.

☆ Definition : We say that categories $\mathcal{C}$ & $\mathcal{D}$ are equivalent if there exist functors

$$F : \mathcal{C} \rightleftarrows \mathcal{D} : G$$

and natural isomorphisms

$$\varepsilon : F \circ G \xrightarrow{\sim} id_{\mathcal{D}} \ \& \ \eta : id_{\mathcal{C}} \xrightarrow{\sim} G \circ F .$$

///

[Motivating Example : Let X be a topological space and consider its "fundamental groupoid" $\Pi_1(X)$. This is a category whose objects are the points of X and whose morphisms are homotopy equivalence classes of paths (thus every morphism is an isomorphism; hence "groupoid").

If X & Y are homotopy equivalent spaces then their groupoids $\Pi_1(X)$ & $\Pi_1(Y)$ are equivalent as categories, but not necessarily isomorphic.]

I'll present just one more definition today.

Since functors can be thought of as morphisms in a category of categories, you might wonder if natural transformations can be thought of as morphisms in a category of functors...

☆ Definition: Let $\mathcal{C}$ & $\mathcal{D}$ be categories and let $\mathcal{C}$ be small (i.e., it has only a *set* of objects). Then we can define the *functor category*

$$\mathcal{D}^{\mathcal{C}}$$

whose objects are functors $F : \mathcal{C} \to \mathcal{D}$ and whose morphisms are natural transformations $\Phi : F \to G$.

[Remark: The notation $\mathcal{D}^{\mathcal{C}}$ agrees with most of the other uses of exponential notation that you know.]

OK, that's enough abstract nonsense for next several days. It's time to begin the subject of "representation theory".

Let G be a group thought of as a (small) category with one object, and let $\mathcal{C}$ be any category.

A functor $\varphi : G \to \mathcal{C}$ is called a representation of G in $\mathcal{C}$. If $\mathrm{Obj}(G) = \{*\}$ and $X := \varphi(*) \in \mathcal{C}$ then φ induces a homomorphism of groups

$$\varphi : G \longrightarrow \mathrm{Aut}_{\mathcal{C}}(X).$$

If the objects of $\mathcal{C}$ are called "things" then often refer to the pair (X, φ) as a "G-thing" and we refer to the functor category

$$\mathcal{C}^G$$

as the *category of G-things*.

The prototypical example is the category Set^G of G-sets. Suppose that (X, φ) is a G-set so that

$$\varphi : G \to \mathrm{Aut}_{\mathrm{Set}}(X)$$

is a homomorphism from G into the group of permutations of the set X.

Let's unpack what this means:

Given $g \in G$ we obtain a function $\varphi_g : X \to X$ satisfying

① $\varphi_1(x) = x$ for all $x \in X$,

② $\varphi_{gh}(x) = \varphi_g(\varphi_h(x))$ for all $g, h \in G$, $x \in X$.

Surprisingly, these two properties are sufficient to define a group homomorphism $\varphi : G \to \mathrm{Aut}(X)$. This makes working in the category of G-sets very concrete.

In fact, let's record a definition.

↓

☆ Definition: Consider a group G and a set X. A left action of G on X is a function

$$\varphi : G \times X \to X$$

satisfing the two properties

① $\varphi(1,x) = x$ for all $x \in X$,

② $\varphi(gh,x) = \varphi(g,\varphi(h,x))$ for all $g,h \in G$, $x \in X$.

To simplify notation we will often use the metaphor

$$\text{“} \varphi(g,x) = g(x) \text{”}$$

and simply say that $g : X \to X$ is a function. Then the properties become

① $1(x) = x$

② $(gh)(x) = g(h(x))$.

This notation makes our lives easier, as long as we're careful.

///

OK, so we have a very concrete notation for G-sets. Is there also a conrete notation for morphisms of G-sets ?

Let $\alpha : G \to \text{Set}$ & $\beta : G \to \text{Set}$ be functors, i.e., choose sets $X, Y \in \text{Set}$ and group homomorphisms

$$\alpha : G \to \text{Aut}(X) \quad \& \quad \beta : G \to \text{Aut}(Y)$$

Since G has just one object, a natural transformation $f : \alpha \to \beta$ is just a function $f : X \to Y$ such that for all "arrows" $g \in G$ the following diagram commutes

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\alpha_g"'] & Y \arrow[d, "\beta_g"] \\
X \arrow[r, "f"'] & Y
\end{tikzcd}$$

If you're willing to use the metaphors

"$\alpha_g(x) = g(x)$" & "$\beta_g(y) = g(y)$"

then we can express the definition succintly as follows

☆ Definition: Let X & Y be G-sets. We say that a function $f: X \to Y$ is G-equivariant (or just a G-function) if for all $x \in X$, $g \in G$ we have

$$\boxed{f(g(x)) = g(f(x))}$$

///

Pretty simple, right? So why did I make all the fuss?

Because sometimes this notation is too simple. It's a great notation as long as you remember the implicit definitions behind it. But if you forget the definitions and start taking the metaphor literally, you'll be lost.

The same remark applies to any kind of representation theory: use the notation responsibly.

11/5/15

Midterm Stats:

Total = 30
Average = 22.9
Median = 22
St. Dev. = 4.2

HW4: TBA.

Let G be a group. Last time we defined the category of G-sets as the "functor category"

$$\text{Set}^G.$$

Today we will work with G-sets in a concrete way and we will prove a fundamental decomposition theorem.

Recall the following concrete interpretation of G-sets:

↓

☆ Let G be a group and X a set. A *left action* of G on X is a function

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g(x) \end{aligned}$$

satisfying the following two properties

- $1(x) = x \qquad \forall\, x \in X$
- $(gh)(x) = g(h(x)) \qquad \forall\, x \in X,\ g, h \in G.$

Sometimes we just write "$G \circlearrowleft X$" to indicate the existence of a left action.

A *right action* (written "$X \circlearrowright G$") is defined by

- $1(x) = x \qquad \forall\, x \in X$
- $(gh)(x) = h(g(x)) \qquad \forall\, x \in X,\ g, h \in G.$

(or you could say $(x)1 = x$ & $(x)(gh) = ((x)g)h$, but I prefer not to do that, thank you very much.)

///

[Remark: A left G-action is the same as a covariant functor $G \to \text{Set}$ and a right action is a contravariant functor $G \to \text{Set}$. The left/right terminology is arbitrary, but keep in mind that they are distinct concepts.]

☆ Let $G \circlearrowright X$ be a G-set and consider a subset $Y \subseteq X$. We will say that Y is a G-subset if

$$\forall g \in G, y \in Y, \; g(y) \in Y.$$

Note that $\emptyset, X \subseteq X$ are trivially G-subsets. We will say that $G \circlearrowright X$ is a simple (or transitive) G-set if it has no nontrivial G-subset.

A G-set is analyzed by means of "orbits" & "stabilizers".

☆ Let $G \circlearrowright X$ and consider an element $x \in X$. Then we define

↓

the orbit of x,

$$\mathrm{Orb}_G(x) = G(x) = \{ g(x) \in X : g \in G \}$$

and the stabilizer of x,

$$\mathrm{Stab}_G(x) = G_x = \{ g \in G : g(x) = x \}.$$

Orbits and stabilizers are intimately connected through the following lemma.

