7202 Algebra 4: Groups and Rings Notes

Based on the 2013 spring lectures by Prof F E A Johnson

MATH7202 – Groups and Rings.

8 January 2013
Prof FEA JOHNSON
Roberts G06.

The conventional definition of a group is $G=(G,\cdot,e)$ s.t. G is a set, $\cdot: G\times G\to G$, $\cdot(g,h)=g\cdot h$ that satisfies the following axioms:

(I) $g\cdot(h\cdot k)=(g\cdot h)\cdot k\ \forall g,h,k\in G$ (II) $g\cdot e=e\cdot g=g\ \forall g\in G$ (III) $\forall g\in G\ \exists g^{-1}\in G$ s.t. $g\cdot g^{-1}=g^{-1}\cdot g=e$

We also know, as a consequence of the axioms, that $(g\cdot h)^{-1}=h^{-1}\cdot g^{-1}$. Furthermore, if G satisfies $\forall g,h\in G$, $g\cdot h=h\cdot g$ then G is said to be abelian.

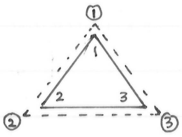
In practice, we do not write groups this way however. We either have the multiplicative convention, or (only in the abelian case) occasionally we use additive convention.

Multiplicative: Instead of e, write 1. Then $(G,\cdot,1)$ is a group, $g\cdot g^{-1}=1=g^{-1}\cdot g$.

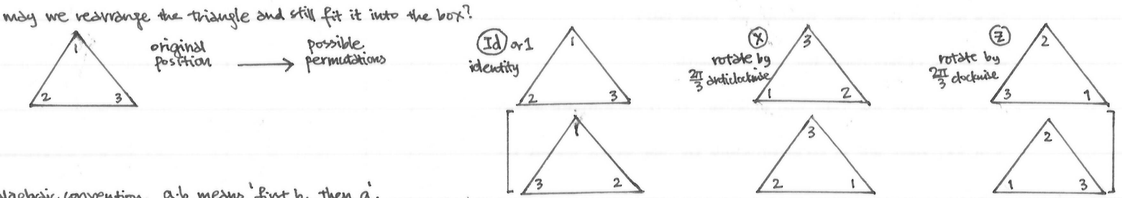
Additive: Instead of $\cdot$ write $+$, of e write 0, of g^{-1} write $-g$. Then $g+(h+k)=(g+h)+k$, $g+0=0+g=g$, $\forall g\ \exists -g$ s.t. $g+(-g)=0$.

Most groups arise as symmetry groups (algebraic or geometric).

For example, C_3 is the symmetry group of a "1-sided equilateral triangle". Imagine such a triangle in a slightly larger box of the same shape. Label the vertices of the triangle i, and the vertices of the box ⓘ, as seen in the diagram.



How may we rearrange the triangle and still fit it into the box?



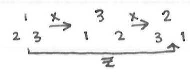
these are NOT symmetries of the 1-sided triangle, as they are unattainable without flipping. These are discussed further later below.

By algebraic convention, $a\cdot b$ means 'first b, then a'.

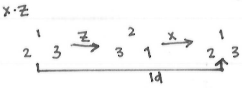
We draw up a table of operations as follows:

C_3	1	x	z
1	1	x	z
x	x	z	1
z	z	1	x

$x\cdot x=z$



$x\cdot z$



This verifies that this is a group – every element has an inverse, 1 is the identity element.

However, here we have unnecessary terms, as $z=x\cdot x$, we can rewrite it by eliminating z, instead putting $z=x^2$. Then

	1	x	x^2
1	1	x	x^2
x	x	x^2	x
x^2	x^2	1	1

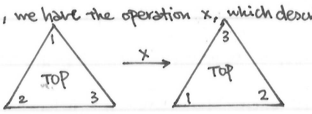
and $x^3=x\cdot x^2=1$.

This is a tedious way of describing C_3. Instead, we can describe it simply as follows: $C_3=\{1,x,x^2\}$, $x^3=1$; or conventionally, $C_3=\langle x\mid x^3=1\rangle$.

There is a generator x, and a relation $x^3=1$. C_3 is the symmetry group of a 1-sided equilateral triangle.

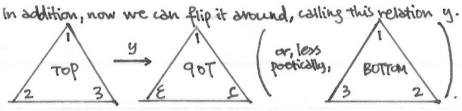
Generalisation: Symmetries of a 2-sided equilateral triangle. Once again we have a box into which we have a triangle. However, now we have a top and bottom side.

As before, we have the operation x, which describes rotation by $\frac{2\pi}{3}$ anticlockwise.



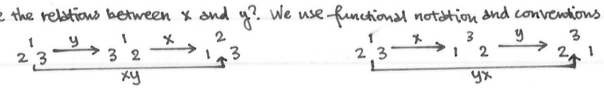
and $x^3=1$.

In addition, now we can flip it around, calling this relation y.



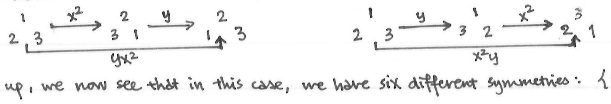
Naturally, $y^2=1$.

What are the relations between x and y? We use functional notation and conventions.



Clearly, $xy\neq yx$. Then what does yx equal? or xy?

We note that:



So we see that $x^2y=yx$, $xy=yx^2$.

Counting up, we now see that in this case, we have six different symmetries: $\{1,x,x^2,y,xy,x^2y\}$ where $xy=yx^2$, $x^2y=yx$.

We can thus write out the multiplication table for this symmetry group:

D_6	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

This group of symmetries is called D_6, which denotes the dihedral group of order 6; giving the group of symmetries of a two-sided equilateral 3-gon (triangle).

Note that we perform the column operation first, then the row. i.e.

$x \to xy$ (y first, then x)

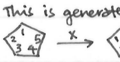
$x^2y\to x^2y\cdot xy=x^2(yx)y=x^2x^2yy=x^4=x$.

A word on notation. $C_3=\{1,x,x^2\}$, $x^3=1=\langle x\mid x^3=1\rangle$. $D_6=\{1,x,x^2,y,xy,x^2y\}$, $x^3=1$, $y^2=1$, $yx=x^2y=\langle x,y\mid x^3=1,\ y^2=1,\ yx=x^2y\rangle$.

In the latter case, we have two generators and three relations. Notice the ease of algebraic generalisation compared to geometric intuition.

We can generalise this to general polygons, e.g. C_n = symmetry of 1-sided regular n-gon. This is generated by x = rotation anticlockwise through $\frac{2\pi}{n}$.

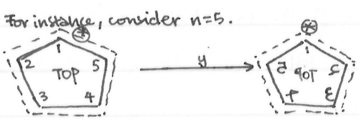
Then $C_n=\{1,x,\dots,x^{n-1}\}$, $x^n=1=\langle x\mid x^n=1\rangle$. e.g. for a pentagon, $n=5$.



(by convention, anti-clockwise).

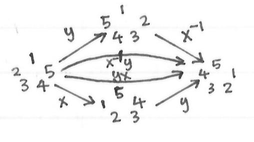
D_{2n} = symmetry of 2-sided n-gon. In addition to generator x = rotation through $\frac{2\pi}{n}$ anticlockwise, we have generator y = flip about specific vertex.

For instance, consider $n=5$.



And $y^2=1$. Again, $yx\neq xy$. In general $yx=x^{-1}y$.

since $x^n=1$, $x^{n-1}=x^{-1}$ so $yx=x^{n-1}y$.



Hence, generally, $D_{2n} = \{1, x, x^2, \cdots, x^{n-1}, y, xy, \cdots, x^{n-1}y\}$, where terms are of form $x^a y^b$, $0 \leq a \leq n-1$, $0 \leq b \leq 1$.

The group has relations $x^n = 1$, $y^2 = 1$, $yx = x^{n-1}y$. i.e. $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, yx = x^{n-1}y \rangle$.

The groups D_{2n} ($n \geq 3$) are non-abelian, the groups C_n are abelian. We zoom in and focus on the group C_2: $C_2 = \{1, x\}$, $x^2 = 1$.

Under the standard multiplicative convention,

$\cdot$	1	x
1	1	x
x	x	1

. We can also use additive convention as group is abelian:

$+$	0	x
0	0	x
x	x	0

.

We move on to another example, Q_8. This is the quaternion group of order 8, discovered by Hamilton.

To motivate this, imagine the complex numbers: $i^2 = -1$, $\{1, i, i^2, i^3\}$, $i^4 = 1$. This is a clear example of C_4, generated by i.

The quaternion group is an extension of the complex numbers, with generators $1, i, j, k$. Its elements are $\{1, -1, i, -i, j, -j, k, -k\}$, and is governed by the following rules: $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$

i k j +ve i k j -ve.

$\cdot$ Q_8	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Q_8 is a non-abelian group of order 8. We know that D_8 is also a non-abelian group of order 8.

They are not the same. How do we know this?

Look at the entries down the main diagonals.

- In Q_8, there are only two elements $(1, -1)$ which are self-inverse.
- In D_8, there are six elements which are self-inverse (all but x, x^3).

$\cdot$ D_8	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1							
x		x^2						
x^2			1					
x^3				x^2				
y					1			
xy						1		
x^2y							1	
x^3y								1

$\therefore$ Q_8 and D_8 are "essentially different." i.e. not isomorphic.

Definition G is a finite group. If $g \in G$, the order of g, $\mathrm{ord}(g) = \min\{n \geq 1 \mid g^n = 1\}$. By convention, $g^0 = 1$.

11 January 2013
Prof FEA JOHNSON
Roberts 106.

We say that two sets X, Y are equivalent (as sets) when there exists a bijective mapping $f: X \to Y$.

Definition Let $G = (G, *, e)$, $H = (H, \circ, E)$ be groups. We say that G and H are isomorphic when $\exists$ bijective mapping $\alpha: G \to H$ which preserves multiplication in the sense that $\boxed{\alpha(g_1 * g_2) = \alpha(g_1) \circ \alpha(g_2)}$.

Definition Let $G = (G, *, e)$, $H = (H, \circ, E)$ be groups. By a group homomorphism, we mean a mapping $\alpha: G \to H$, which satisfies the above condition $\alpha(g_1 * g_2) = \alpha(g_1) \circ \alpha(g_2)$ $\forall g_1, g_2 \in G$ (need not be bijective!)

e.g. Take $\mathbb{R} = (\mathbb{R}, +, 0)$ be the additive group of real numbers, $\mathbb{R}_> = (\mathbb{R}_>, \cdot, 1)$ be the multiplicative group of real positive numbers (i.e. $\mathbb{R}_> = \{x \in \mathbb{R} : x > 0\}$.

Then the groups are isomorphic, as $\exp: \mathbb{R} \to \mathbb{R}_>$ with $\exp(x) = \sum_{r \geq 0}^{\infty} \frac{x^r}{r!}$, $\exp(x+y) = \exp(x)\exp(y)$.

Hence $\mathbb{R}$ is isomorphic to $\mathbb{R}_>$, i.e. $\mathbb{R} \cong \mathbb{R}_>$. Of course, exp is bijective, so there is an inverse $\log: \mathbb{R}_> \to \mathbb{R}$, $\log(x) = \int_1^x \frac{dt}{t}$.

e.g. the sign of a permutation. Recall $\sigma_n = \{f : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}\}$, f is a bijective permutation on n letters.

We claim that σ_n is a group with respect to composition, since if $f, g \in \sigma_n$, then $f \circ g \in \sigma_n$, $f^{-1} \in \sigma_n$, Id is an identity element as $\mathrm{Id} \circ f = f \circ \mathrm{Id} = f$.

The sign: $\sigma_n \to \{+1, -1\} \cong C_2$. We see that $\mathrm{sign}(f \circ g) = \mathrm{sign}(f)\,\mathrm{sign}(g)$, and hence sign is a group homomorphism.

Elementary properties of homomorphisms

Let $G = (G, \cdot, 1_G)$, $H = (H, \cdot, 1_H)$ be groups, and $\varphi: G \to H$ be a homomorphism. Then

i) $\varphi(1_G) = 1_H$ and ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$.

We prove these quickly: i) $1_G = 1_G \cdot 1_G \Rightarrow \varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G) \in H$. So, $\varphi(1_G)\varphi(1_G)^{-1} = \varphi(1_G)\varphi(1_G)\varphi(1_G)^{-1} \Rightarrow 1_H = \varphi(1_G) \cdot 1_H = \varphi(1_G)$// q.e.d.

ii) Take any $g \in G$, then $g \cdot g^{-1} = 1_G$, then $\varphi(g \cdot g^{-1}) = \varphi(1_G) \Rightarrow \varphi(g)\varphi(g^{-1}) = 1_H$. But also, $\varphi(g)\varphi(g)^{-1} = 1_H$, so $\varphi(g)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1}$

Multiply on left by $\varphi(g)^{-1}$, and thus, $\varphi(g)^{-1}\varphi(g)\varphi(g^{-1}) = \varphi(g)^{-1}\varphi(g)\varphi(g)^{-1} \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$// q.e.d.

e.g. $\exp: \mathbb{R} \to \mathbb{R}_{>0}$. Then i) $\exp(0) = 1$ (identity maps to identity), and ii) $\exp(-x) = \exp(x)^{-1} = \frac{1}{\exp(x)}$ (inverse maps to inverse).

Hence, we have a principle for classifying groups:

- To show that two groups are isomorphic, we need to construct an isomorphism.
- Suppose two groups are not isomorphic, is there any quick way of seeing this? Consider the order of $g \in G$.