☆ Orbit - Stabilizer Lemma :

Let $G \circlearrowright X$. Then for all $x \in X$, the stabilizer $\mathrm{Stab}_G(x) \subseteq G$ is a subgroup and we have a bijection of sets

$$\mathrm{Orb}_G(x) \longleftrightarrow G / \mathrm{Stab}_G(x).$$

$$g(x) \longleftrightarrow g\,\mathrm{Stab}_G(x)$$

Proof : For all $g, h \in G$ we have

$$\downarrow$$

$$\begin{aligned} g(x) = h(x) &\iff g^{-1}h(x) = x \\ &\iff g^{-1}h \in \mathrm{Stab}_G(x) \\ &\iff g\,\mathrm{Stab}_G(x) = h\,\mathrm{Stab}_G(x), \end{aligned}$$

so the function is well-defined and injective in both directions. ///

In fact this is more than a bijection. Given two G-sets X & Y and a function $f: X \to Y$, we say that f is a <u>G-equivariant</u> function (or just a <u>G-function</u> if $\forall\, x \in X, g \in G$, we have

$$f(g(x)) = g(f(x)).$$

[Remark: This is the same as a natural transformation between functors $G \to \mathrm{Set}$.]

We will say that G-sets X & Y are isomorphic if there exists a G-equivariant bijection $X \xrightarrow{\sim} Y$.
[The inverse will automatically be equivariant.]

☆ Orbit-Stabilizer Theorem :

Let $G \circlearrowleft X$. Then for all $x \in X$ we have an isomorphism of G-sets,

$$\mathrm{Orb}_G(x) \approx G/\mathrm{Stab}_G(x).$$

Proof : we should first say in what sense these are G-sets.

- $\mathrm{Orb}_G(x)$ is a G-subset of X.
- We let $G \circlearrowleft G/\mathrm{Stab}_G(x)$ by left multiplication : $g\big(h\,\mathrm{Stab}_G(x)\big) := (gh)\mathrm{Stab}_G(x)$.

Then the bijection $\Phi(h(x)) = h\,\mathrm{Stab}_G(x)$ is equivariant since for all $g \in G$ and $h(x) \in \mathrm{Orb}_G(x)$ we have

$$\begin{aligned} \Phi(g(h(x))) &= \Phi((gh)(x)) \\ &= (gh)\,\mathrm{Stab}_G(x) \\ &= g(h\,\mathrm{Stab}_G(x)) \\ &= g(\Phi(h(x))). \end{aligned}$$

///

This theorem is the key to the structure theory of G-sets.

Recall that a G-set X is simple if it has no nontrivial G-subsets. Since every orbit is a G-subset we conclude that

$$G \circlearrowright X \text{ is simple} \iff \forall x \in X,\ \mathrm{Orb}_G(x) = X.$$

There is a convenient way to rephrase this.

☆ Lemma: $G \circlearrowright X$ is simple $\iff$ for all $x, y \in X$ there exists $g \in G$ such that

$$g(x) = y$$

Proof: Let $G \circlearrowright X$ be simple and consider any $x, y \in X$. Since $\mathrm{Orb}_G(x) = X$ we have $y \in \mathrm{Orb}_G(x)$ as desired.

Conversely, suppose $\forall x, y \in X, \exists g \in G, g(x) = y$. Then for all $x \in X$ we have $y \in \mathrm{Orb}_G(x)$ for all $y \in X$ and hence $\mathrm{Orb}_G(x) = X$. We conclude that $G \circlearrowright X$ is simple. ///

We can also think of orbits as equivalence classes for the following equivalence relation on X :

$$x \sim_G y \iff \exists g \in G,\ g(x) = y.$$

Then I guess we would write

$$\mathrm{Orb}_G(x) = [x]_G .$$

This makes it clear that X is a disjoint union of orbits.

☆ Theorem : Every G-set can be expressed uniquely as a disjoint union of simple G-sets.

Proof : Let $G \circlearrowleft X$. Then we have

$$* \qquad X = \bigsqcup_{i \in I} [x_i]_G$$

where $\{x_i : i \in I\}$ is a set of representatives for the orbits. To show that this expression is unique, let $Y \subseteq X$ be any simple G-subset.

↓

Now choose any element $y \in Y$, which generates a G-subset $[y]_G \subseteq Y$. Since Y is simple we must have $Y = [y]_G$. Then from the disjoint union $*$, $\exists\, i$ such that $y \in [x_i]_G$ and it follows that

$$Y = [y]_G = [x_i]_G.$$

///

It remains to classify the simple G-sets up to isomorphism.

If $G \circlearrowright X$ is simple, then by the Orbit-Stabilizer Theorem we have an isomorphism of G-sets

$$X \approx G/H$$

where $H = \mathrm{Stab}_H(x)$ for any $x \in X$. Certainly, every subgroup $H \subseteq G$ occurs because we could just define $X := G/H$ with left multiplication.

The classification will be completed by the following result.

☆ Theorem: Let $H, K \leq G$ be subgroups. Then we have an isomorphism of G-sets

$$G/H \approx G/K$$

if and only if $H = gKg^{-1}$ for some $g \in G$.

///

We'll give the proof in three steps:

(1) Let $G \circlearrowright X$. Then for all $g \in G$ and $x \in X$ we have

$$\mathrm{Stab}_G(g(x)) = g\,\mathrm{Stab}_G(x)\,g^{-1}.$$

Proof: For all $h \in G$ we have

$$\begin{aligned} h \in \mathrm{Stab}_G(g(x)) &\Longleftrightarrow h(g(x)) = g(x) \\ &\Longleftrightarrow g^{-1}hg\,(x) = x \\ &\Longleftrightarrow g^{-1}hg \in \mathrm{Stab}_G(x) \\ &\Longleftrightarrow h \in g\,\mathrm{Stab}_G(x)\,g^{-1}. \end{aligned}$$

///

↓

(2) If $\varphi : X \to Y$ is an isomorphism of G-sets, then $\forall\, x \in X$ we have

$$\mathrm{Stab}_G(x) = \mathrm{Stab}_G(\varphi(x)).$$

Proof: Let $g \in \mathrm{Stab}_G(x)$. Then

$$g(\varphi(x)) = \varphi(g(x)) = \varphi(x)$$

implies that $g \in \mathrm{Stab}_G(\varphi(x))$. We conclude that $\mathrm{Stab}_G(x) \subseteq \mathrm{Stab}_G(\varphi(x))$.

Now using the fact that φ^{-1} is also a G-function gives

$$\begin{aligned}\mathrm{Stab}_G(\varphi(x)) &\subseteq \mathrm{Stab}_G(\varphi^{-1}(\varphi(x))) \\ &= \mathrm{Stab}_G(x)\end{aligned}$$

///

(3) Let $H, K \leq G$ be subgroups.

If there exists an isomorphism of G-sets $\varphi : G/H \to G/K$ then let $\varphi(H) = gK$. It follows from (1) and (2) that

↓

$$\begin{aligned} H &= \{ g \in G : gH = H \} \\ &= \mathrm{Stab}_G(H). \\ &= \mathrm{Stab}_G(\varphi(H)) \\ &= \mathrm{Stab}_G(gK) \\ &= g\, \mathrm{Stab}_G(K)\, g^{-1} \\ &= g \{ g \in G : gK = K \} g^{-1} \\ &= g K g^{-1}. \end{aligned}$$

Conversely, suppose that $H = gKg^{-1}$ for some $g \in G$. Then we have

$$\begin{aligned} H &= gKg^{-1} \\ &= g\, \mathrm{Stab}_G(K)\, g^{-1} \\ &= \mathrm{Stab}_G(gK) \end{aligned}$$

and the Orbit-Stabilizer Theorem gives

$$\begin{aligned} G/H &= G/\mathrm{Stab}_G(gK) \\ &\approx \mathrm{Orb}_G(gK) \\ &= \{ hgK : h \in G \} \\ &= \{ gK : g \in G \} \\ &= G/K. \end{aligned}$$

QED.