Recall that if $G = (G, \cdot, 1)$ is a group, then if $g \in G$, order of g, $\mathrm{ord}(g) = \min\{r \geq 1 : g^r = 1\}$. (or $\mathrm{ord}(g) = \infty$ if $g^r \neq 1$ $\forall r \geq 1$).

e.g. $G = D_6 = \{1, x, x^2, y, xy, x^2y\}$ $x^3 = 1$, $y^2 = 1$, $yx = x^2y$. Then $\mathrm{ord}(1) = 1$ $\because 1^1 = 1$. $\mathrm{ord}(x) = 3$, $\mathrm{ord}(x^2) = 3$. $\because x^2, (x^2)^2 \neq 1, (x^2)^3 = 1$.

$\mathrm{ord}(y) = 2$, $\mathrm{ord}(xy) = 2$ $\because (xy)^2 = xyxy = x(x^2y)y = x^3y^2 = 1$, $\mathrm{ord}(x^2y) = 2$.

F202-07

Ex. Find the order of all elements in C_8.

Soln. $C_8 = \{1, x, x^2, \dots, x^7\}$. $\mathrm{ord}(1) = 1$, $\mathrm{ord}(x) = 8$, $\mathrm{ord}(x^2) = 4$, $\mathrm{ord}(x^3) = 8$, $\mathrm{ord}(x^4) = 2$, $\mathrm{ord}(x^5) = 8$, $\mathrm{ord}(x^6) = 4$, $\mathrm{ord}(x^7) = 8$.

Note: observe that $\mathrm{ord}(x^r) = \frac{8}{\gcd(8,r)}$.

Consider $C_n = \{1, x, \dots, x^{n-1}\}$, $x^n = 1$.

Proposition Suppose $x^N = 1$ where $N \geq 1$, then N is a multiple of n (i.e. $N = nk$ for some k).

Proof – clearly $n \leq N$; because $1, x, \dots, x^{n-1}$ are distinct. Use the division algorithm to write $N = nk + r$, $0 \leq r \leq n-1$. Then we have $x^N = x^{nk+r} = (x^n)^k x^r$.

Since $x^n = 1$, then $x^N = 1^k x^r = x^r$, and we know $x^N = 1$, so $x^r = 1$. Since $0 \leq r \leq n-1$, $r = 0 \Rightarrow N = nk + 0 = nk$ q.e.d.

Corollary $C_n = \{1, x, \dots, x^{n-1}\}$, $x^n = 1$. Then $\mathrm{ord}(x^r) = \frac{n}{\gcd(n,r)} = \frac{n}{\mathrm{hcf}(n,r)}$.

Proof – Suppose $(x^r)^t = 1$, so $x^{rt} = 1 \Rightarrow rt$ is a multiple of n. Put $t = \mathrm{ord}(x^r)$. Then $n \mid rt$ and obviously $r \mid rt$; and rt is a common multiple of n and r.

For r fixed, t is minimal when rt is minimised. Hence, $rt = \mathrm{lcm}(n,r) = \frac{nr}{\mathrm{hcf}(n,r)} \Rightarrow t = \frac{n}{\mathrm{hcf}(n,r)}$ q.e.d.

Examine all homomorphisms $\varphi: C_n \to C_n$, i.e. consider all mappings $\varphi: \{1, 2, \dots, x^{n-1}\} \to \{1, 2, \dots, x^{n-1}\}$ which preserve multiplication i.e. $\varphi(x^s x^t) = \varphi(x^s)\varphi(x^t)$.

Let r be an integer s.t. $0 \leq r \leq n-1$. Define $\varphi_r: C_n \to C_n$ by $\varphi_r(x^s) = x^{rs}$.

Proposition $\varphi_r: C_n \to C_n$ is a homomorphism.

Proof – $\varphi_r(x^s) = x^{rs}$, $\varphi_r(x^t) = x^{rt}$. Then $\varphi_r(x^s x^t) = \varphi_r(x^{s+t}) = x^{r(s+t)} = x^{rs}x^{rt} = \varphi_r(x^s)\varphi_r(x^t)$.

Theorem Every homomorphism $\varphi: C_n \to C_n$ has the form $\varphi = \varphi_r$ for some r: $0 \leq r \leq n-1$.

Proof – Let $\varphi: C_n \to C_n$ be a homomorphism. Look at $\varphi(x)$ – $\varphi(x)$ must be of the form $\varphi(x) = x^r$ for some r: $0 \leq r \leq n-1$.

$\varphi(x^2) = \varphi(x)\varphi(x) = x^r x^r = x^{2r}$. Likewise, $\varphi(x^3) = \varphi(x^2)\varphi(x) = x^{2r}x^r = x^{3r}$. So in general, inductively, $\varphi(x^s) = x^{rs}$ as we have

$\left.\begin{array}{l}\varphi(x^{s-1}) = x^{r(s-1)} \\ \varphi(x) = x^r\end{array}\right\}$ $\varphi(x^s) = \varphi(x x^{s-1}) = \varphi(x)\varphi(x^{s-1}) = x^{rs}$. Hence, $\varphi = \varphi_r$ q.e.d.

The principle is thus: If you know the value of $\varphi(x)$, then you know the value of $\varphi(x^s)$ for any s. $\varphi(x^s) = \varphi(x)^s$.

Question: Which homomorphisms $\varphi_r: C_n \to C_n$ are bijective? Such a φ_r is then an isomorphism of C_n with itself.

Ex. Let $n = 6$ for C_n i.e. $\varphi: C_6 \to C_6$. $C_6 = \{1, x, \dots, x^5\}$ $x^6 = 1$. How many homomorphisms are there? How many isomorphisms?

Soln. By above, $\varphi = \varphi_r$ for some r: $0 \leq r \leq 5$. $\Rightarrow$ there are 6 homomorphisms $\varphi: C_6 \to C_6$.

Let $r = 0$, $\varphi_0(x^s) = x^{0s} = x^0 = 1$ (trivial homomorphism). $r = 1$, $\varphi_1(x^s) = x^s$. $\varphi_1(1) = 1$, $\varphi_1(x) = x$, $\varphi_1(x^2) = x^2, \dots, \varphi_1(x^5) = x^5$ (identity homomorphism).

$r = 2$: $\varphi_2(1) = 1$, $\varphi_2(x) = x^2$, $\varphi_2(x^2) = x^4$, $\varphi_2(x^3) = 1$, $\varphi_2(x^4) = x^2$, $\varphi_2(x^5) = x^4$. Hence, φ_2 is not surjective (no x in range) nor injective $\Rightarrow$ not isomorphism.

$r = 3$: $\varphi_3(1) = 1$, $\varphi_3(x) = x^3$, $\varphi_3(x^2) = 1$, $\varphi_3(x^3) = x^3$, $\varphi_3(x^4) = 1$, $\varphi_3(x^5) = x^3$. φ_3 is not bijective.

$r = 4$: $\varphi_4(1) = 1$, $\varphi_4(x) = x^4$, $\varphi_4(x^2) = x^2$, $\varphi_4(x^3) = 1$, $\varphi_4(x^4) = x^4$, $\varphi_4(x^5) = x^2$. φ_4 is not bijective.

$r = 5$: $\varphi_5(1) = 1$, $\varphi_5(x) = x^5$, $\varphi_5(x^2) = x^4$, $\varphi_5(x^3) = x^3$, $\varphi_5(x^4) = x^2$, $\varphi_5(x^5) = x$. φ_5 is bijective.

$\therefore$ isomorphisms (bijective homomorphisms) are φ_1 and φ_5 only.

In general, for C_n, $\varphi_r: C_n \to C_n$ is bijective $\Leftrightarrow \gcd(r, n) = 1$. We state this as a theorem.

Theorem $\varphi_r: C_n \to C_n$ is bijective $\Leftrightarrow \gcd(r,n) = 1$.

Proof – Since C_n is finite, then $\varphi_r: C_n \to C_n \Leftrightarrow \varphi_r: C_n \to C_n$ is surjective (forward by definition, backwards by finiteness and equality of domain & codomain)

$\varphi_r: C_n \to C_n$ is surjective $\Leftrightarrow \{\varphi_r(x)^t : 0 \leq t \leq n-1\} = C_n \Leftrightarrow \mathrm{ord}\,\varphi_r(x) = n \Leftrightarrow \frac{n}{\gcd(r,n)} = n \Leftrightarrow \gcd(r,n) = 1$ q.e.d.

15 January 2013.
Prof FEA JOHNSON
Roberts 406

Recall that if G, H are groups, by an isomorphism we mean a bijective homomorphism. If such φ exists we write $G \cong H$. $\varphi: G \xrightarrow{\simeq} H$.

Special case: $G = H$. Obviously $\mathrm{Id}_G: G \xrightarrow{\simeq} G$. An isomorphism $\alpha: G \xrightarrow{\simeq} G$ is called an <u>automorphism</u> of G. We denote $\boxed{\mathrm{Aut}(G) = \{\alpha: G \to G,\ \alpha \text{ is an automorphism}\}}$

Proposition $\mathrm{Aut}(G)$ forms a group in which

(i) group multiplication = composition of mapping, (ii) the group identity is Id_G.

Proof – First observe that if $\alpha, \beta \in \mathrm{Aut}(G)$, then $\alpha \circ \beta: G \to G$ is an automorphism. $\because \alpha, \beta$ bijective $\Rightarrow \alpha \circ \beta$ is bijective. We know that $\alpha \circ \beta$ is also a homomorphism: $(\alpha \circ \beta)(xy) = \alpha(\beta(xy)) = \alpha(\beta(x)\beta(y)) = \alpha(\beta(x))\,\alpha(\beta(y)) = (\alpha \circ \beta)(x)\,(\alpha \circ \beta)(y)$. This gives us a "multiplication" $\mathrm{Aut}(G) \times \mathrm{Aut}(G) \to \mathrm{Aut}(G)$,

$(\alpha, \beta) \mapsto \alpha\beta$. $\circ$ is associative as composition is always associative. Id_G acts as identity: $(\mathrm{Id}_G \circ \alpha)(x) = \mathrm{Id}_G(\alpha(x)) = \alpha(x)$, $\mathrm{Id}_G \circ \alpha = \alpha$.

Likewise, $\alpha \circ \mathrm{Id}_G = \alpha$. We just need to verify "inverses property". So let $\alpha \in \mathrm{Aut}(G) \Rightarrow \exists$ inverse mapping $\alpha^{-1}: G \to G$ as α is bijective.

We must show that α^{-1} is a homomorphism, i.e. NTP: $\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y)$. Apply α to both sides: $\alpha(\alpha^{-1}(xy)) = xy$, and

$\alpha(\alpha^{-1}(x)\alpha^{-1}(y)) = \alpha(\alpha^{-1}(x))\,\alpha(\alpha^{-1}(y)) = (\alpha\alpha^{-1})(x)(\alpha\alpha^{-1})(y) = xy$, so $\alpha[\alpha^{-1}(xy)] = \alpha[\alpha^{-1}(x)\alpha^{-1}(y)]$. α is injective, so $\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y) \Rightarrow \alpha^{-1} \in \mathrm{Aut}(G)$ q.e.d.

Here, we are taking a group and mapping it to another group: $G \to \mathrm{Aut}(G)$.

$\boxed{\text{Ex}}$ Calculate $\mathrm{Aut}(C_3)$.

Soln. $C_3 = \{1, x, x^2\}$. $x^3 = 1$. We have shown that there are three homomorphisms $\varphi: C_3 \to C_3$, namely $\varphi_r(x) = x^r$, $r = 0, 1, 2$.

$\varphi_0(x) = x^0 = 1 = \varphi_0(x^2) = \varphi_0(1) \Rightarrow \varphi_0$ is the trivial homomorphism, not bijective. $\varphi_1 = \mathrm{Id}$ $\because$ $\varphi_1(x) = x$, $\varphi_1(x^2) = x^2$, $\varphi_1(1) = 1 \Rightarrow$ bijective. Likewise, φ_2 is bijective.

$\varphi_2 \circ \varphi_2(x) = \varphi_2(x^2) = x^4 = x \Rightarrow \varphi_2 \circ \varphi_2 = \mathrm{Id}$. This gives us the following group multiplication table for $\mathrm{Aut}(C_3)$.

$\mathrm{Aut}(C_3)$	1	τ
1	1	τ
τ	τ	1

Take $\tau = \varphi_2$, $1 = \mathrm{Id}_{C_3}$, $\tau^2 = \varphi_2^2$. Hence, $\mathrm{Aut}(C_3) \cong C_2$ //

Note: this is analogous to complex numbers, where ω, ω^2 are third roots of unity, $\tau(\omega) = \omega^2$, and also complex conjugation.

$\boxed{\text{Ex}}$ Calculate $\mathrm{Aut}(C_5)$.

Soln. $C_5 = \{1, x, x^2, x^3, x^4\}$ $x^5 = 1$. Homomorphisms are $\varphi: C_5 \to C_5$, $\varphi_r(x) = x^r$, $r = 0, 1, 2, 3, 4$. i.e. $\varphi_r(a) = x^{ra}$. φ_0 is the trivial homomorphism, not bijective.

φ_r is bijective $\Leftrightarrow \gcd(r, 5) = 1$ $\therefore$ $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ are bijective. Thus, $\mathrm{Aut}(C_5) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$. $\varphi_1 = \mathrm{Id}$ (denote by 1), $\because \varphi_1(x) = x$, $\varphi_1(x^a) = x^a$.

$\varphi_2(x) = x^2$, $\varphi_2 \circ \varphi_2(x) = \varphi_2(\varphi_2(x)) = \varphi_2(x^2) = x^4 = \varphi_4(x) \Rightarrow \varphi_2 \circ \varphi_2 = \varphi_4$. $\varphi_2^2 = \varphi_4$. $\varphi_2^3(x) = \varphi_2 \circ \varphi_2 \circ \varphi_2(x)$, $\varphi_2(x^4) = x^8 = x^3 = \varphi_3(x)$, $\varphi_2^4 = \varphi_1 = \mathrm{Id}$.

We do up a multiplication table for $\mathrm{Aut}(C_5)$, taking $\alpha = \varphi_2$, $\alpha^2 = \varphi_4$, $\alpha^3 = \varphi_3$.