In summary, let me state the full result.

☆ Fundamental Theorem of G-sets:

- Every G-set has a unique expression as a disjoint union of <u>simple</u> G-sets

- Every simple G-set has the form G/H for some subgroup $H \leq G$ and we have

$$G/H \approx G/K$$

if and only if H & K are conjugate.

///

This inspires a very deep idea:

> There is no such thing as a G-set; there is only G.

11/10/15

HW4 : still TBA.

Last time we proved the following result.

☆ Fundamental Theorem of G-sets :

- Every G-set can be expressed uniquely as a disjoint union of simple G-sets.
- The simple G-sets are just G/H where H is a subgroup. Furthermore, we have

$$G/H \approx G/K$$

if and only if $H = gKg^{-1}$ for some $g \in G$.

///

This theorem suggests a deep idea :

> There is no such thing as a G-set;
> there is only G acting on itself.

This idea was famously expressed by Felix Klein in his "Erlangen Program".

///

So let's investigate how G acts on itself.

Given a subgroup $H \subseteq G$ we can define a left action of H on G by right multiplication as follows

$$\begin{aligned} G \times H &\longrightarrow G \\ (g, h) &\longmapsto gh^{-1}. \end{aligned}$$

Check the axioms: we have

- $g1^{-1} = g \quad \forall\, g \in G$,
- $g(h_1 h_2)^{-1} = (gh_2^{-1})h_1^{-1} \quad \forall\, g \in G,\ h_1, h_2 \in H$,

as desired. ///

The orbits of this action are the left cosets of H in G:

$$\begin{aligned} \mathrm{Orb}_H(g) &= \{ gh^{-1} : h \in H \} \\ &= \{ gh : h \in H \} = gH. \end{aligned}$$

Now we can define a left action of G on the set G/H of H-orbits by left multiplication as follows

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g_1, g_2H) &\longmapsto (g_1g_2)H. \end{aligned}$$

Check: For all $gH \in G/H$, $g_1, g_2 \in G$,

- $(1g)H = gH$

- $$\begin{aligned} (g_1g_2)(gH) &= ((g_1g_2)g)H \\ &= (g_1(g_2g))H \\ &= g_1(g_2(gH)). \end{aligned}$$ ///

Note that the G-set G/H is simple because G acts transitively: For all $g_1H, g_2H \in G/H$ there exists $g_2g_1^{-1} \in G$ such that

$$(g_2g_1^{-1})(g_1H) = (g_2g_1^{-1}g_1)H = g_2H.$$

Note that $\forall\, gH \in G/H$ we have

$$\mathrm{Orb}_G(gH) = G/H \quad \& \quad \mathrm{Stab}_G(gH) = gHg^{-1},$$

hence the orbit-stabilizer theorem says

$$G/H = \mathrm{Orb}_G(g) \approx G/\mathrm{Stab}_G(g) = G/gHg^{-1},$$

which we already knew. So let's consider a more general situation.

☆ Definition: Let $H, K \subseteq G$ be subgroups. Then we can define a left action of the direct product $H \times K$ on G by

$$\begin{aligned} (H\times K)\times G &\longrightarrow G \\ ((h,k),g) &\longmapsto hgk^{-1}. \end{aligned}$$

The orbits of this action are called double cosets. For all $g \in G$ we have

$$\begin{aligned} \mathrm{Orb}_G(g) &= \{hgk^{-1} : h\in H, k\in K\} \\ &= \{hgk : h \in H, k\in K\} \\ &=: HgK. \end{aligned}$$

We will denote the set of double cosets by

$$H\backslash G/K := \{HgK : g\in G\}.$$

///

What does orbit-stabilizer say here?

First consider the action $H \circlearrowright G/K$ defined by $h(gK) = (hg)K$ and note that the double coset HgK is given by

$$HgK = \bigcup_{h \in H} (hg)K$$

$$= \bigsqcup_{C \in \mathrm{Orb}_H(gK)} C \quad ,$$

where second union is disjoint by definition. Since any two cosets g_1K, g_2K are in bijection we obtain a bijection

$$HgK \longleftrightarrow \mathrm{Orb}_H(gK) \times K .$$

Then since

$$\begin{aligned} \mathrm{Stab}_H(gK) &= \{h \in H : hgK = gK\} \\ &= \{h \in H : g^{-1}hgK = K\} \\ &= \{h \in H : g^{-1}hg \in K\} \\ &= \{h \in H : h \in gKg^{-1}\} \\ &= H \cap gKg^{-1} \quad , \end{aligned}$$

orbit-stabilizer gives a bijection of H-sets:

$$\mathrm{Orb}_H(gK) \longleftrightarrow H/(H \cap gKg^{-1}).$$

Putting the two bijections together gives

$$HgK \longleftrightarrow \left(H/(H \cap gKg^{-1})\right) \times K.$$

[Remark: Starting instead with the action $H \backslash G \circlearrowleft K$ gives a bijection

$$HgK \longleftrightarrow H \times \left(K/(g^{-1}Hg \cap K)\right).$$]

Finally, if H & K are both finite the above bijection implies that

$$|HgK| = \left|\frac{H}{H \cap gKg^{-1}}\right| \cdot |K|$$

$$= \frac{|H|}{|H \cap gKg^{-1}|} \cdot |K|$$

$$= |H| \cdot |K| \Big/ |H \cap gKg^{-1}|.$$

In summary, we have the following.

☆ Theorem: Let $H, K \leq G$ be <u>finite</u> subgroups. Then for all $g \in G$ we have

$$|HgK| = \frac{|H| \cdot |K|}{|H \cap gKg^{-1}|} = \frac{|H| \cdot |K|}{|g^{-1}Hg \cap K|} .$$

☆ Corollary: Setting $g=1$ gives

$$|HK| = |H| \cdot |K| \,/\, |H \cap K| ,$$

even when HK is not a group. ///

The most interesting examples of double cosets come from matrix groups.

For example, let's consider the "LU decomposition" of an invertible matrix.

☆ Definition: Given a field K and a nonzero scalar $\alpha \in K^\times$ we define the <u>elementary</u> matrices

$$E_{ij}(\alpha)\,,\ E_{ii}(\alpha)\,,\ P_{ij} \in GL_n(K)$$

as follows:

$$E_{ij}(\alpha) = \begin{array}{cc} & \begin{matrix} & & & & j & & \end{matrix} \\ \begin{matrix} \\ \\ i \\ \\ \\ \\ \\ \end{matrix} & \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & \cdots & \alpha & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array}$$

$$E_{ii}(\alpha) = \begin{array}{cc} & \begin{matrix} & & & i & & & \end{matrix} \\ \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ \end{matrix} & \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \alpha & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array}$$

$$P_{ij} = \begin{array}{cc} & \begin{matrix} & & & i & & & & j & & & \end{matrix} \\ \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \\ \end{matrix} & \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & 0 & \cdots & \cdots & \cdots & 1 & & & \\ & & & & 1 & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & 1 & & & & \\ & & & 1 & \cdots & \cdots & \cdots & 0 & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & \ddots & \\ & & & & & & & & & & 1 \end{pmatrix} \end{array}$$

///

Now suppose $A \in GL_n(K)$ has kth row a_k. Then we have,

- kth row of $E_{ij}(\alpha)A = \begin{cases} a_k & k \neq i \\ a_k + \alpha a_j & k = i \end{cases}$

- kth row of $E_{ii}(\alpha)A = \begin{cases} a_k & k \neq i \\ \alpha a_k & k = i \end{cases}$

- kth row of $P_{ij}A = \begin{cases} a_k & k \notin \{i,j\} \\ a_j & k = i \\ a_i & k = j \end{cases}$.