$\mathrm{Aut}(C_5)$	1	α	α^2	α^3
1	1	α	α^2	α^3
α	α	α^2	α^3	1
α^2	α^2	α^3	1	α
α^3	α^3	1	α	α^2

Hence, we have demonstrated that $\mathrm{Aut}(C_5) \cong C_4$.

We have shown that $\mathrm{Aut}(C_3) \cong C_2$, $\mathrm{Aut}(C_5) \cong C_4$. Is there a pattern?

$\boxed{\text{Ex}}$ Calculate $\mathrm{Aut}(C_9)$.

Soln. Homomorphisms $\varphi: C_9 \to C_9$ are of form $\varphi = \varphi_r$, $r = 0, 1, \ldots, 8$. φ_r is bijective $\Leftrightarrow \gcd(r, 9) = 1$. $r = 1, 2, 4, 5, 7, 8$. Then $\mathrm{Aut}(C_9) = \{\varphi_1, \varphi_2, \varphi_4, \varphi_5, \varphi_7, \varphi_8\}$

$\varphi_1 = \mathrm{Id}$. $\varphi_2^2 = \varphi_4$, $\varphi_2^3 = \varphi_8$, $\varphi_2^4 = \varphi_7$, $\varphi_2^5 = \varphi_5$, $\varphi_2^6 = \varphi_1 = \mathrm{Id}$. Then take $\alpha = \varphi_2$, $\mathrm{Aut}(C_9) = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$, $\alpha^6 = 1$.

Here, $\alpha = \varphi_2$, $\alpha^2 = \varphi_4$, $\alpha^3 = \varphi_8$, $\alpha^4 = \varphi_7$, $\alpha^5 = \varphi_5$, $\alpha^6 = 1$. $\mathrm{Aut}(C_9) \cong C_6$.

$\boxed{\text{Ex}}$ Calculate $\mathrm{Aut}(C_8)$.

Soln. Homomorphisms $\varphi: C_8 \to C_8$ are $\varphi_1, \varphi_3, \varphi_5, \varphi_7$. $\varphi_1 = \mathrm{Id}$. $\varphi_3^2 = \mathrm{Id}$, $\varphi_5^2 = \mathrm{Id}$, $\varphi_7^2 = \mathrm{Id}$.

$\mathrm{Aut}(C_8)$	Id	φ_3	φ_5	φ_7
Id	Id	φ_3	φ_5	φ_7
φ_3	φ_3	Id	φ_7	φ_5
φ_5	φ_5	φ_7	Id	φ_3
φ_7	φ_7	φ_5	φ_3	Id.

We plot out a multiplication table. Clearly, this group is not isomorphic to C_4 $\because$ every element $\alpha \in \mathrm{Aut}(C_8)$ satisfies $\alpha^2 = 1$, whereas C_4 has an element of order 4. Recall that if G, H are groups then $G \times H$ is a group.

Claim: $\mathrm{Aut}(C_8) \cong C_2 \times C_2$. First factor $C_2 = \{1, \alpha\}$, $\alpha^2 = 1$, second factor $C_2 = \{1, \beta\}$, $\beta^2 = 1$. Then elements are $C_2 \times C_2 = \{(1,1), (\alpha, 1), (1, \beta), (\alpha, \beta)\}$. Write down a multiplication table: as on right.

$C_2 \times C_2$	$(1,1)$	$(\alpha,1)$	$(1,\beta)$	(α,β)
$(1,1)$	$(1,1)$	$(\alpha,1)$	$(1,\beta)$	(α,β)
$(\alpha,1)$	$(\alpha,1)$	$(1,1)$	(α,β)	$(1,\beta)$
$(1,\beta)$	$(1,\beta)$	(α,β)	$(1,1)$	$(\alpha,1)$
(α,β)	(α,β)	$(1,\beta)$	$(\alpha,1)$	$(1,1)$.

Take $1 \mapsto (1,1)$, $\varphi_3 \mapsto (\alpha, 1)$, $\varphi_5 \mapsto (1, \beta)$, $\varphi_7 \mapsto (\alpha, \beta)$ under Ψ. Then Ψ is a homomorphism that preserves multiplication because of group structure (compare tables).

Overall, we have thus far: the following isomorphisms of automorphisms of cyclic groups: $\cong$

$\mathrm{Aut}(C_3)$	$\mathrm{Aut}(C_4)$	$\mathrm{Aut}(C_5)$	$\mathrm{Aut}(C_6)$	$\mathrm{Aut}(C_7)$	$\mathrm{Aut}(C_8)$	$\mathrm{Aut}(C_9)$
C_2	C_2	C_4	C_2	C_6	$C_2 \times C_2$	C_6.

The theory for finding $\mathrm{Aut}(C_n)$ for any n will be fleshed out further later into the course.

It is not in general true that $\mathrm{Aut}(C_n)$ is cyclic, but it is abelian:

$\boxed{\text{Proposition}}$ $\mathrm{Aut}(C_n)$ is abelian.

Proof – $\mathrm{Aut}(C_n) = \{\varphi_r : r \text{ coprime to } n\}$. Let $\varphi_r, \varphi_s \in \mathrm{Aut}(C_n)$; $C_n = \langle x \mid x^n = 1 \rangle$. Then $(\varphi_r \circ \varphi_s)(x) = \varphi_r(\varphi_s(x)) = \varphi_r(x^s) = \varphi_r(x)^s = (x^r)^s = x^{rs}$.

$(\varphi_s \circ \varphi_r)(x) = \varphi_s(\varphi_r(x)) = \varphi_s(x^r) = \varphi_s(x)^r = (x^s)^r = x^{rs} \Rightarrow \varphi_r \circ \varphi_s = \varphi_s \circ \varphi_r$ $\forall r, s$; so $\mathrm{Aut}(C_n)$ is abelian // q.e.d.

This is a very special result, as $\mathrm{Aut}(G)$ is, generally speaking, non-abelian. e.g. $\mathrm{Aut}(C_2 \times C_2)$ is non-abelian.

Observe too that $\mathrm{Aut}(C_2)$ is a special case due to its low order:

$\boxed{\text{Proposition}}$ $\mathrm{Aut}(C_2)$ is the trivial group.

Proof – $C_2 = \{1, x\}$, $x^2 = 1$. $\alpha: C_2 \to C_2$ is a bijective homomorphism $\Rightarrow \alpha(1) = 1$, $\alpha(x) = x \Rightarrow \alpha = \mathrm{Id}$ is the only element $\Rightarrow \mathrm{Aut}(C_2)$ is a trivial group // q.e.d.

Review of Lagrange's Theorem:

Take G to be a finite group. $H \subset G$ is a subgroup of G if H is itself a group (i.e. $1_G \in H$; $x, y \in H \Rightarrow xy \in H$; $x \in H \Rightarrow x^{-1} \in H$).

For example, if $G = D_6 = \{1, x, x^2, y, xy, x^2y\}$ $x^3 = y^2 = 1$, $yx = xy^2$; then $X = \{1, x, x^2, y\} \subset D_6$ but X is not a subgroup.

$\boxed{\text{Theorem}}$ (Lagrange's Theorem).

If G is a finite group and $H \subset G$ is a subgroup, then $|H|$ divides $|G|$ exactly.

Proof – If $g \in G$, define the left coset of H by g, $gH = \{gh : h \in H\}$. (e.g. $G = D_6$, $H = \{1, y\}$ is a subgroup. $1 \cdot H = \{1, y\}$, $xH = \{x, xy\}$, $x^2H = \{x^2, x^2y\}$, $yH = \{y, 1\}$, $xyH = \{xy, x\}$ $x^2yH = \{x^2y, x^2\}$ two cosets).

We will show that $|G| = n|H|$, where n is the number of distinct cosets. We claim that $\exists$ a bijective mapping $H \to gH$.

In particular, this implies that $|gH| = |H|$. Let $\lambda g: H \to gH$ by $\lambda g(h) = gh$. λg is well-defined, and by definition λg is surjective. 18 January 2013 Prof FEA JOHNSON Roberts 106.

If $\lambda g(h_1) = \lambda g(h_2)$, then $gh_1 = gh_2$. Left-multiply by g^{-1} to get $h_1 = h_2 \Rightarrow \lambda g$ is injective $\Rightarrow \lambda g$ is bijective $\Rightarrow$

$\lambda g: H \to gH$ is bijective and $|gH| = |H|$. It is possible that $gH = g'H$ but $g \neq g'$ i.e. same coset may be represented in different ways.

We obtain a rule of equality for left cosets: If $H \subset G$ is a subgroup, $g_1 H = g_2 H \Leftrightarrow g_2^{-1} g_1 \in H$. We prove this claim:

($\Rightarrow$): Suppose $g_1 H = g_2 H$. Clearly, $g_2 \in g_2 H$ $\because$ $1 \in H$, $g_2 = g_2 \cdot 1$. Then $g_2 \in g_1 H \Rightarrow \exists h \in H$ s.t. $g_2 = g_1 h \Rightarrow g_2^{-1} g_2 = g_2^{-1} g_1 h \Rightarrow 1 = (g_2^{-1} g_1) h$; $h^{-1} = g_2^{-1} g_1$

$h^{-1} \in H \Rightarrow g_2^{-1} g_1 \in H$.

($\Leftarrow$): Suppose $g_2^{-1} g_1 \in H$. Then $g_2^{-1} g_1 = h \in H$. Then $g_1 = g_2 H$ and $g_1 \in g_2 H$. Let $h' \in H$, then $g_1 h' = g_2 h h'$. $hh' \in H$, so $g_1 h' \in g_2 H \Rightarrow g_1 H \subset g_2 H$

but $|g_1 H| = |g_2 H| = |H|$, so $g_1 H = g_2 H$. (We avoid working with right cosets, but corresponding law of equality is $Hg_1 = Hg_2 \Leftrightarrow g_2 g_1^{-1} \in H$).

We introduce another claim — Let G be a group, $H \subset G$ be a subgroup. Let $g_1, g_2 \in G$, then either (i) $g_1 H = g_2 H$ or (ii) $(g_1 H) \cap (g_2 H) = \phi$.

By our earlier statement, it suffices to show that if $(g_1 H) \cap (g_2 H) \neq \phi$, then $g_1 H = g_2 H$. So suppose $\exists z \in (g_1 H) \cap (g_2 H)$. Then $z = g_1 h_1 = g_2 h_2$.

Then $g_2^{-1} g_1 = h_2 h_1^{-1}$. Naturally, $h_2 h_1^{-1} \in H$, so $g_2^{-1} g_1 \in H \Rightarrow$ from previous claim, $g_1 H = g_2 H$.

We list the distinct left cosets of H, in such a way that each coset is listed exactly once: $\gamma_1 H, \gamma_2 H, \dots, \gamma_m H$. Every $g \in G$ belongs to some coset $\because$ $g \in gH$.

i.e. $\forall g \in G$, $\exists i$ s.t. $g \in \gamma_i H$. Then $G = \gamma_1 H \cup \gamma_2 H \cup \dots \cup \gamma_m H$. Also, $\gamma_i H \cap \gamma_j H = \phi$ if $i \neq j$. Then $|G| = \sum_{i=1}^{m} |\gamma_i H|$. But we know that

$|\gamma_i H| = |H| \Rightarrow |G| = \sum_{i=1}^{m} |H| = m|H|$, and since $m \in \mathbb{Z}$, $|H| \,\big|\, |G|$ // q.e.d. (m is the number of distinct left cosets).

Let G be a group, $H \subset G$ be a subgroup. Define $G/H = \{gH : g \in G\}$ as the set of distinct left cosets. Then, Lagrange's theorem can be properly expressed as $|G| = |G/H||H|$.

It is also true for right cosets. If $H\backslash G = \{Hg : g \in G\}$ is the set of right-cosets, then it is also true that $|G| = |H\backslash G||H|$.

In the proof of Lagrange's theorem, we listed the distinct cosets $\gamma_1 H, \gamma_2 H, \dots, \gamma_m H$. Then $\{\gamma_1 H, \gamma_2 H, \dots, \gamma_m H\}$ is said to be a <u>set of coset representatives</u>, where $G = \bigcup_{i=1}^{m} \gamma_i H$, $\gamma_i H \cap \gamma_j H = \phi$ if $i \neq j$.

e.g. Take $G = D_6 = \{1, x, x^2, y, xy, x^2 y\}$, $H = \{1, y\} \subset G$. The distinct left cosets are $\gamma_i H = \{1, y\}$ or $\{x, xy\}$, $\{x^2, x^2 y\}$ $\Rightarrow G/H = \{\{1,y\}, \{x, xy\}, \{x^2, x^2 y\}\}$.

(Cauchy's Theorem).

$\boxed{\text{Corollary}}$ Let G be a finite group and let $g \in G$. Then $\mathrm{ord}(g)$ divides $|G|$ exactly.

Proof – If $\mathrm{ord}(g) = n$, put $H = \{1, g, \dots, g^{n-1}\} \cong C_n$. Then $n = |H|$ divides $|G|$ // q.e.d.

$\boxed{\text{Corollary}}$ If p is prime and G is a group with $|G| = p$, then $G \cong C_p$.

Proof – If $g \in G$, $g \neq 1$; then $\mathrm{ord}(g) | p \Rightarrow \mathrm{ord}(g) = 1$ or p. $\mathrm{ord}(g) \neq 1 \because g \neq 1 \Rightarrow \mathrm{ord}(g) = p \Rightarrow \{1, g, \dots, g^{p-1}\} = G$ as cardinalities are the same. $\Rightarrow G \cong C_p$ // q.e.d.

22 January 2013 Prof FEA JOHNSON Roberts G06.

We seek to describe all homomorphisms of the form $h: C_n \to \Gamma$, where Γ is some finite group.

$\boxed{\text{Theorem}}$ Let $h: G \to \Gamma$ be a group homomorphism, and let $g \in G$. Then $\mathrm{ord}(h(g))$ divides $|G|$.