Thus multiplying on the left of A by elementary matrices performs "elementary row operations". Similarly, multiplying on the right of A performs "elementary column operations".

Now the familiar Gaussian elimination algorithm can be phrased as follows.

☆ Gaussion Elimination: Let $A \in GL_n(K)$. Then we can reduce A to the identity matrix in three steps,

(1) Multiply on the left by lower triangular matrices $E_{ij}(\alpha)$ $(j \leq i)$.

(2) Multiply on the left by permutation matrices P_{ij}.

(3) Multiply on the left by upper triangular matrices $E_{ij}(\alpha)$ $(i \leq j)$.

In summary, we obtain

$$UPLA = I$$
$$A = L^{-1}P^{-1}U^{-1}$$

where L^{-1} is lower triangular, P^{-1} is a permutation, and U^{-1} is upper triangular.

///

For example, consider the matrix

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ -1 & 0 & 4 \end{pmatrix}.$$

Then we have

① $$\begin{pmatrix} 0 & \textcircled{1} & 2 \\ 1 & 2 & 3 \\ -1 & 0 & 4 \end{pmatrix} \xrightarrow{E_{21}(-2)} \begin{pmatrix} 0 & \textcircled{1} & 2 \\ \textcircled{1} & 0 & -1 \\ -1 & 0 & 4 \end{pmatrix}$$

$$\xrightarrow{E_{32}(1)} \begin{pmatrix} 0 & \textcircled{1} & 2 \\ \textcircled{1} & 0 & -1 \\ 0 & 0 & \textcircled{3} \end{pmatrix} \xrightarrow{E_{33}(1/3)} \begin{pmatrix} 0 & \textcircled{1} & 2 \\ \textcircled{1} & 0 & -1 \\ 0 & 0 & \textcircled{1} \end{pmatrix}$$

② $$\xrightarrow{P_{12}} \begin{pmatrix} \textcircled{1} & 0 & -1 \\ 0 & \textcircled{1} & 2 \\ 0 & 0 & \textcircled{1} \end{pmatrix}$$

③ $$\xrightarrow{E_{23}(-2)} \begin{pmatrix} \textcircled{1} & 0 & -1 \\ 0 & \textcircled{1} & 0 \\ 0 & 0 & \textcircled{1} \end{pmatrix} \xrightarrow{E_{13}(1)} \begin{pmatrix} \textcircled{1} & 0 & 0 \\ 0 & \textcircled{1} & 0 \\ 0 & 0 & \textcircled{1} \end{pmatrix}.$$

We conclude that

$$E_{13}(1)\,E_{23}(-2)\,P_{12}\,E_{33}(1/3)\,E_{32}(1)\,E_{21}(-2)\,A = I$$

$$\Longrightarrow \quad A = LPU,$$

where $L = E_{21}(-2)^{-1}\,E_{32}(1)^{-1}\,E_{33}(1/3)^{-1}$

$$\downarrow$$

$$= E_{21}(+2)\, E_{32}(-1)\, E_{33}(3)$$

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

$$= \begin{pmatrix} 1 & & \\ 2 & 1 & \\ & -1 & 3 \end{pmatrix},$$

$$P = P_{12}^{-1} = P_{12} = \begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix},$$

$$U = E_{23}(-2)^{-1}\, E_{13}(1)^{-1}$$

$$= E_{23}(+2)\, E_{13}(-1)$$

$$= \begin{pmatrix} 1 & & \\ & 1 & 2 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & & -1 \\ & 1 & \\ & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & & -1 \\ & 1 & 2 \\ & & 1 \end{pmatrix}.$$

///

To be fancy, we will let

$$B^+, B^- \subseteq GL_n(K)$$

be the subgroups of upper and lower triangular matrices and we will call them positive and negative *Borel* subgroups. We will denote the subgroup of permutation matrices by

$$W \subseteq GL_n(K)$$

and will call it a *Weyl* subgroup.

Now let the direct product $B^- \times B^+$ act on $GL_n(K)$ by

$$(B^- \times B^+) \times GL_n(K) \longrightarrow GL_n(K)$$

$$((l, u), g) \longmapsto l g u^{-1} .$$

Gaussian elimination tells us that every double coset $B^- g B^+$ contains a permutation matrix.

Proof : Consider an element $lgu \in B^- g B^+$. Applying Gaussian elimination gives

$$lgu = l_1 w u_1$$

for some $l_1 \in B^-$, $w \in W$, $u_1 \in B^+$ and then we have

$$w = l_1^{-1} l g u u_1^{-1} \in B^- g B^+ .$$ ///

In fact it is not too difficult to show that each double coset contains a unique permutation, so we can express $GL_n(K)$ as a disjoint union parametrized by W :

$$GL_n(K) = \bigsqcup_{w \in W} B^- w B^+ .$$

For some reason algebraists prefer to use a modified form of Gaussian elimination and to use double cosets of $B^+ \times B^+$ to show that

$$GL_n(K) = \bigsqcup_{w \in W} B^+ w B^+ ,$$

and they call this a Bruhat decomposition of $GL_n(K)$. This decomposition is an importont tool in studying $GL_n(K)$ as an algebraic variety.

Remark: The Bruhat decomposition of $GL_n(K)$ also induces a partial order on the set W of permutations.

Given $u, v \in W$, the cosets B^+uB^+ and B^+vB^+ are disjoint, but their closures (~~in~~ a certain topology) might be related. So we define

$$u \leq_B v \iff B^+uB^+ \subseteq \overline{B^+vB^+}.$$

When $K = \mathbb{C}$ the topology is the obvious one (i.e. we think of $GL_n(\mathbb{C})$ as a subset of $\mathbb{C}^{n\times n}$).

11/12/15

HW4 : still TBA.

In the philosophy of Klein's "Erlangen Program" there is no such thing as a G-set ; there is only G acting on itself.

Last time we discussed the "regular" action of G on itself by left or right multiplication (or both).

Today we'll discuss a very importont special case, called "conjugation".

Recall that we have a group homomorphism $\varphi : G \times G \longrightarrow G$ defined by

$$\varphi_{g,h}(a) := gah^{-1}$$

If we compose this with the left or right embedding

$$G \longrightarrow G \times G \qquad \& \qquad G \longrightarrow G \times G$$
$$g \longmapsto (g,1) \qquad\qquad g \longmapsto (1,g)$$

we obtain the left or right *regular* action. However, if we compose with the *diagonal* embedding

$$\begin{aligned}\Delta : G &\longrightarrow G\times G\\ g &\longmapsto (g,g)\end{aligned}$$

Then we obtain the action of G on itself by *conjugation*:

$$\begin{tikzcd}
G \arrow[r, "\Delta"] & G\times G \arrow[r, "\varphi"] & \mathrm{Aut}(G) \\
g \arrow[r, mapsto] & (g,g) \arrow[r, mapsto] & \varphi_{g,g}
\end{tikzcd},$$

defined by

$$\varphi_{g,g}(a) = gag^{-1}. \qquad ///$$

Let's investigate what orbit-stabilizer says about conjugation.

☆ Definition: Let $G \circlearrowleft G$ by conjugation. For all $a \in G$ we define its *conjugacy class*

$$K_G(a) := \mathrm{Orb}_G(a) = \{ gag^{-1} : g \in G \}$$

and its centralizer

$$\begin{aligned} Z_G(a) := \mathrm{Stab}_G(a) &= \{ g \in G : gag^{-1} = a \} \\ &= \{ g \in G : ga = ag \}, \end{aligned}$$

[K is for "Klasse", Z is for "Zentrum".]

Then orbit-stabilizer gives a bijection

$$K(a) \longleftrightarrow G/Z(a).$$

We also define the center of G

$$Z(G) := \{ a \in G : ga = ag \ \forall g \in G \}.$$

and note that

$$\begin{aligned} |K(a)| = 1 &\iff K(a) = \{a\} \\ &\iff gag^{-1} = a \quad \forall g \in G \\ &\iff ga = ag \quad \forall g \in G \\ &\iff a \in Z(G). \end{aligned}$$

If we let K_i, $i \in I$, be the conjugacy classes of G with corresponding centralizers Z_i (defined up to conjugacy) then we obtain the orbit decomposition

$$\begin{aligned} G &= \bigsqcup_i K_i \\ &= \Big(\bigsqcup_{|K_i|=1} K_i \Big) \sqcup \Big(\bigsqcup_{|K_i|\neq 1} K_i \Big) \\ &= \Big(\bigsqcup_{a \in Z(G)} \{a\} \Big) \sqcup \Big(\bigsqcup_{|K_i|\neq 1} K_i \Big) \\ &= Z(G) \sqcup \Big(\bigsqcup_{|K_i|\neq 1} K_i \Big) \end{aligned}$$

and orbit-stabilizer gives a bijection

$$G \leftrightarrow Z(G) \sqcup \Big(\bigsqcup_{Z_i \neq G} G/Z_i \Big)$$

If G is finite we obtain

☆ $$|G| = |Z(G)| + \sum_{Z_i \neq G} \frac{|G|}{|Z_i|}$$

which is called the class <u>equation</u> of G.

///

Example: The symmetric group S_n.

Recall that congugacy classes of S_n are parametrized by "integer partitions" of n, i.e. sequences

$$\lambda = (\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_\ell)$$

such that $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_\ell \geq 1$ and $\sum_i^\ell \lambda_i = n$.

Let K_λ be the class of permutations of "cycle type" λ and let Z_λ be the corresponding centralizer. If λ has m_i parts of size i then one can check that

$$|Z_\lambda| = 1^{m_1} m_1! \, 2^{m_2} m_2! \, 3^{m_3} m_3! \cdots$$

$$= \prod_{i \geq 1} i^{m_i} \cdot m_i!$$

and hence

$$|K_\lambda| = \frac{n!}{\prod_{i \geq 1} i^{m_1} \cdot m_i!}$$

For example, when $n=5$ we have

λ	m	$\lvert Z_\lambda \rvert$	$\lvert K_\lambda \rvert$
5	00001	$5^1 \cdot 1! = 5$	24
41	1001	$1^1 \cdot 1!\, 4^1 \cdot 1! = 4$	30
32	011	$2^1 \cdot 1!\, 3^1 \cdot 1! = 6$	20
311	201	$1^2 \cdot 2!\, 3^1 \cdot 1! = 6$	20
221	12	$1^1 \cdot 1!\, 2^2 \cdot 2! = 8$	15
2111	31	$1^3 \cdot 3!\, 2^1 \cdot 1! = 12$	10
11111	5	$1^5 \cdot 5! = 120$	1

Note that $|K_\lambda| = 1 \iff \lambda = (1,1,1,1,1)$ and hence

$$Z(S_5) = \{1\}$$

In general we have $Z(S_n) = \{1\}$ which shows that S_n "very" non-abelian.

Note also that

$$1 + 10 + 15 + 20 + 20 + 30 + 24 = 120,$$

so we probably didn't make a mistake.

One application of the class equation is that every normal subgroup is a union of conjugacy classes. If we know the sizes of the conjugacy classes then this greatly restricts the sizes of possible normal subgroups.

Thus, a normal subgroup $N \trianglelefteq S_5$ must have size

$$1 + (\text{some of } 10, 15, 20, 20, 30, 24)$$

and the size must divide $|S_5| = 120$. It turns out there are only three nontrivial possibilities:

$$N_1 = K_{11111} \sqcup K_{221} \sqcup K_5$$

$$N_2 = K_{11111} \sqcup K_{221} \sqcup K_{311} \sqcup K_5$$

$$N_3 = K_{11111} \sqcup K_{221} \sqcup K_{32} \sqcup K_5$$

It turns out that $N_2 = A_5 \trianglelefteq S_5$ and that N_1 & N_3 are not subgroups.

We conclude that A_5 is the only nontrivial normal subgroup of S_5. However, this does not quite prove that A_5 is simple. [For that, see HW4.].

///

The other major applictation of the class equation is to Sylow Theory.

If G is a finite group, recall that "Lagrange's Theorem" says:

If there exists a subgroup $H \leq G$ of size n, then $n \mid |G|$.

Unfortunately, the converse statement,

$\circledast$ If $n \mid |G|$ then there exists a subgroup $H \leq G$ of order n.

is FALSE.

Proof : we will show that the alternating group of order 12 ,

$$A_4 = K_{1111} \sqcup K_{22} \sqcup K_3 \trianglelefteq S_4$$

has *no* subgroup of order 6 .

So suppose $H \subseteq A_4$ is a subgroup with $|H| = 6$. Then $H \approx \mathbb{Z}/6\mathbb{Z}$ or D_6 . Since A_4 has no element of order 6 we must have

$$H \approx D_6 .$$

Since D_6 has three elements of order 2 we must have

$$K_{22} = \{(12)(34), (13)(24), (14)(23)\} \subseteq H .$$

But the elements of order 2 in D_6 (i.e. the reflections) *don't* commute and the elements of K_{22} *do* commute.

Contradiction.

///.

Sylow Theory is the attempt to find the strongest possible approximation to $\circledast$ that is true, i.e. to determine all properties of G that depend only on its size $|G|$.

Here is the main result.

☆ Sylow's Theorem:

Suppose that $|G| = p^\alpha m$ with p prime and $p \nmid m$, We say that $H \leq G$ is a Sylow p-subgroup if $|H| = p^\alpha$. Let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups. Then

① $\mathrm{Syl}_p(G) \neq \emptyset$.

② If $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is any p-subgroup (i.e. $|Q| = p^\beta$, $\beta \leq \alpha$) then $\exists\, g \in G$ such that

$$gQg^{-1} \leq P.$$

↓

In particular, any two Sylow p-subgroups are conjugate.

③ $|\mathrm{Syl}_p(G)| = 1 \mod p$

& $|\mathrm{Syl}_p(G)| \,\Big|\, m$.

///

We'll prove the theorem next week. [Suprisingly, It turns out that part ① is the hardest.]

For now, here's a cool analogy:

Let $G = GL_n(K)$. We say $g \in G$ is <u>unipotent</u> if all of its eigenvalues are 1. A subgroup $H \leq G$ is called <u>unipotent</u> if all of its elements are unipotent.

It turns out that the group of upper unitriangular matrices

$$U = \left\{ \begin{pmatrix} 1 & & * \\ & 1 \ddots & \\ 0 & & 1 \end{pmatrix} \in G \right\}$$

is a *maximal* unipotent subgroup and furthermore, if $H \leq G$ is *any* unipotent subgroup then $\exists\, g \in G$ such that

$$gHg^{-1} \subseteq U .$$

Over a general field K this is called "Kolchin's Theorem" and it is fairly tricky to prove.

However, if K is a finite field of characteristic p it turns out that a subgroup

$$H \leq GL_n(K)$$

is unipotent if and only if it is a p-group, so in this case Kolchin's Theorem is equivalent to part ② of Sylow's Theorem.

Cool, right?

11/17/15

HW4 due Thurs Dec 3.

Last time I stated Sylow's Theorem. It requires some terminology.