$\boxed{\text{Definition}}$ Let $h: G \to \Gamma$ be a group homomorphism. Define $\mathrm{Ker}(h) = \{g \in G : h(g) = 1_\Gamma\}$ as the <u>kernel</u>, $\mathrm{Im}(h) = \{\gamma \in \Gamma : \gamma = h(g)$ for some $g \in G\}$ as the <u>image</u>.

$\boxed{\text{Proposition}}$ With the above notation:

(i) $\mathrm{Ker}(h)$ is a subgroup of G, and (ii) $\mathrm{Im}(h)$ is a subgroup of Γ.

Proof – (i) $h(1_G) = 1_\Gamma \Rightarrow 1_G \in \mathrm{Ker}(h)$. If $x, y \in \mathrm{Ker}(h)$, $h(x) = h(y) = 1 \Rightarrow h(xy) = h(x)h(y) = 1 \Rightarrow xy \in \mathrm{Ker}(h)$. If $x \in \mathrm{Ker}(h)$, $h(x^{-1}) = h(x)^{-1} = 1^{-1} = 1 \Rightarrow x^{-1} \in \mathrm{Ker}(h)$ q.e.d.

(ii) $1_\Gamma = h(1_G) \Rightarrow 1_H \in \mathrm{Im}(h)$. If $\xi, \eta \in \mathrm{Im}(h)$, $\exists x, y$ s.t. $h(x) = \xi$, $h(y) = \eta \Rightarrow h(xy) = \xi\eta \Rightarrow \xi\eta \in \mathrm{Im}(h)$. If $\xi \in \mathrm{Im}(h)$, $h(x) = \xi$, $h(x^{-1}) = \xi^{-1} \Rightarrow \xi^{-1} \in \mathrm{Im}(h)$ // q.e.d

Recall that in Linear Algebra, $T: V \to W \Rightarrow \dim V = \dim \mathrm{Ker}(T) + \dim \mathrm{Im}(T)$. A similar relationship exists for our two defined subgroups:

Namely that if G, Γ are finite groups, then if $h: G \to \Gamma$, $|G| = |\mathrm{Ker}(h)||\mathrm{Im}(h)|$. We typically express this as $G/\mathrm{Ker}(h) \leftrightarrow \mathrm{Im}(h)$.

$\boxed{\text{Theorem}}$ Let $h: G \to \Gamma$ be a group homomorphism. Then $\exists$ a bijective mapping $h^*: G/\mathrm{Ker}(h) \xrightarrow{\cong} \mathrm{Im}(h)$

Note: Eventually, this will become a group isomorphism: Noether's Zeroth Isomorphism.

Proof – Put $K = \mathrm{Ker}(h)$. Then $G/K = \{gK : g \in G\}$. Define $h^*: G/K \to \mathrm{Im}(h)$ by $h_*(gK) = h(g)$. We must show that this is a well-defined mapping.

i.e. we must show that if $g_1 K = g_2 K$, $h(g_1) = h(g_2)$. Suppose $g_1 K = g_2 K \Rightarrow g_2^{-1} g_1 \in K = \mathrm{Ker}(h) \Rightarrow h(g_2^{-1} g_1) = h(g_2)^{-1} h(g_1) = 1 \because g_2^{-1} g_1 \in \mathrm{Ker}(h)$.

$\Rightarrow h(g_2) = h(g_1) \Rightarrow h^*$ is well-defined. Then $h^*: G/K \to \mathrm{Im}(h)$ is obviously surjective: $\gamma \in \mathrm{Im}(h) \Rightarrow \gamma = \mathrm{Im}(g)$, then $h_*(gK) = h(g) = \gamma$.

Suppose that $h_*(g_1 K) = h_*(g_2 K)$. Then $h(g_1) = h(g_2) \Rightarrow h(g_2)^{-1} h(g_1) = 1 \Rightarrow h(g_2^{-1} g_1) = 1 \Rightarrow g_2^{-1} g_1 \in K \Rightarrow g_1 K = g_2 K$. Hence, we see that

$h_*(g_1 K) = h_*(g_2 K) \Rightarrow g_1 K = g_2 K \Rightarrow$ injective mapping. Hence, h^* is a bijective mapping // q.e.d.

This result gives us a few corollaries:

$\boxed{\text{Corollary}}$ If $h: G \to \Gamma$ is a homomorphism with G finite, then $|G| = |Ker(h)||Im(h)|$

Proof – $|G/Ker(H)| = \frac{|G|}{|Ker(h)|}$ by Lagrange's theorem, q.e.d.

$\boxed{\text{Corollary}}$ If $h: G \to \Gamma$ is a homomorphism with G finite, then $|Im(h)|$ divides $|G|$ exactly.

Proof – Same as previous.

We finish with a proof of our earlier stated theorem, which is now no more than a corollary.

Proof. – $ord(h(g))$ divides $|Im(h)|$ and $|Im(h)|$ divides $|G|$, so $ord(h(g)) \mid |G|$. q.e.d.

$\boxed{\text{Ex}}$ Describe all homomorphisms of the form $h: C_{15} \to C_{10}$.

Soln. $C_{15} = \{1, x, \dots, x^{14}\}$, $C_{10} = \{1, z, \dots, z^9\}$. To determine h, it suffices to specify $h(x)$, since $h(x^a) = h(x)^a$ by homomorphism theory. We seek values b, $0 \le b \le 9$ s.t. we have a homomorphism h with $h(x) = z^b$.

Element	1	z	z^2	z^3	z^4	z^5	z^6	z^7	z^8	z^9
order	1	10	5	10	5	2	5	10	5	10

In order for $z^b = h(x)$ for some homomorphism h, it is necessary that $ord(z^b)$ divides $|C_{15}| = 15$. Only possible ones are $h(x) = 1, z^2, z^4, z^6, z^8$.

There are precisely 5 homomorphisms $h: C_{15} \to C_{10}$. To specify, we only need to state what $h(x)$ equals:

1. $h(x) = 1 \Rightarrow$ trivial $h(x^a) = 1$. 2. $h(x) = z^2 \Rightarrow h(x^a) = z^{2a}$ 3. $h(x) = z^4 \Rightarrow h(x^a) = z^{4a}$ 4. $h(x) = z^6 \Rightarrow h(x^a) = z^{6a}$ 5. $h(x) = z^8 \Rightarrow h(x^a) = z^{8a}$. //

$\boxed{\text{Theorem}}$ Let Γ be a finite group and $\gamma \in \Gamma$. Then there exists a homomorphism $h: C_n \to \Gamma$ with the property $h(x) = \gamma \iff ord(\gamma)$ divides n.

Proof – ($\Rightarrow$) Already done.

($\Leftarrow$). Suppose $ord(\gamma)$ divides n. Define $h: C_n \to \Gamma$, $h(x^a) = \gamma^a$, then h is a well-defined homomorphism. // q.e.d.

$\boxed{\text{Ex}}$ Investigate what happens if this condition is violated: Take $h: C_6 \to C_4$, and show that there are exactly two homomorphisms, and that $h(x) = z$ is not a homomorphism.

Soln. $h: C_6 \to C_4 = \{1, z, z^2, z^3\}$ $ord(1) = 1$, $ord(z) = 4$, $ord(z^2) = 2$, $ord(z^3) = 4$ $\Rightarrow$ $\exists$ exactly two homomorphisms $h: C_6 \to C_4$; specifically $h(x) = 1$, $h(x) = z^2$.

If we take $h(x) = z$, we have $1 \mapsto 1$, $x \mapsto z$, $x^2 \mapsto z^2$, $x^3 \mapsto z^3$, $x^4 \mapsto 1$, $x^5 \mapsto z$, $x^6 \mapsto z^2$. However, $x^6 = 1$, so $h(x^6) = h(1) = 1 \neq z^2$.

We send 1 to two different things $\Rightarrow$ it is not a mapping // q.e.d.

$\boxed{\text{Ex}}$ Examine homomorphisms of form $h: C_6 \to C_2 \times C_4$.

Soln. $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$. $C_2 \times C_4 = \{1, Y, Z, YZ, Z^2, YZ^2, Z^3, YZ^3\}$ where $1 = (1,1)$, $Y = (y, 1)$, $Z = (1, z)$. Then $Y^2 = 1$, $Z^4 = 1$, $YZ = ZY$.

Element	1	Z	Z^2	Z^3	Y	YZ	YZ^2	YZ^3
order	1	4	2	4	2	4	2	4

$ord(\gamma) \mid n \Rightarrow$ $\exists$ homomorphism $h: C_n \to C_2 \times C_4$, so we can take $\gamma = 1, Z^2, Y, YZ^2 = h(x)$.

1. $h(x) = 1 \Rightarrow$ trivial 2. $h(x) = Z^2$, $h(x^a) = Z^{2a}$ 3. $h(x) = Y$, $h(x^a) = Y^a$ 4. $h(x) = YZ^2$; $h(x^a) = Y^a Z^{2a}$. $\Rightarrow$ there are exactly four // homomorphisms.

Recall that $D_6 = \{1, x, x^2, y, xy, x^2y\}$, $x^3 = 1$, $y^2 = 1$, $yx = x^2y$. Contrast this with $C_3 \times C_2 = \{1, X, X^2, Y, XY, X^2Y\}$, $X^3 = 1$, $Y^2 = 1$, $YX = XY$.

Note that the elements are all the same, but the relations are different! Hence, they are not the same group. The former is non-abelian, the latter is abelian.

$C_3 \times C_2$ is a direct product, D_6 is not: we have $yx = x^2y \Rightarrow yxy^{-1} = x^2$. In contrast, for $C_3 \times C_2$, $YXY^{-1} = X$.

$\boxed{\text{Definition}}$ Let G be a group, $K \subset G$ be a subgroup. We say that K is <u>normal</u> in G when $\forall g \in G$, $gK = Kg$. We denote this $K \triangleleft G$.

Note: these are highly unusual! French name "distingué" is probably more appropriate.

$\boxed{\text{Proposition}}$ Let K be a subgroup of G. The following conditions are equivalent:

(i) $\forall g \in G$, $gK = Kg$ (ii) $\forall g \in G$, $\forall k \in K$, $gkg^{-1} \in K$.

Proof – Next lecture. e.g. $D_6 = \{1, x, x^2, y, xy, x^2y\} = G$, $K = \{1, x, x^2\}$. $1 \cdot K = x \cdot K = x^2 K = K$, $gK = xyK = x^2yK$; likewise $K \cdot 1 = K \cdot x = Kx^2$, $Ky = Kxy = Kx^2y$.

In each case, $gK = Kg$ $\forall g$. So K is normal.

(i) $\Rightarrow$ (ii): Suppose $gK = Kg$, and let $k \in K$. Then $gk \in gK$, so $gk \in Kg = \{k'g : k' \in K\}$. So $gk = k'g$ for some $k' \in K$

$\therefore gkg^{-1} = k' \in K$ // q.e.d.

25 January 2013.
Prof FEA Johnson.
Darwin 106.

(ii) $\Rightarrow$ (i): Suppose $gkg^{-1} \in K$ when $k \in K$. Then $gkg^{-1} = k'$ for some k'. Then $gk = k'g \in Kg$. So for all $k \in K$, $gK \subset Kg$. If K is finite, $|gK| = |Kg| = |K|$.

Hence, $gK = Kg$. If K is infinite, $g^{-1}k(g^{-1})^{-1} \in K$ $\forall g$, $g^{-1}kg \in K$, $kg \in gK \Rightarrow Kg \subset gK$. Thus $gK \subset Kg \subset gK$, so $gK = Kg$ // q.e.d.

Note: this gives us an alternative definition for a normal subgroup $K \triangleleft G$, from the condition first stated.

$\boxed{\text{Proposition}}$ Suppose $K \triangleleft G$. If $g \in G$, write $C_g(k) = gkg^{-1}$. Then $C_g : K \to K$ is an automorphism of K. (We call this the <u>conjugation</u> of K by $g \in G$).

Proof – NTP: $C_g : K \to K$ is a bijective homomorphism. $C_g(k_1k_2) = g(k_1k_2)g^{-1} = gk_1g^{-1}gk_2g^{-1} = C_g(k_1)C_g(k_2) \Rightarrow C_g$ is a homomorphism.

For bijectivity, we simply show C_g is invertible. $(C_g^{-1}C_g)(k) = C_{g^{-1}}(gkg^{-1}) = g^{-1}(gkg^{-1})(g^{-1})^{-1} = g^{-1}gkg^{-1}g = k \Rightarrow (C_{g^{-1}} \circ C_g) = Id$. Likewise $(C_g \circ C_{g^{-1}}) = Id$.

$\Rightarrow C_{g^{-1}} = C_g^{-1} \Rightarrow C_g$ is bijective $\Rightarrow C_g : K \to K$ is an automorphism // q.e.d.

7202-06.

We have shown that for $K \triangleleft G$, $g \in G$, $c_g : K \to K$, then $c_g \in \mathrm{Aut}(K)$.

Now, we introduce a new mapping $c : G \to \mathrm{Aut}(K)$, $g \mapsto c_g$.

$\boxed{\text{Proposition}}$ Let $K \triangleleft G$. Then the mapping $c : G \to \mathrm{Aut}(K)$, $c(g) = c_g$ is a homomorphism.

Proof – $c_{g_1 g_2}(k) = (g_1 g_2)(k)(g_1 g_2)^{-1} = g_1(g_2 k g_2^{-1})g_1^{-1} = c_{g_1}(g_2 k g_2^{-1}) = c_{g_1}(c_{g_2}(k)) = (c_{g_1} \circ c_{g_2})(k)$. Thus, $c_{g_1 g_2} = c_{g_1} \circ c_{g_2}$, q.e.d.

We will consider the following situation: (i) G is a group, (ii) K, Q are subgroups of G, and $K \triangleleft G$. Then we can restrict homomorphism c to domain Q. $c : Q \to \mathrm{Aut}(K)$, $c_q(k) = qkq^{-1}$. (iii) $K \cap Q = \{1\}$ and $|G| = |K||Q|$.

As an example, we consider a familiar group, $G = D_6 = \{1, x, x^2, y, xy, x^2y\}$, $x^3 = 1$, $y^2 = 1$, $yxy^{-1} = x^2$. Here we take $K = \{1, x, x^2\} \cong C_3$, $Q = \{1, y\} \cong C_2$.

Note that $\mathrm{Aut}(K) \cong \mathrm{Aut}(C_3) \cong C_2 = \{1, \tau\}$, $\tau^2 = \mathrm{Id}$. where $\tau(x) = x^2$. Note here that $c_y(x) = yxy^{-1} = x^2$, so $c_y = \tau \in \mathrm{Aut}(K)$, and in this case,

$c : Q \xrightarrow{\cong} \mathrm{Aut}(K)$ is an isomorphism.

For another example, $G = C_3 \times C_2 = \{1, X, X^2, Y, XY, X^2Y\}$, $X^3 = 1$, $Y^2 = 1$, $YX = XY$ (or $YXY^{-1} = X$). Take $K = \{1, X, X^2\} \cong C_3$, $Q = \{1, Y\} \cong C_2$.

But now, the conjugation mapping $c : Q \to \mathrm{Aut}(K)$ is a trivial homomorphism. $c_y(x) = yxy^{-1} = x$, $c_y = \mathrm{Id}$.

Semi-direct products.

Suppose K, Q are groups and $h : Q \to \mathrm{Aut}(K)$ is a homomorphism. Define $K \rtimes_h Q$, the <u>semi-direct product of K by Q</u>.

multiplication in K multiplication in Q.

As a set: $K \rtimes_h Q = K \times Q$. We have the operation of multiplication, $* : (K \rtimes Q) \times (K \rtimes Q) \to K \rtimes Q$ with $(k_1, q_1) * (k_2, q_2) = (k_1 \cdot h(q_1)(k_2),\ q_1 \cdot q_2)$

$h : Q \to \mathrm{Aut}(K)$, $h(1) = 1$. $h : Q \to \mathrm{Aut}(K)$, $(h(q))(1) = 1$.

Observe that $(1,1)$ is the identity element: $(1,1) * (k, q) = (1 \cdot h(1)(k),\ 1 \cdot q) = (1 \cdot \mathrm{Id}(k),\ 1 \cdot q) = (1 \cdot k,\ 1 \cdot q) = (k, q)$. $(k, q) * (1,1) = (k \cdot h(q)(1),\ q \cdot 1) = (k \cdot 1, q \cdot 1) = (k, q)$

Then, we need to show that $(K \rtimes_h Q, *, (1,1))$ is a group.

29 January 2013
Prof FEA JOHNSON.
Darwin G06.

We can reduce the multiplication rule to the following special cases:

(I): $(k_1, 1) * (k_2, 1) = (k_1\ h(1)(k_2),\ 1 \cdot 1) = (k_1\ \mathrm{Id}(k_2),\ 1) = (k_1 k_2, 1)$.

(II): $(1, q_1) * (1, q_2) = (1\ h(q_1)(1),\ q_1 q_2) = (1, q_1 q_2)$ $\because$ $h(q_1)$ is an automorphism, $1 \mapsto 1$.

(III): $(k, 1) * (1, q) = (k\ h(1)(1),\ 1 \cdot q) = (k, q)$

these three cases are not particularly useful or surprising.

(crucial case)
(IV): $(1, q) * (k, 1) = (1\ h(q)(k),\ q \cdot 1) = (h(q)(k), q)$. As q jumps over k, it operates by $h(q)$.

$\boxed{\text{Ex}}$ Take $K = C_3 = \{1, x, x^2\}$, $Q = C_2 = \{1, y\}$. We know that $\mathrm{Aut}(K) \cong C_2 = \{1, \tau\}$, $\tau(x) = x^2$. Take $h : C_2 \to \mathrm{Aut}(C_3)$, $h(y) = \tau$, so $h(y)(x) = x^2$. Find $K \rtimes_h Q$.

Soln. Crucial calculation: $(1, y) * (x, 1) = (h(y)(x), y) = (x^2, y)$. It helps to rewrite $X = (x, 1)$, $Y = (1, y)$. So $XY = (x, y)$, $YX = (x^2, y) = (x^2, 1)(1, y) = X^2Y$.

So in this case, our crucial calculation gives $YX = X^2Y$, $X^3 = 1$, $Y^2 = 1$, so $C_3 \rtimes_h C_2 \cong D_6$, where $h(y) = \tau$.

$\boxed{\text{Ex}}$ Take the same groups, but take $h : C_2 \to \mathrm{Aut}(C_3)$ to be trivial homomorphism $h(y) = \mathrm{Id}$. Find $C_3 \rtimes_h C_2$.

Soln. Crucial calculation: $(1, y) * (x, 1) = (h(y)x, y) = (\mathrm{Id}(x), y) = (x, y)$. i.e. $YX = XY \Rightarrow C_3 \rtimes_h C_2 \cong C_3 \times C_2$.

All this theory motivates us to discover new groups:

Consider the non-abelian group of order 21. Take $K = C_7 = \langle x \mid x^7 = 1 \rangle$, $Q = C_3 = \langle y \mid y^3 = 1 \rangle$. We evaluate every possible operator homomorphism $h : C_3 \to \mathrm{Aut}(C_7)$.

$\mathrm{Aut}(C_7) \cong C_6$; $\mathrm{Aut}(C_7) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}$. Take $\alpha = \varphi_3$, $\alpha^2 = \varphi_2$, $\alpha^3 = \varphi_6$, $\alpha^4 = \varphi_4$, $\alpha^5 = \varphi_5$, $\alpha^6 = \varphi_1 = \mathrm{Id}$. i.e. $\mathrm{Aut}(C_7) = \{1, \alpha^2, \alpha, \alpha^4, \alpha^5, \alpha^3\}$.

Hence, we seek homomorphisms $h : C_3 \to C_6 = \{1, \alpha, \dots, \alpha^5\}$. We can send y to any element which has order that divides $\mathrm{ord}(y) = 3$. $\Rightarrow$ we can send y to $1, \alpha^2, \alpha^4$.

i.e. there are three homomorphisms from $C_3 \to C_6$: $h_0(y) = \mathrm{Id}$, $h_1(y) = \alpha^2$, $h_2(y) = \alpha^4$. $\Rightarrow$ $h_0(y)(x) = x$ $h_1(y)(x) = \alpha^2(x) = \varphi_2(x) = x^2$ $h_2(y)(x) = \alpha^4(x) = \varphi_4(x) = x^4$

h_0: $YX = (1, y) * (x, 1) = (h_0(y)(x), y) = (x, y) = (x, 1) * (1, y) = XY$. Thus $YX = XY$, $C_7 \rtimes_h C_3 \cong C_7 \times C_3$. (Note: trivial homomorphism gives direct product).

h_1: $YX = (1, y) * (x, 1) = (h_1(y)(x), y) = (\varphi_2(x), y) = (x^2, y) = X^2Y$. Thus $YX = X^2Y$. In this case, with $h_1(y) = \alpha^2 = \varphi_2$, we have $X^7 = 1$, $Y^3 = 1$, $X^2Y = YX$.

This is a nonabelian group of order 21.

h_2: $YX = (h_2(y)(x), y) = (\varphi_4(x), y) = (x^4, y) = X^4Y$. We have $X^7 = Y^3 = 1$, $YX = X^4Y$.

$\langle X, Y \mid X^7 = 1, Y^3 = 1, YX = X^2Y \rangle$ $\langle X, Y \mid X^7 = 1, Y^3 = 1, YX = X^4Y \rangle$.

0) abelian I) non-abelian II) non-abelian

To summarise, take $K = C_7$, $Q = C_3$. There are three possible operator homomorphisms • $h_0(y)(x) = x$ • $h_1(y)(x) = x^2$ • $h_2(y)(x) = x^4$.

Apparently, we have three groups of order 21, but in fact we only have 2: the non-abelian groups are isomorphic. In C_3, put $z = y^2$, $z^2 = y$.

$C_3 = \{1, z, z^2\} = \{1, y, y^2\}$. Take h_1, and replace y by z. $ZX = (1, z)(x, 1) = (1, y^2)(x, 1) = (1, y)(1, y)(x, 1) = Y^2X$ then $YX = X^2Y$, $YXY^{-1} = X^2$.

Thus $Y^2XY^{-2} = Y(YXY^{-1})Y^{-1} = YX^2Y^{-1} = (YXY^{-1})(YXY^{-1}) = X^2X^2 = X^4$ $\therefore$ $Y^2XY^{-2} = X^4$, $Y^2X = X^4Y^2 = X^4Z$.

For I), replace y by $z = y^2$. Then $X^7 = Z^3 = 1$, $ZX = X^4Z$ which is II). i.e. $\langle X, Z \mid X^7 = Z^3 = 1, ZX = X^4Z \rangle$.

$\therefore$ the two non-abelian groups produced are isomorphic.

Recognition Criterion for semi-direct products.

$\boxed{\text{Theorem}}$ (Recognition criterion).

Suppose G is a finite group, and suppose G contains subgroups K, Q such that

i) $K \trianglelefteq G$, ii) $K \cap Q = \{1\}$, and iii) $|G| = |K||Q|$,

then $G \cong K \rtimes_c Q$ for some homomorphism $c: Q \to \mathrm{Aut}(K)$.

Proof – Define $c: Q \to \mathrm{Aut}(K)$ by $c(q)(k) = qkq^{-1}$, which is well defined because K is normal. Define $\Phi: K \rtimes_c Q \to G$ by $\Phi(k,q) = kq$.

NTP: · Φ is an isomorphism from $K \rtimes_c Q \xrightarrow{\cong} G$. $\Phi((k_1,q_1) * (k_2,q_2)) = \Phi(k_1\, c(q_1)(k_2), q_1q_2) = \Phi(k_1 q_1 k_2 q_1^{-1}, q_1q_2) = k_1q_1k_2q_1^{-1}q_1q_2 = k_1q_1k_2q_2$

Hence, $\Phi((k_1,q_1) * (k_2,q_2)) = (k_1q_1)(k_2q_2) = \Phi(k_1,q_1)\Phi(k_2,q_2) \Rightarrow \Phi$ is a homomorphism. Suppose that $\Phi(k_1,q_1) = \Phi(k_2,q_2)$. Then $k_1q_1 = k_2q_2 \Rightarrow k_2^{-1}k_1 = q_2q_1^{-1}$. Since LHS $\in K$, RHS $\in Q$, $k_2^{-1}k_1 = q_2q_1^{-1} \in K \cap Q = \{1\} \Rightarrow k_2^{-1}k_1 = q_2q_1^{-1} = 1 \Rightarrow k_1 = k_2, q_1 = q_2 \Rightarrow (k_1,q_1) = (k_2,q_2)$.

$\Rightarrow \Phi$ is injective. Since group is finite, and $\exists$ injective mapping $\Phi: K \rtimes_c Q \to G$, then $|K \rtimes_c Q| = |K||Q| = |G| \Rightarrow \Phi$ is also surjective.

$\therefore \Phi$ is an isomorphism from $K \rtimes_c Q \to G \Rightarrow G \cong K \rtimes_c Q$ // q.e.d.

This allows us to classify finite groups by identifying which of them are direct products.

We now pause to classify the groups that we have identified thus far.

$\lvert G\rvert$	1	2	3	4	5	6	7	8	9	10	11	12.	13	14	15
Groups G	$\{1\}$	C_2	C_3	$C_4, C_2\times C_2$	C_5	C_6, D_6	C_7	$C_8, C_4\times C_2, C_2\times C_2\times C_2, D_8, Q_8$	$C_9, C_3\times C_3$	C_{10}, D_{10}	C_{11}	$C_{12}, C_6\times C_2, D_{12}, \ldots$	C_{13}	C_{14}, D_{14}	C_{15}
Is this complete?	Yes	Yes (prime)	Yes	?	Yes	? (Here, $C_6 \cong C_3\times C_2$)	Yes.	?	?	?	Yes	No (total of 5)	Yes	?	?

All the "?" actually are "yes", but we will have to establish that. Eventually, we will consider up to $|G|$, with special cases for 16, 18, 27.

$\boxed{\text{Theorem}}$ Let G be a finite group, such that $\forall x \in G$, $x^2 = 1$. Then (i) G is abelian, (ii) $G \cong \overbrace{C_2 \times \cdots \times C_2}^{n \text{ copies}}$ for some n, and (iii) $|G| = 2^n$.

Proof – (i) Let $x, y \in G$. Then $x^2 = 1, y^2 = 1$. Since $\underset{\text{which is legitimate}}{xy \in G}$, $(xy)^2 = 1$. $x = x^{-1}, y = y^{-1}$. Hence, $(xy)^{-1} = y^{-1}x^{-1} = yx$. Thus, $(xy)^{-1} = (xy) \Rightarrow xy = yx$ // q.e.d.

(ii) We switch back to the additive convention, since G is abelian. i.e. replace '$\cdot$' by '+', '1' by '0'. i.e. '$2x = 0$'. Let $\mathbb{F}_2 = \{0,1\}$ be a field.

Then G is a vector space over $\mathbb{F}_2$. Apply the basis theorem. $G \cong \overbrace{\mathbb{F}_2 \times \cdots \times \mathbb{F}_2}^{n}$ which has dimension $n = \dim_{\mathbb{F}_2}(G)$.

However, $\mathbb{F}_2 = \{0,1\}$, $1+1=0$ $\cong$ $C_2 = \{1, x\}$, $x^2 = 1$, with $0 \mapsto 1$, $1 \mapsto x$. So $G \cong \overbrace{C_2 \times \cdots \times C_2}^{n}$ // q.e.d.