☆ Definition: Let p be prime. A p-group is a finite group of size p^α for some α. We say that a subgroup $H \leq G$ is a p-subgroup if H is a p-group.

Now let $|G| = p^\alpha m$ with $\gcd(p,m)=1$. A Sylow p-subgroup is a p-subgroup $H \leq G$ with size $|H| = p^\alpha$.

Let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups of G.

☆ Sylow's Theorem (1872):

Let $|G| = p^\alpha m$ with $\gcd(p,m)=1$. Then we have

① $\mathrm{Syl}_p(G) \neq \emptyset$.

i.e., a Sylow p-subgroup exists.

② If $P \in Syl_p(G)$ and $Q \leq G$ is any p-subgroup then there exists $g \in G$ such that

$$gQg^{-1} \subseteq P.$$

This implies that

- Every p-subgroup is contained in a Sylow p-subgroup

- Any two Sylow p-subgroups are conjugate, hence if there exists a unique Sylow p-subgroup it must be normal.

③ $|Syl_p(G)| = 1 \bmod p$

& $|Syl_p(G)| \mid m.$

///

Before proving the theorem, let me show you an application.

☆ Theorem: Let $|G| = pqr$ with $p<q<r$ prime. Then G is not simple.

Proof: By ① we have

$$\begin{aligned} n_p &:= |\mathrm{Syl}_p(G)| \geq 1, \\ n_q &:= |\mathrm{Syl}_q(G)| \geq 1, \\ n_r &:= |\mathrm{Syl}_r(G)| \geq 1. \end{aligned}$$

If any of n_p, n_q, n_r equals 1 then we obtain a normal Sylow subgroup by ②.

So assume for contradiction that $n_p, n_q, n_r > 1$. By ③ we must have

$$\begin{aligned} n_r &= pq, \\ n_q &\in \{r, pr\}, \\ n_p &\in \{q, r, qr\}. \end{aligned}$$

Note that the Sylow subgroups of G are isomorphic to

$$\mathbb{Z}/p\mathbb{Z}, \quad \mathbb{Z}/q\mathbb{Z}, \quad \text{or } \mathbb{Z}/r\mathbb{Z}.$$

Since p, q, r are prime any two of these subgroups intersect trivially.

Now let's count the elements of G with orders $p, q, r, 1$, and show that there are too many.

Each of the n_p copies of $\mathbb{Z}/p\mathbb{Z}$ contains $p-1$ elements of order p, and similarly for q and r. Thus we have

$$
\begin{aligned}
|G| &\geq n_r(r-1) + n_q(q-1) + n_p(p-1) + 1 \\
&\geq pq(r-1) + r(q-1) + q(p-1) + 1 \\
&= pqr - \cancel{pq} + qr - r + \cancel{pq} - q + 1 \\
&= pqr + (q-1)(r-1).
\end{aligned}
$$

Since $|G| = pqr$ this implies that

$$(q-1)(r-1) \leq 0$$

which contradicts the fact that $q-1 > 0$ and $r-1 > 0$.

///

Pretty slick, right? That's the typical way that Sylow's Theorem gets applied.

Now let's prove it. We'll start small and work our way up.

☆ Theorem: Let A be a finite abelian group and let p be prime.

If $p \mid |A|$, the A has an element of order p.

Proof by induction on $|A|$:

If A is cyclic we're done. So consider an element $1 \neq x \in A$ such that $H := \langle x \rangle \subsetneq A$.

If $p \mid |H|$ then by induction H has an element of order p, hence so does A.

So assume that $p \nmid |H|$ and consider the quotient group A/H.

(Note that $H \trianglelefteq A$ because A is abelian.) Since $p \mid |A|$ and $p \nmid |H|$ we have

$$p \mid |A|/|H| = |A/H| .$$

By induction this implies that A/H has on element of order p, say aH. Then we have

$$aH \neq H$$
$$(aH)^p = a^p H = H$$

hence $a \notin H$ and $a^p \in H$.

Now let $m = |H|$, so by Lagrange we have

$$a^p \in H \implies (a^p)^m = 1 .$$

But then $(a^m)^p = (a^p)^m = 1$, so that a^m has order dividing p. If a^m has order p we're done.

So assume that a^m has order 1, i.e., $a^m = 1$.

Then we have

$$(aH)^m = a^m H = H$$

This implies that the order of aH divides m. But the order of aH is p and we assumed that

$$p \nmid |H| = m.$$

Contradiction. ///

[Remark: This result could be proved more easily with stronger technology, e.g., the Fundamental Theorem of Finite Abelian Groups, but we don't have that yet. We'll prove it next semester]

We have shown that

$$p \mid |A| \implies \exists \text{ element of order } p$$

when A is an abelian group. Next we'll prove it for non-abelian groups.

☆ Cauchy's Theorem (1815):

Consider a finite group G and a prime p.

If $p \mid |G|$ then G has an element of order p.

Proof by induction on $|G|$:

Let $p \mid |G|$ and consider the class equation of G,

$$|G| = |Z(G)| + \sum_{Z_i \neq G} \frac{|G|}{|Z_i|},$$

where Z_i are the non-trivial stabilizer subgroups. If $p \mid |Z_i|$ for some $Z_i \neq G$ then by induction Z_i has an element of order p, hence so does G.

So assume that $p \nmid |Z_i|$ for all $Z_i \neq G$. Then we have

$$p \mid |G| / |Z_i|,$$

so the class equation implies $p \mid |Z(G)|$.

If $Z(G) \neq G$ then by induction $Z(G)$ has an element of order p, hence so does G.

So assume that $Z(G) = G$. Then G is abelian, so the previous theorem implies that G has an element of order p.

In particular, this shows that if $p \mid |G|$ then G has a <u>subgroup</u> of order p (the cyclic group generated by an element of order p).

Our next job is to lift this to higher powers of p.

☆ Theorem (Sylow ①) :

Let G be a finite group and let p be prime. If $p^n \mid |G|$ then G has subgroups of order p^m for all $1 \leq m \leq n$.

Proof by induction on $|G|$:

Let $p^n \mid |G|$ and consider the class equation

$$|G| = |Z(G)| + \sum_{Z_i \neq G} \frac{|G|}{|Z_i|}.$$

If $p^n \mid |Z_i|$ for some $Z_i \neq G$ then we're done by induction. So assume that $p^n \nmid |Z_i|$ for all $Z_i \neq G$. Since $p^n \mid |G|$ this implies that

$$p \mid |G|/|Z_i| \quad \text{for all } Z_i \neq G$$

and the class equation then implies that $p \mid |Z(G)|$. Hence p has on element of order p, say $z \in Z(G)$.