(iii) Clearly $|G| = |C_2| \cdot |C_2| \cdots |C_2| = |C_2|^n = 2^n$ // q.e.d.

$\boxed{\text{Corollary}}$ If G is a group $|G| = 4$, then either $G \cong C_4$ or $G \cong C_2 \times C_2$.

Proof – Let $g \in G$, $g \neq 1$. Then by Lagrange's Theorem, $\mathrm{ord}(g) = 4$ or 2. If $\exists g \in G$ s.t. $\mathrm{ord}(g) = 4$, then $G \cong C_4$. If not, $\forall g \in G$, $g^2 = 1$.

So by above, $G \cong C_2 \times C_2$ // q.e.d.

1 February 2013
Prof FEA JOHNSON.
Roberts 106

$\boxed{\text{Proposition}}$ Let p be a prime and consider the automorphism $\alpha: C_p \to C_p$ ($C_p = \{1, x, \cdots, x^{p-1}\}$) to be such that $\alpha^2 = \mathrm{Id}$.

Then α is one of the following: ① $\alpha = \mathrm{Id}$, or ② $\alpha(x) = x^{-1}$ s.t. $\alpha(x^a) = x^{-a}$

Proof – Take the element $z \in C_p$ so $z = x\alpha(x)$, $x \in C_p$, $\alpha(x) \in C_p$. Apply α to it to get $\alpha(z) = \alpha(x \cdot \alpha(x)) = \alpha(x)\,\alpha^2(x) = \alpha(x)\,\mathrm{Id}(x) = \alpha(x) \cdot x$

But $\alpha(x) \cdot x = x \cdot \alpha(x) = z$, so $\alpha(z) = z$. Now, we either have (i) $z = 1$ or (ii) $z \neq 1$.

- If $z = 1$, then $z = 1 = x\,\alpha(x) \Rightarrow \alpha(x) = x^{-1}$. Otherwise,
- If $z \neq 1$, then z generates C_p, so we can write C_p in terms of z as follows: $C_p = \{1, z, \cdots, z^{p-1}\}$.

Then $\alpha(z) = z \Rightarrow \alpha(z^a) = z^a \Rightarrow \alpha = \mathrm{Id}$ // q.e.d.

$\boxed{\text{Theorem}}$ If p is an odd prime, and $|G| = 2p$, then either:

① $G \cong C_{2p} \cong C_2 \times C_p$ or ② $G \cong D_{2p}$.

Proof – We will prove this theorem in 5 parts, to establish five claims in order.

Claim 1: G has at least one element with order p.

Let $g \in G$. Then by Lagrange's Theorem, possible values of $\mathrm{ord}(g)$ are $1, 2, p$ or $2p$ (since p is an odd prime).

We argue by contradiction: Suppose $\nexists g \in G$ s.t. $\mathrm{ord}(g) = p$, then we have either of two possibilities:

(a) $\exists g \in G$ s.t. $\mathrm{ord}(g) = 2p$, or (b) $\nexists g \in G$ s.t. $\mathrm{ord}(g) = 2p$ i.e. $\forall g \in G - \{1\}$, $\mathrm{ord}(g) = 2$ and $g^2 = 1$.

- If (a), then $\mathrm{ord}(g^2) = \frac{2p}{2} = p$. But $g^2 \in G \Rightarrow \mathrm{ord}(g^2) = p$ contradicts assumption that $\nexists$ such elements in G.
- If (b), then $|G| = 2^n$ for some $n \Rightarrow |G| = 2p = 2^n \Rightarrow p = 2^{n-1}$ which is a contradiction as p is an odd prime.

Since both (a) and (b) yield contradictions, we conclude that $\exists g \in G$ s.t. $\mathrm{ord}(g) = p$.

claim 2: $\exists$ a group K s.t. $K \cong C_p$ and $K \triangleleft G$.

Let $x \in G$ be s.t. $\text{ord}(x) = p$. We generate a group K with this element: $K = \{1, x, \dots, x^{p-1}\} \cong C_p$. We want to show $K \triangleleft G$, i.e. $\forall g \in G$ $gK = Kg$.

We consider two possibilities: ① if $g \in G$, $g \in K$, then $gK = Kg = K$; otherwise ② if $g \in G$, $g \notin K$, then

$G = K \cup gK$ and $K \cap gK = \phi$; $G = K \cup Kg$ and $K \cap Kg = \phi$ $\Rightarrow$ again $gK = Kg$. Hence for both cases, $gK = Kg$ $\forall g \in G \Rightarrow K \triangleleft G$.

claim 3: $\exists y \in G$ s.t. $\text{ord}(y) = 2$.

Consider the group K in claim 2, and choose element $z \in G - K$, s.t. $zK \neq K$. We claim $z^2 \in K$. By contradiction, suppose $z^2 \notin K$.

Then $zK = z^2K \Rightarrow z^{-1}zK = z^{-1}z^2K \Rightarrow K = zK \Rightarrow$ contradiction, so $z^2 \in K$. Then there are two possibilities: ① $z^2 = 1$ or ② $z^2 \neq 1$.

① $z^2 = 1 \Rightarrow \text{ord}(z) = 2$. Take $y = z$, then clearly $\text{ord}(y) = 2$.

② $z^2 \neq 1 \Rightarrow \text{ord}(z^2) = p \Rightarrow \text{ord}(z) = 2p$. Thus $\text{ord}(z^p) = 2$. Take $y = z^p$, then $\text{ord}(y) = 2$.

claim 4: $G \cong C_p \rtimes_h C_2$ for some homomorphism $h: C_2 \to \text{Aut}(C_p)$.

Let K be as above, and $Q = \{1, y\}$, $y^2 = 1$ be another subgroup. By Lagrange's theorem, $K \cap Q = \{1\}$, and $|G| = 2p = |K||Q|$.

By recognition criterion, $G \cong K \rtimes_h Q \cong C_p \rtimes_h C_2$ for some $h: C_2 \to \text{Aut}(C_p)$.

claim 5: Final statement of theorem.

Write $C_2 = \{1, y\}$ $y^2 = 1$, $C_p = \{1, x, \dots, x^{p-1}\}$ $x^p = 1$. We examine $h: C_2 \to \text{Aut}(C_p)$. Clearly, $h(y) \in \text{Aut}(C_p)$, $h(y)^2 = h(y^2) = 1$.

Hence, either ① $h(y) = \text{Id}$, or ② $h(y)(x) = x^{-1}$. If ①, $h(y) = \text{Id} \Rightarrow G \cong C_p \rtimes_{\text{Id}} C_2 \cong C_p \times C_2$. Otherwise, in case ②,

$h(y)(x) = x^{-1}$. Let $X = (x, 1)$, $Y = (1, y)$. Then $YX = (1, y) \times (x, 1) = (h(y)(x), y) = (x^{-1}, y) = X^{-1}Y \Rightarrow YX = X^{-1}Y \Rightarrow YXY^{-1} = X^{-1}$

$\therefore$ $G \cong D_{2p}$. Hence $G \cong C_{2p}$ or D_{2p} // q.e.d.

We can also extend our list of orders to classify some more small-order groups.

$\lvert G\rvert$	16	17	18	19	20	21	22	23
G	Messy!	C_{17}	Tricky, may study later	C_{19}	Will show later	$C_{21} \cong C_3 \times C_7$, $G(21)$	$C_{22} \cong C_{11} \times C_2$, D_{22}	C_{23}

non-abelian group of order 21

Then, we will move on to prove an extremely important result – the main theorem of the Groups part of the course. (We will only prove this later on in the course).

$\boxed{\text{Theorem}}$ (Sylow's Theorems).

Let G be a finite group, with $|G| = kp^n$ where p is prime, $(k, p) = 1$. Then

(I) G has at least one subgroup of order p^n,

(II) If N_p is the number of subgroups of order p^n, then $N_p \equiv 1 \mod p$.

(III) N_p divides the order of the group,

(IV) If H_1, H_2 are subgroups of orders p^n and p^m respectively, and $m \leq n$, then $\exists g \in G$ s.t. $gH_2g^{-1} \subset H_1$.

We expand upon this theorem, with an example for applying it – Sylow counting.

$\boxed{\text{Ex}}$ Use Sylow counting to prove that $|G| = 15 \Rightarrow G \cong C_{15}$.

soln. $|G| = 15 = 3 \cdot 5$. We consider the larger prime first. $p = 5$: $N_5 \equiv 1 \mod 5 \Rightarrow N_5 = 1$ or $N_5 \geq 6 \Rightarrow$ number of subgroups of order 5 is 1 or 6 (or larger).

If $N_5 \geq 6$, we have 6 distinct subgroups of order 5: $K_1, \dots, K_6$; where $K_i \cong C_5$ $\forall i = 1, 2, \dots, 6$. since C_5 is the only group of order 5.

Then $K_1 \cup \dots \cup K_6$ contains $6 \times (5-1) = 24$ distinct elements, but $|G| = 15 < 24$. Hence clearly $N_5 = 1 \Rightarrow$ we call this single subgroup K, $K \cong C_5$.

If $g \in G$, gKg^{-1} is a subgroup of order $5 \Rightarrow gKg^{-1} \subseteq K \Rightarrow K \triangleleft G$. Then, we consider second prime; now take $p = 3$.

By Sylow's theorem with $p = 3$, $k = 5$, $n = 1$, (I) $\Rightarrow$ $\exists$ a subgroup Q s.t. $|Q| = 3$. Thus $Q \cong C_3$.

By recognition criterion, $G \cong C_5 \rtimes_h C_3 \Rightarrow h: C_3 \to \text{Aut}(C_5) \cong C_4$. Since $(3, 4) = 1$, h is trivial (Id) $\Rightarrow G \cong C_5 \times C_3 \cong C_{15}$ // q.e.d.

5 February 2013.
Prof Frank EA Johnson
Roberts G06.

$\boxed{\text{Ex}}$ Classify groups of order 44.

soln. $|G| = 44 = 2^2 \cdot 11$. Consider $p = 11$. Therefore $N_{11} \equiv 1 \mod 11 \Rightarrow N_{11} = 1$ or $N_{11} \geq 12$. Suppose $N_{11} \geq 12$. Let $K_1, \dots, K_{12}$ all be subgroups of order 11.

11 is prime, so $K_i \cong C_{11}$. $\therefore$ $K_i \neq K_j$ if $i \neq j$, but $K_i \cap K_j = \{1\}$ for if $z \in K_i \cap K_j$ and z is non-trivial, z generates both K_i and $K_j \Rightarrow$

$K_i = K_j$, which is not true. Hence, $|K_i - \{1\}| = 10$ $\forall i$, with each element of order 11. $\Rightarrow$ G has at least $12(11-1) = 120$ distinct elements > 44

$\Rightarrow$ contradiction. Hence $N_{11} = 1$. Let K be the unique subgroup of order 11. Then $K \cong C_{11}$, we claim $K \triangleleft G$, $\because$ if $g \in G$, gKg^{-1} is a subgroup

of order 11. By uniqueness of subgroups of order 11, $gKg^{-1} = K \Rightarrow gK = Kg \Rightarrow K \triangleleft G$. So far, we have shown $|G| = 44 \Rightarrow$ G has normal subgroup K, $|K| = 11$, $K \cong C_{11}$.

Consider $p = 2$, $n = 2$, $k = 11$. By Sylow's Theorem, G has at least a subgroup of order 2^2; $|Q| = 4$. Observe that $K \cap Q = \{1\}$ as $|K|, |Q|$ are coprime by Lagrange's theorem.

Apply recognition criteria: $G \cong K \rtimes_h Q$ where $K \cong C_{11}$, $|Q| = 4$. So we get two families: $G \cong C_{11} \rtimes_h C_4$, $G \cong C_{11} \rtimes_h (C_2 \times C_2)$.

Family (I) $G \cong C_{11} \rtimes_h C_4$. Write $K \cong C_{11} = \langle x \mid x^{11}=1\rangle$, $Q \cong C_4 = \langle y \mid y^4=1\rangle$. $\mathrm{Aut}(C_{11}) \cong C_{10}$. We find homomorphisms $h: C_4 \to \mathrm{Aut}(C_{11}) \cong C_{10}$.

C_{10} has exactly one element of order 2, $\tau(x) = x^{-1} = x^{10}$. So there are precisely two homomorphisms $h: C_4 \to \mathrm{Aut}(C_{11})$.

h_0 is trivial homomorphism, $h_0 = \mathrm{Id}$. then $G \cong C_{11} \rtimes_{h_0} C_4 \cong C_{11} \times C_4 \cong C_{44}$.

h_1 gives $h_1(y) = \tau \Rightarrow$ crucial calculation is $YX = \tau(X)Y = X^{-1}Y$ (or $X^{10}Y$). Then $G \cong C_{11} \rtimes_{h_1} C_4 = \langle X, Y \mid X^{11} = Y^4 = 1,\ YX = X^{-1}Y\rangle$.

this group is known as the quaternion group of order 44, $Q(44)$ (can also be D^*_{22}, which is not a dihedral group!).

Family (II) $G \cong C_{11} \rtimes_h (C_2 \times C_2)$. How many homomorphisms are there that take form $h: C_2 \times C_2 \to \mathrm{Aut}(C_{11}) \cong C_{10}$? $C_2 \times C_2 = \{1, s, t, st\}$, $s^2 = t^2 = 1$, $ts = st$.

then either $h(s) = 1$ or τ, $h(t) = 1$ or τ. We appear to get 4 homomorphisms, as follows: (a) $h_0(s) = 1$, $h_0(t) = 1 \Rightarrow h(st) = 1$.

(b) $h_1(s) = \tau$, $h_1(t) = 1 \Rightarrow h_1(st) = \tau$ (c) $h_2(s) = 1$, $h_2(t) = \tau \Rightarrow h_2(st) = \tau$. (d) $h_3(s) = \tau$, $h_3(t) = \tau$, $h_3(st) = \tau^2 = 1$.

For each homomorphism, we get a group presentation corresponding to it. (a) h_0: $X^{11} = 1$, $S^2 = T^2 = 1$, $ST = TS$, $SX = XS$, $TX = XT \Rightarrow G \cong C_{11} \times C_2 \times C_2 \cong C_{22} \times C_2$.

(b) For h_1: $X^{11} = 1$, $S^2 = 1$, $T^2 = 1$, $TS = ST$. $SX = X^{-1}S$, $TX = XT$. Ignore T to get $D_{22} = \langle X, S \mid X^{11} = S^2 = 1\rangle$, $C_2 = \langle T \mid T^2 = 1\rangle$. they commute $\Rightarrow G \cong D_{22} \times C_2$.

(c) For h_2: there is symmetry with h_1 – instead of $G \cong \overset{\langle X,S\rangle}{D_{22}} \times \overset{\langle T\rangle}{C_2}$, we have $G \cong \overset{\langle X,T\rangle}{D_{22}} \times \overset{\langle S\rangle}{C_2}$. These are isomorphic.

(d) For h_3: this is also isomorphic to $G \cong \overset{\langle X,T\rangle \text{ or } \langle X,S\rangle}{D_{22}} \times \overset{\langle ST\rangle}{C_2}$, where ST is a generator for C_2. Isomorphic as well.

Through the theorem, there are precisely 4 isomorphically distinct groups of order 44: $\overbrace{C_{44} \cong C_{11} \times C_4,\ C_{22} \times C_2 \cong C_{11} \times C_2 \times C_2}^{\text{2 abelian}}, \overbrace{Q(44),\ D_{22} \times C_2}^{\text{2 non-abelian}}$.

We move on to examine groups such as $Q(44)$, which are quarternion groups (or binary dihedral groups).

<u>the group $Q(4n)$</u>. Alternative name is: D^*_{2n}, the binary dihedral group.

$Q(4n) = \langle X, Y \mid X^n = 1,\ Y^4 = 1,\ YXY^{-1} = X^{-1}\rangle$ is <u>the quarternion group</u>. <u>Not</u> to be confused with $D_{2n} = \langle X, Y,\ X^n = 1,\ Y^2 = 1,\ YXY^{-1} = X^{-1}\rangle$!!!

D_{2n} sits inside $O(3)$ (rotation group), $Q(4n)$ sits inside S^3 (unit quarternions).

$\boxed{\text{Ex}}$ classify groups of order 12.

Soln. $|G| = 2^2 \times 3$. We try larger prime $p=3$. By Sylow's theorem, $\exists$ subgroup H, $|H| = 3$ and $N_3 \equiv 1 \bmod 3 \Rightarrow N_3 = 1, 4$ or $N_3 \geq 7$. If $N_3 \geq 7$, we get at least $7 \times (3-1) = 14$ elements of order 3. $14 > 12 = |G| \Rightarrow$ contradiction. Then we are left with either $N_3 = 1$ or $N_3 = 4$.

If $N_3 = 1$, $\exists$ unique subgroup of order 3 with $|H| = 3$, $H \triangleleft G$. If $N_3 = 4$, $\exists\ 4 \times (3-1) = 8$ elements of order 3. $12 - 8 = 4$ elements (including the identity) are unaccounted for.

Invoke Sylow for $p = 2$: $\exists$ subgroup of order 4, $|L| = 4$. Then if $N_3 = 4$, L is the set of elements (four of them) of order $\neq 3$.

there is no more room for more than one such subgroup L.

To summarise: let H, L be subgroups of G; $|H| = 3$, $|L| = 4$. If $N_3 = 1$, $H \triangleleft G$. If $N_3 = 4$, $N_4 = 1$, $L \triangleleft G \Rightarrow$ if $|G| = 12$, G has a normal subgroup: either H of order 3, or L of order 4. Either way, we have $G \cong H \rtimes_h L$ ($|H| = 3$, $H \triangleleft G$) or $G \cong L \rtimes_h H$ ($|L| = 4$, $L \triangleleft G$).

$H \cong C_3$, but $L = C_4$ or $C_2 \times C_2$. Hence, we get four families of groups: (I) $C_3 \rtimes_h C_4$, (II) $C_3 \rtimes_h (C_2 \times C_2)$ (III) $C_4 \rtimes_h C_3$ (IV) $(C_2 \times C_2) \rtimes_h C_3$

Family (I) $C_3 = \{1, x, x^2\}$, $C_4 = \{1, y, y^2, y^3\}$. $h: C_4 \to \mathrm{Aut}(C_3) \cong C_2 = \{1, \tau\}$. $\exists$ two homomorphisms: $h_0(y) = \mathrm{Id}$, $G \cong C_3 \rtimes_{h_0} C_4 \cong C_3 \times C_4$.

$h_1(y) = \tau$, $h_1(y)(x) = \tau(x) = x^2$. then $G \cong \langle X, Y \mid X^3 = Y^4 = 1,\ YX = X^2Y = X^{-1}Y\rangle \cong Q(12)$.

Family (II) Four homomorphisms: $C_2 \times C_2 = \langle s, t \mid s^2 = t^2 = 1,\ ts = st\rangle$. (a) $h_0(s) = 1$, $h_0(t) = 1 \Rightarrow h_0(st) = 1$ (b) $h_1(s) = \tau$, $h_1(t) = 1 \Rightarrow h_1(st) = \tau$.

(c) $h_2(s) = 1$, $h_2(t) = \tau \Rightarrow h_2(st) = \tau$ (d) $h_3(s) = \tau$, $h_3(t) = \tau \Rightarrow h_3(st) = \tau^2 = 1$. h_0 corresponds to $C_3 \times C_2 \times C_2 \cong C_6 \times C_2$.

h_1 corresponds to $G \cong \langle X, S, T \mid X^3 = 1,\ S^2 = 1,\ T^2 = 1,\ SX = X^2S,\ TX = XT,\ TS = ST\rangle \cong \langle X, S \mid X^3 = 1,\ S^2 = 1,\ SX = X^2S\rangle \times \langle T \mid T^2 = 1\rangle \cong D_6 \times C_2$.

h_2 corresponds also $D_6 \times C_2$ with $C_2 \cong \langle S \mid S^2 = 1\rangle$, h_3 as well with $C_2 \cong \langle ST \mid (ST)^2 = 1\rangle$.

Family (III). This is trivial. $C_4 \rtimes_h C_3 \Rightarrow h: C_3 \to \mathrm{Aut}(C_4) \cong C_2$. We only have the trivial identity homomorphism: $C_4 \times C_3 \cong C_{12}$ (repetition).

Family (IV). $(C_2 \times C_2) \rtimes_h C_3$. Then $h: C_3 \to \mathrm{Aut}(C_2 \times C_2) \cong D_6$. Take $C_2 \times C_2 = \{1, s, t, st\}$, $C_3 = \{1, y, y^2\}$, $h(y)$ has order 1 or 3.

there are two elements in the automorphism group of $C_2 \times C_2$ that have order 3: α and α^2. Define $\alpha(s) = st$, $\alpha(t) = s$, $\alpha(st) = t$; $\alpha^2(s) = t$, $\alpha^2(t) = st$, $\alpha^2(st) = s$.

of course, we also have $h(y) = \mathrm{Id}$, which corresponds to $C_2 \times C_2 \times C_3 \cong C_6 \times C_2$. (repetition). then if we take

$h(y) = \alpha$, we get the following presentation: $G \cong \langle S, T, Y \mid S^2 = T^2 = 1,\ ST = TS,\ Y^3 = 1,\ YS = STY,\ YT = SY\rangle$.

$h(y) = \alpha^2$, we get the following presentation: $G \cong \langle S, T, Y \mid S^2 = T^2 = 1,\ ST = TS,\ Y^3 = 1,\ YS = TY,\ YT = STY\rangle$.

isomorphic, taking $Y \leftrightarrow Z = Y^2$.

this is a familiar group: recall $\mathfrak{S}_n = \{\sigma : \{1, \dots, n\} \to \{1, \dots, n\} \text{ bijective}\}$, the set of permutations on n. then $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n : \mathrm{sign}(\sigma) = 1\}$.

$\mathfrak{A}_n$ is the set of even permutations on $\{1, \dots, n\}$. Then this final group is just $\mathfrak{A}_4$. Take $S = (1\ 2)(3\ 4)$, $T = (1\ 3)(2\ 4)$

and $ST = (1\ 4)(2\ 3)$. then if $Y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, $YSY^{-1} = YS\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = Y\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix} = ST$, $YTY^{-1} = S$.

In summary then, there are precisely 5 distinct groups of order 12: namely

abelian: ① $C_{12} \cong C_3 \times C_4$, ② $C_6 \times C_2$

non-abelian: ③ $Q(12)$ ④ $D_6 \times C_2$ ⑤ $\mathfrak{A}_4$

8 February 2013.
Prof FEA JOHNSON
Roberts 106.

Group Actions.

Let X be a set and G be a group. By a (left) action of G on X, we mean a mapping $\circ: G\times X \to X$, $g\circ x = \circ(g,x)$ s.t.

(i) $g\circ(h\circ x) = (gh)\circ x$ for all $g,h\in G$, all $x\in X$. (ii) $1_G \circ x = x$ for all $x\in X$.

There is a corresponding notion of right action: $\circ: X\times G \to X$, $x\circ g = xg$. However, we generally stick to left actions.

If X is a set denoted by $\sigma_X = \{\alpha: X\to X : \alpha \text{ is a bijective mapping}\}$. σ_X = permutations on X is a group under composition.

$$\begin{tikzcd} X \arrow[r, "\alpha"] & X \arrow[d, "h"] \\ Y \arrow[u, "h^{-1}"] \arrow[r, "h\alpha h^{-1}"'] & Y \end{tikzcd}$$

Note that if $h: X\to Y$ is bijective, then $\sigma_X \cong \sigma_Y$. $\alpha \mapsto h\alpha h^{-1}$ is an isomorphism $\sigma_X \cong \sigma_Y$.

So if $|X|=n$ then $\sigma_X \cong \sigma_n$.

Alternative formulation of group action: Let $\varphi: G\to \sigma_X$ be a homomorphism. Obtain group action $G\times X \to X$ by $g\cdot x = \varphi(g)(x)$.

Every group action arises in this way. Given a group $\circ: G\times X\to X$, define $\lambda: G\to\sigma_X$ by $\lambda(g)(x) = g\circ x$.

Observe $\lambda(g)\in\sigma_X$. $\lambda(g)(x) = \lambda(g)(y)$, $g\circ x = g\circ y$. Multiply on left by g^{-1}: $x=y$. Then $\lambda(g)$ is injective, also $\lambda(g)$ is surjective. $\lambda(g)\in\sigma_X$.

λ is a homomorphism: $\lambda(g_1g_2)(x) = (g_1g_2)\circ x = g_1\circ(g_2\circ x) = \lambda(g_1)(\lambda(g_2)(x)) \Rightarrow \lambda(g_1g_2) = \lambda(g_1)\lambda(g_2)$.

So we have two points of view: group action $\circ: G\times X\to X$ or homomorphism $G\to\sigma_X$. Preference is a matter of taste.

$\boxed{\text{Ex}}$ (Cayley's Theorem)

Prove that if G is a finite group with $|G|=n$, then G is isomorphic to a subgroup of σ_n.

Soln. There is an obvious group action of G on itself. $G\times G\to G$, $(g,h)\mapsto gh$ multiplication on G. This is left translation.

If it is interpreted as a group homomorphism, $\lambda: G\to\sigma_G$, $\lambda(g)(h) = gh$. So $\mathrm{Im}(\lambda)$ is a subgroup of σ_G.

In this case however, λ is injective, because if $\lambda(g_1)=\lambda(g_2)$, $\lambda(g_1)(1) = \lambda(g_2)(1)$ so $g_1\cdot 1 = g_2\cdot 1 \Rightarrow g_1 = g_2$.

So $\lambda: G\to \mathrm{Im}(\lambda)$ is an isomorphism. $\mathrm{Im}(\lambda)\subset \sigma_G \cong \sigma_n$. // q.e.d.

e.g. We show the Cayley multiplication for D_6 on the right:

input

		1	x	x^2	y	xy	x^2y
	1	1	x	x^2	y	xy	x^2y
$\lambda(x)\rightarrow$	x	x	x^2	1	xy	x^2y	y
	x^2	x^2	1	x	x^2y	y	xy
output	y	y	x^2y	xy	1	x^2	x
$\lambda(xy)\rightarrow$	xy	xy	y	x^2y	x	1	x^2
	x^2y	x^2y	xy	y	x^2	x	1.

In a Cayley table, we apply the left operator λ to our input to get the rows. We can also look the other direction we can obtain right operators ρ. c.f. Latin squares.

We have seen that Cayley's theorem $\equiv$ left translation in G. We see here another example: conjugation.

Conjugation is a group action: If G is a group, obtain conjugation action $*: G\times G\to G$, $g*h = ghg^{-1}$.

This is used extensively in the proof of Sylow's Theorem.

Orbits.

Let $\circ: G\times X\to X$ be a group action. Let $x\in X$. Define $\langle x\rangle = \{g\circ x : g\in G\}$ as the orbit of x.

$\boxed{\text{Proposition}}$ Let $\circ: G\times X\to X$ be a group action. Let $x,y\in X$, then either (i) $\langle x\rangle = \langle y\rangle$ or (ii) $\langle x\rangle\cap\langle y\rangle = \phi$.

Proof - Consider when $\langle x\rangle\cap\langle y\rangle \neq \phi$, NTP: $\langle x\rangle = \langle y\rangle$. Suppose $z\in\langle x\rangle\cap\langle y\rangle$. Then $z = g\circ x = h\circ y$ for some $g\in G$, $h\in G$.