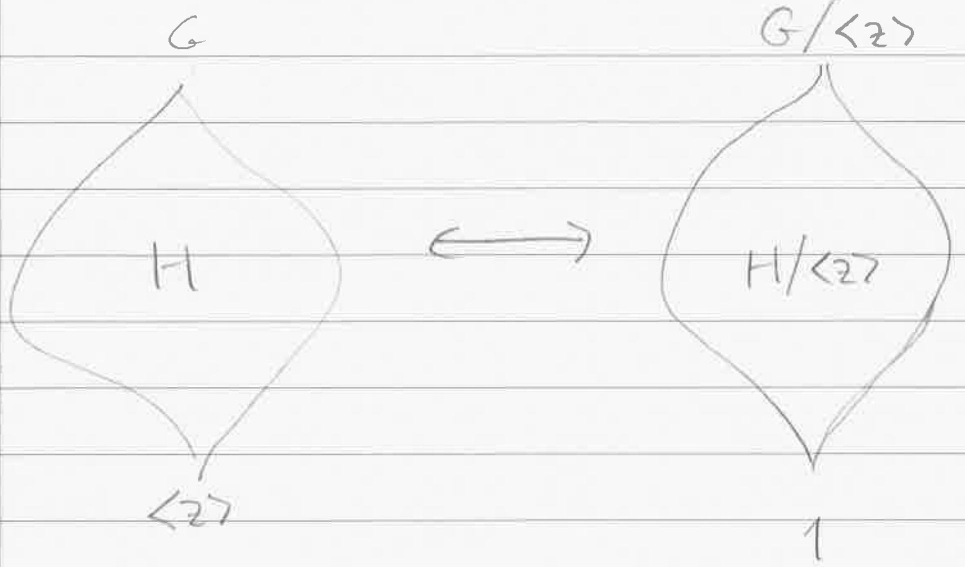
Now consider the group $\langle z \rangle \leq G$ with $|\langle z \rangle| = p$. Since $z \in Z(G)$ we have $\langle z \rangle \trianglelefteq G$ and then

$$p^{n-1} \mid |G/\langle z \rangle| = |G|/p.$$

By induction, $G/\langle z \rangle$ has subgroups of size p^m for all $1 \le m \le n-1$.

By the correspondence theorem, every subgroup of $G/\langle z \rangle$ has the form $H/\langle z \rangle$ for some subgroup

$$\langle z \rangle \le H \le G.$$



Finally, note that

$$p^m = |H/\langle z \rangle| \iff |H| = p^{m+1},$$

so G has subgroups of size p^m for all $1 \le m \le n$.

//

Remark: Note that we only used the abelian version of Cauchy's Theorem in this proof. So maybe I was just wasting your time when we proved Cauchy's Theorem. Or maybe there was some pedagogical reason to do it.

We have shown that Sylow p-subgroups exist. Our next job is to investigate how G acts on its p-subgroups by conjugation.

The main tool will be *double cosets*.

(Nothing is wasted.)

11/19/15

HW4 due Thurs Dec 3

Last time we proved Sylow ① :

If $|G| = p^{\alpha} m$ with $\gcd(p, m) = 1$, then G has subgroups of order p^{β} for all $1 \leq \beta \leq \alpha$. ///

The subgroups of size p^{α} are called Sylow p-subgroups. Let $\mathrm{Syl}_p(G)$ be the set of these. Now suppose that

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

where $p_1, p_2, \ldots, p_n$ are distinct primes and for each p_i choose a Sylow p_i-subgroup $P_i \in \mathrm{Syl}_{p_i}(G)$. Then it is possible to express G as some kind of product

$$G = \text{``} P_1 P_2 P_3 \cdots P_n \text{''}$$

but it is not clear what kind of product this is because the partial products $P_i P_j$ might not be subgroups.

However, if $G = A$ is abelian then every Sylow subgroup is normal and we can express A as a direct product

$$A = P_1 \times P_2 \times P_3 \times \cdots \times P_4 .$$

This is called the primary decomposition of a finite abelian group.

We will see today that the primary decomposition is unique because there exists a unique Sylow p_i-subgroup for each prime $p_i \mid |A|$.

Our goal is to prove the remaining pieces of Sylow's Theorem.

(2) If $P \in Syl_p(G)$ and if Q is any p-subgroup then $\exists \ g \in G$ such that

$$gQg^{-1} \subseteq P$$

(3) $|Syl_p(G)| = 1 \mod p$

& $|Syl_p(G)| \Bigm| m$, where $|G| = p^\alpha m$.

Our tool will be the action of G on its subgroups by conjugation.

☆ Definition: Let G be a group and define an action $G \circlearrowright \mathcal{L}(G)$ by

$$G \times \mathcal{L}(G) \longrightarrow \mathcal{L}(G)$$

$$(g, H) \longmapsto gHg^{-1}.$$

Observe that $H \trianglelefteq G$ if and only if

$$\mathrm{Stab}_G(H) = \{ g \in G : gHg^{-1} = H \} = G.$$

For a general subgroup $H \in \mathcal{L}(G)$ we define its normalizer

$$N_G(H) := \mathrm{Stab}_G(H)$$

This is the largest subgroup of G in which H is normal. In other words, if $K \leq G$ is a subgroup such that $H \trianglelefteq K$ then we must have $K \leq N_G(H)$.

///

Proof of Sylow (2) :

Let $|G| = p^\alpha m$ with $\gcd(p, m) = 1$. Let $P, Q \leq G$ be subgroups with $|G| = p^\alpha$ and $|Q| = p^\beta$ for some $1 \leq \beta \leq \alpha$.

Consider the decomposition of G into double cosets

$$G = \bigsqcup_i P g_i Q .$$

Recall from last week that we proved

$$|P x_i Q| = \frac{|P| \cdot |Q|}{|P \cap g_i Q g_i^{-1}|}$$

so we have

$$|G| = \sum_i \frac{|P| \cdot |Q|}{|P \cap g_i Q g_i^{-1}|} \tag{$*$}$$

Assume for contradiction that

$$P \cap g_i Q g_i^{-1} \subsetneq g_i Q g_i^{-1}$$

for all i, so that

$$|P \cap g_i Q g_i^{-1}| < |g_i Q g_i^{-1}| = |Q| = p^{\beta}.$$

The intersection of p-groups is a p-group so we have

$$|P \cap g_i Q g_i^{-1}| = p^{\gamma_i} \quad \text{with} \quad \gamma_i < \beta$$

for all i. But then

$$\frac{|P|\cdot|Q|}{|P \cap g_i Q g_i^{-1}|} = \frac{p^{\alpha}\cdot p^{\beta}}{p^{\gamma_i}} = p^{\alpha+(\beta-\gamma_i)}$$

is divisible by $p^{\alpha+1}$ for all i and from ⊛ we conclude that $p^{\alpha+1} \mid |G|$.

Contradiction.

We conclude that there exists $g_i \in G$ such that

$$P \cap g_i Q g_i^{-1} = g_i Q g_i^{-1},$$

hence $g_i Q g_i^{-1} \subseteq P$.

///

[I once had a professor who called this a "sleazy" proof. I don't know what he meant by that.]

Remarks:

- Sylow ② implies that every p-subgroup is contained in a Sylow p-subgroup.

Proof: $gQg^{-1} \leq P \Rightarrow Q \leq g^{-1}Pg$. ///

Thus the concept of "Sylow p-subgroup" is the same as "maximal p-subgroup".

- It also implies that any two Sylow p-subgroups are conjugate.

Proof: $gQg^{-1} \leq P$ and $|gQg^{-1}| = |P|$ imply that $gQg^{-1} = P$. ///

If G is abelian (hence every subgroup is normal) this implies that there is a unique Sylow p-subgroup for each prime $p \mid |G|$. This proves the uniquess of the primary decomposition.

Proof of Sylow ③ :

Let $|G| = p^\alpha m$ with $\gcd(p, m) = 1$. Now consider the conjugation action $G \circlearrowright \mathcal{L}(G)$ restricted to the set of Sylow p-subgroups:

$$G \circlearrowright \mathrm{Syl}_p(G).$$

By Sylow ② we know that this action is transitive, so for all $P \in \mathrm{Syl}_p(G)$ we have a bijection

$$\mathrm{Syl}_p(G) = \mathrm{Orb}_G(P) \longleftrightarrow G/N_G(P)$$

and hence

$$|\mathrm{Syl}_p(G)| = \frac{|G|}{|N_G(P)|}$$

Since $P \subseteq N_G(P)$ has order p^α, Lagrange tells up that $p^\alpha \mid |N_G(P)|$, say

$$|N_G(P)| = p^\alpha n.$$

↓

Then we have

$$|\mathrm{Syl}_p(G)| = \frac{|G|}{|N_G(P)|} = \frac{\cancel{p^\alpha} m}{\cancel{p^\alpha} n} = \frac{m}{n} \;\Big|\; m .$$

///

To prove $|\mathrm{Syl}_p(G)| = 1 \bmod p$ we need a lemma.

Lemma: Let $P, Q \in \mathrm{Syl}_p(G)$. Then we have

$$P \le N_G(Q) \iff P = Q .$$

Proof: Suppose that $P \le N_G(Q)$. This implies that the product set PQ is a subgroup of G and hence $|PQ|$ divides $|G|$. But note that

$$|PQ| = \frac{|P|\cdot|Q|}{|P\cap Q|} = p^{2\alpha-\beta}$$

where $|P\cap Q| = p^\beta$ for some $0 \le \beta \le \alpha$. If $\beta < \alpha$ then we conclude that $|PQ|$ and hence $|G|$ is divisible by $p^{\alpha+1}$. Contradiction. This implies that $|P\cap Q| = p^\alpha$ and hence

$$P = P\cap Q = Q .$$

///

Finally, let $P \in Syl_p(G)$ and consider the action of P on $Syl_p(G)$ by conjugation. We obtain an orbit decomposition

$$Syl_p(G) = \bigsqcup_i Orb_p(Q_i).$$

By orbit-stabilizer we have

$$|Orb_p(Q_i)| = \frac{|P|}{|Stab_p(Q_i)|} = p^{\gamma_i}$$

for some $0 \leq \gamma_i \leq \alpha$. Furthermore, we have

$$\begin{aligned} \gamma_i = 0 &\iff |Orb_p(Q_i)| = 1 \\ &\iff gQ_ig^{-1} = Q_i \quad \forall g \in P \\ &\iff P \leq N_G(Q_i) \\ &\iff P = Q_i. \qquad \text{(lemma)}. \end{aligned}$$

We conclude that

$$\begin{aligned} |Syl_p(G)| &= 1 + \sum_{Q_i \neq P} |Orb_p(Q_i)| \\ &= 1 \bmod p. \end{aligned}$$

QED.

On Tuesday we applied Sylow's Theorem to show that a group of size pqr is not simple. Now let's look at some more applications.

☆ Theorem: If $|G| = p^\alpha$, $\alpha \geq 2$, then G is not simple.

Proof: If G is abelian then Sylow (1) gives a subgroup of order p which must be normal. So assume that G is non-abelian, i.e., $1 \subseteq Z(G) \underset{\neq}{\trianglelefteq} G$. Then since $p \mid |G|$ and $p \mid |G|/|Z_i|$ for all Z_i, the class equation says that $p \mid |Z(G)|$, hence $1 \subsetneq Z(G)$.

///

☆ Theorem: Let $|G| = p^\alpha m$ with $m > 1$ and $\gcd(p,m) = 1$. If m has <u>no</u> divisor $d \mid m$ such that

- $d \neq 1$
- $d = 1 \bmod p$

then G is <u>not</u> simple.

Proof: By Sylow ③ we have $|\mathrm{Syl}_p(G)| \mid m$ and $|\mathrm{Syl}_p(G)| = 1 \bmod p$. By assumption this implies that $|\mathrm{Syl}_p(G)| = 1$, so G has a unique Sylow p-subgroup which is normal by part ②. Finally, since $m > 1$ this subgroup is proper. ///

☆ Theorem: Let $p < q$ be prime.

- If $q \neq 1 \bmod p$ then

  $|G| = pq \implies G$ is cyclic.

- If $q = 1 \bmod p$ then there are exactly two groups of size pq: one cyclic and one non-abelian.

Proof sketch: Let $n_q = |\mathrm{Syl}_q(G)|$ and $n_p = |\mathrm{Syl}_p(G)|$. Sylow ③ says

$$n_q \mid p \;\; \& \;\; n_q = 1 \bmod q.$$

Since $p < q$, this implies $n_q = 1$.

Hence we obtain a normal Sylow q-subgroup

$$Q \approx \mathbb{Z}/q\mathbb{Z}.$$

We also have $n_p \mid q$ and $n_p = 1 \mod p$.

- If $q \neq 1 \mod p$ this implies that $n_p = 1$ and we obtain a normal Sylow p-subgroup

$$P \approx \mathbb{Z}/p\mathbb{Z}.$$

Since $|G| = |P| \cdot |Q|$ with P & Q both normal we have

$$G = P \times Q.$$

Furthermore, if $P = \langle x \rangle$ & $Q = \langle y \rangle$ then we have

$$\begin{aligned} \operatorname{ord}_G(x,y) &= \operatorname{lcm}(\operatorname{ord}_P(x), \operatorname{ord}_Q(y)) \\ &= pq, \end{aligned}$$

hence $G = \langle (x,y) \rangle$ is cyclic. ///

- If $q = 1 \mod p$ then we may have $n_p = 1$ (in which case G is again cyclic) or we may have $n_p = q$.

In the second case, let $P \approx \mathbb{Z}/p\mathbb{Z}$ be <u>any</u> Sylow p-subgroup. Then we have

$$G = P \ltimes_\varphi Q$$

where the action $\varphi : P \to \mathrm{Aut}(Q)$ is by conjugation. We know that φ is not trivial because $n_p = q \neq 1$ implies that P is <u>not</u> normal.

What could φ be? Recall that

$$\mathrm{Aut}(Q) = \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/q\mathbb{Z})^\times,$$

which is a group of size $q-1$. In fact, the "primitive root theorem" [proof omitted] says that

$$(\mathbb{Z}/q\mathbb{Z})^\times \approx \mathbb{Z}/(q-1)\mathbb{Z}.$$

Now let $P = \langle x \rangle$ and consider any two nontrivial automorphisms

$\varphi_1, \varphi_2 : P \to \mathrm{Aut}(Q)$.

By assumption $\ker\varphi_1, \ker\varphi_2 \neq P$. Since $|P|$ is prime this implies $\ker\varphi_1 = \ker\varphi_2 = 1$, hence

$$|\varphi_1(P)| = |\varphi_2(P)| = p.$$

Since $\mathrm{Aut}(Q)$ is cyclic it has a unique subgroup of order p which is also cyclic, hence

$$\varphi_1(P) = \varphi_2(P) = \langle \varphi_1(x) \rangle = \langle \varphi_2(x) \rangle.$$

Let $\varphi_1(x) = \varphi_2(x)^m$. Then the map

$$\begin{aligned} \theta : P &\longrightarrow P \\ x &\longmapsto x^m \end{aligned}$$

is a group automorphism. Finally, one can use the fact $\varphi_1 = \theta \circ \varphi_2$ to prove that

$$P \ltimes_{\varphi_1} Q \approx P \ltimes_{\varphi_2} Q.$$

Remarks :

- Let q be an odd prime. Then the unique nonabelian group of size $2q$ is the dihedral group.

- Is there an explicit description of the nonabelian group for general $p < q$ with $q \equiv 1 \bmod p$?

  Yes. Think of $\mathbb{Z}/q\mathbb{Z}$ as a one-dimensional vector space and consider the "general affine" group $GA(\mathbb{Z}/q\mathbb{Z})$ as in HW4 Problem 3. We can view this as a matrix group

$$GA(\mathbb{Z}/q\mathbb{Z}) = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x, y \in \mathbb{Z}/q\mathbb{Z},\ x \neq 0 \right\}$$

  The unique nonabelian group of order pq is isomorphic to the subgroup

$$\left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in GA(\mathbb{Z}/q\mathbb{Z}) : x^p = 1 \right\}.$$