Then $y = (h^{-1}g)\circ x$. So if $\gamma\in G$, $\gamma\circ y = (\gamma h^{-1}g)\circ x$ i.e. $\langle y\rangle\subset\langle x\rangle$. Conversely, $x = (g^{-1}h)\circ y \Rightarrow \gamma\circ x = (\gamma g^{-1}h)\circ y \Rightarrow \langle x\rangle\subset\langle y\rangle$.

i.e. $\langle x\rangle\subset\langle y\rangle\subset\langle x\rangle \Rightarrow \langle x\rangle = \langle y\rangle$ // q.e.d.

Class Equation

Consider $G = D_6 = \{1, x, x^2, y, xy, x^2y\}$. Let D_6 act on itself by conjugation. Then $\langle 1\rangle = \{g\cdot 1\cdot g^{-1} : g\in D_6\} = \{1\}$; $\langle x\rangle = \{gxg^{-1} : g\in D_6\} = \{x, x^2\}$.

$\langle x^2\rangle = \{x^2, x\}$, $\langle y\rangle = \{y, xy, x^2y\}$, $\langle xy\rangle = \{y, x, x^2y\}$, $\langle x^2y\rangle = \{y, xy, x^2y\}$. Then we have three orbits (conjugacy classes).

$\langle 1\rangle = \{1\}$, $\langle x\rangle = \langle x^2\rangle = \{x, x^2\}$, $\langle y\rangle = \langle xy\rangle = \langle x^2y\rangle = \{y, xy, x^2y\}$. Then $D_6 = \langle 1\rangle\cup\langle x\rangle\cup\langle y\rangle$, $\langle 1\rangle\cap\langle x\rangle = \langle 1\rangle\cap\langle y\rangle = \langle x\rangle\cap\langle y\rangle = \phi$.

We introduce the notation as follows: Suppose $A = A_1\cup A_2\cup\cdots\cup A_m$, $A_i\cap A_j \neq \emptyset$ if $i\neq j$, then A is a disjoint union and we write $A = A_1\sqcup A_2\sqcup\cdots\sqcup A_m$.

Then $D_6 = \langle 1\rangle\sqcup\langle x\rangle\sqcup\langle y\rangle$.

In general, given a group action $\circ: G\times X\to X$, choose elements $x_1,\dots,x_m$ which list the distinct orbits $\langle x_1\rangle,\cdots\langle x_m\rangle$ so $\langle x_i\rangle\cap\langle x_j\rangle = \phi$ if $i\neq j$.

So then $X = \langle x_1\rangle\sqcup\langle x_2\rangle\sqcup\cdots\sqcup\langle x_m\rangle$, which gives us the set theoretic class equation $|X| = \sum_{i=1}^{m}|\langle x_i\rangle|$ (naive numerical class equation).

So for D_6 under conjugation, $|D_6| = |\langle 1\rangle| + |\langle x\rangle| + |\langle y\rangle|$.

19 February 2013.
Prof FEA JOHNSON.
Roberts G06.

Let G be a finite group acting on finite set X. For $x\in X$. $\langle x\rangle = \{gx : g\in X\}$, distinct orbits are disjoint.

If $x_1,\dots,x_m\in X$ represent distinct orbits, $X = \bigsqcup_{i=1}^{m}\langle x_i\rangle$ (set theory version of class equation)

Definition If $x \in X$, define stability subgroup of x, $G_x = \{g \in G : gx = x\}$.

Proposition G_x is a subgroup of G.

Proof – $1 \in G_x \because 1 \cdot x = x$. Let $g, h \in G_x$. Then $(gh)\cdot x = g(h \cdot x) = g \cdot x$ ($\because h \in G_x$) $= x$ ($\because g \in G_x$) $\Rightarrow gh \in G_x$.

If $g \in G$, $x = gx \Rightarrow g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1 \cdot x = x \Rightarrow g^{-1} \in G_x$. Hence G_x is a subgroup // q.e.d.

Proposition If finite group G acts on X and $x \in X$, then $\exists$ a bijective mapping $G/G_x \overset{\simeq}{\longleftrightarrow} \langle x \rangle$. In particular, $|\langle x \rangle| = |G|/|G_x|$.

Proof – Define $\mathfrak{h}: G/G_x \to \langle x \rangle$ as follows. $\mathfrak{h}(g \cdot G_x) = gx$. Clearly $gx \in \langle x \rangle$. We need to show that this is well-defined, i.e. if $g_1 \cdot G_x = g_2 \cdot G_x$, then $g_1 x = g_2 x$

s.t. $\mathfrak{h}(g_1 \cdot G_x) = \mathfrak{h}(g_2 \cdot G_x)$. Suppose $g_1 G_x = g_2 \cdot G_x$. By rule of equality, $g_2^{-1} g_1 \in G_x \Rightarrow (g_2^{-1} g_1)x = x \Rightarrow g_2^{-1}(g_1 x) = x \Rightarrow g_1 x = g_2 x$.

So, the mapping is well-defined. We just need to show bijectivity:

- Clear that $\mathfrak{h}$ is surjective: if $g \cdot x \in \langle x \rangle$, then $\mathfrak{h}(g \cdot G_x) = gx$, so $\mathfrak{h}$ is surjective.
- To show $\mathfrak{h}$ is injective, suppose $\mathfrak{h}(g \cdot G_x) = \mathfrak{h}(h \cdot G_x)$. Then NTP: $g \cdot G_x = h \cdot G_x$.

$\mathfrak{h}(g \cdot G_x) = \mathfrak{h}(h \cdot G_x)$ means that $gx = hx \Rightarrow (h^{-1}g)x = x \Rightarrow h^{-1}g \in G_x \Rightarrow g \cdot G_x = h \cdot G_x$ by rule of equality // q.e.d.

Corollary (Full Class Equation).

Suppose finite group G acts on finite set X. Let $x_1, \dots, x_m$ represent the distinct orbits, then $|X| = \sum_{i=1}^{m} |G|/|G_{x_i}|$

Ex Let $G = X = D_6$, with G acting by conjugation $D_6 \times D_6 \to D_6$, $g \cdot z = gzg^{-1}$, $D_6 = \{1, x, x^2, y, xy, x^2y\}$. Show that the full class equation holds.

Soln. We let $1, x, y$ represent the distinct orbits. $G_1 = \{g \in D_6 : g \cdot 1 \cdot g^{-1} = 1\}$, so $G_1 = G = D_6$.

- $|\langle 1 \rangle| = |G|/|G| = 1$, $\langle 1 \rangle = \{1\}$
- $G_x = \{g \in D_6 : gxg^{-1} = x\}$. In fact, $G_x = \{1, x, x^2\}$. Also, $yxy^{-1} = x^2$, $(xy)x(xy)^{-1} = x^2$, $(x^2y)x(x^2y)^{-1} = x^2 \Rightarrow y \notin G_x$, $xy \notin G_x$, $x^2y \notin G_x$.

  So in this case, $|\langle x \rangle| = |G|/|G_x| = \frac{6}{3} = 2$. Okay because $\langle x \rangle = \{x, x^2\}$
- $G_y = \{g \in G : gyg^{-1} = y\}$. In fact, $G_y = \{1, y\}$, $|\langle y \rangle| = |G|/|G_y| = \frac{6}{2} = 3$. True, as $\langle y \rangle = \{y, xy, x^2y\}$.

  Note that $G_{xy} = \{1, xy\}$, $G_{x^2y} = \{1, x^2y\}$ etc. Class equation now gives $|G| = \frac{|G|}{|G_1|} + \frac{|G|}{|G_2|} + \frac{|G|}{|G_3|} \Rightarrow 6 = 1 + 2 + 3$ // q.e.d.

Note: Order of each orbit divides order of group, i.e. $|\langle x \rangle| \,\big|\, |G|$.

Overall, this presents us with three versions of the class equation, as follows:

(1) $|X| = \langle x_1 \rangle \sqcup \langle x_2 \rangle \sqcup \dots \sqcup \langle x_m \rangle$, where $x_1, \dots, x_m$ represent distinct orbits, (2) $|X| = \sum_{i=1}^{m} |\langle x_i \rangle|$, (3) $\boxed{|X| = \sum_{i=1}^{m} |G|/|G_{x_i}|}$ We will use mainly this.

Definition Let G act on X, $\cdot : G \times X \to X$. We say that $x \in X$ is a fixed point under G when $\forall g \in G$, $g \cdot x = x$.

Note: We can express this in a number of equivalent ways by definition:

(i) x is a fixed point (ii) $\langle x \rangle = \{x\}$ (iii) $|\langle x \rangle| = 1$ (iv) $G_x = G$.

Theorem Let p be prime and let G be a group with $|G| = p^n$ $(n \geq 1)$. If G acts on X, put $X^G = \{x \in X : \forall g \in G, gx = x\}$ i.e. X^G is the set of fixed points.

Then $|X| \equiv |X^G| \pmod p$.

Note: Beware that this only works when $|G| = p^n$.

Proof – Let $x_1, \dots, x_m$ represent distinct orbits. We choose labelling s.t. $x_1, \dots, x_k$ are precisely the fixed points, i.e. $|\langle x_i \rangle| = 1$ for $1 \leq i \leq k$, $|\langle x_j \rangle| > 1$ for $j > k$

i.e. label fixed points first. Apply class equation: $|X| = \frac{|G|}{|G_{x_1}|} + \frac{|G|}{|G_{x_2}|} + \dots + \frac{|G|}{|G_{x_k}|} + \sum_{j>k} \frac{|G|}{|G_{x_j}|} = k + \sum_{j>k} \frac{|G|}{|G_{x_j}|} \because \frac{|G|}{|G_{x_i}|} = 1 \ \forall 1 \leq i \leq k$.

We know that $|G| = p^n$, G_{x_j} is a subgroup of G. Also, $j > k \Rightarrow G_{x_j} \neq G \Rightarrow$ by Lagrange's theorem, $|G_{x_j}| = p^{e_j}$, $e_j < n$.

Then $|X| = k + \sum_{j>k} p^{n-e_j}$ where $n - e_j \geq 1$. Take mod $p \Rightarrow |X| \equiv k \pmod p$. But $k = |X^G|$, so $|X| \equiv |X^G| \pmod p$ // q.e.d.

Theorem (Wilson's theorem).

If p is a prime, $k \in \mathbb{N}$, then $\binom{kp^n}{p^n} \equiv k \pmod p$.

Proof – Let G be a group with $|G| = p^n$. Let $k \geq 1$. Put $X = G \times \{1, 2, \dots, k\}$. Then $(h, r) \in X$ where $h \in G$, $1 \leq r \leq k \Rightarrow |X| = kp^n$.

We define the action $\cdot : G \times X \to X$ s.t. $g \cdot (h, r) = (gh, r)$ i.e. G leaves second factor untouched. Then we define another set:

$\mathcal{X} = \{A \subset X : |A| = p^n\}$, where $\mathcal{X}$ denotes the set of all subsets with p^n elements (not necessarily groups). Clearly, $|\mathcal{X}| = \binom{kp^n}{p^n}$.

Denote the group action $*: G \times \mathcal{X} \to \mathcal{X}$, where $g * A = \{g * a : a \in A\}$. So by what we have just proven, $|\mathcal{X}| \equiv |\mathcal{X}^G| \pmod p$.

Recall that $A \subset X = G \times \{1, \dots, k\}$, with $|A| = p^n$. Imagine we fix a value of $1 \leq r \leq k$, then $G \times \{r\}$ is a fixed point $\because g \cdot (h, r) = (gh, r)$.

Now, we suppose A is a fixed point of $\mathcal{X}$, and $(h, r) \in A$. If $(h', s) \in A$ also, we claim $r = s$: consider $g(h, r) = (gh, r)$. A is fixed, so

$(gh, r) \in A$ $\forall g \in G$. Then $G \times \{r\} \subset A$. However, $|G \times \{r\}| = |A| = p^n$, so $G \times \{r\} = A$. $(h', s) \in A$ with $h' \in G$, so $s = r$ indeed.

This tells us that the only possible fixed points of $\mathcal{X}$ are sets $G \times \{r\}$, $1 \leq r \leq k$. Hence $|\mathcal{X}^G| = k$, and $|\mathcal{X}| \equiv |\mathcal{X}^G| \equiv k \pmod p \Rightarrow \binom{kp^n}{p^n} \equiv k \pmod p$ // q.e.d.

With all this preliminary groundwork put into place, we are finally in a position to begin proving Sylow's theorem:

Recall – (Sylow's Theorems: I). Let p be prime, G be a group s.t. $|G| = kp^n$, $\gcd(k,p)=1$. Then G has a subgroup H with $|H| = p^n$.

Proof – Define set $X = \{A \subset G : |A| = p^n\}$, where A is a subset (not necessarily subgroup of G. Then $|X| = \binom{kp^n}{p^n}$. Perform induction on k.

If $k=1$, nothing to prove (trivially true). So we assume hypothesis is true for groups of order $k'p^n$, where $k'<k$. Let G act on X by $\cdot : G \times X \to X$,

with $g \cdot A = \{ga : a \in A\}$. If $k>1$ then this action has no fixed point: because if A is fixed, $a \in A$, we get a mapping $G \to A$ by $g \mapsto g\cdot a$.

Then mapping would be injective i.e. $g\cdot a = h \cdot a \Rightarrow g=h$ (multiply on right by a^{-1}). $\overset{|G|=kp^n}{G} \to \overset{|A|=p^n}{A}$ and $kp^n \leq p^n \Rightarrow k=1$.

Apply class equation. Let $A_1, \dots, A_m$ represent distinct orbits, then $\binom{kp^n}{p^n} = |X| = \sum_{i=1}^{m} \frac{|G|}{|G_{A_i}|}$. By Wilson's theorem, $\binom{kp^n}{p^n} \equiv k \pmod p \Rightarrow \sum_{i=1}^{m} \frac{|G|}{|G_{A_i}|} \equiv k \pmod p$.

By Lagrange's theorem, $|G_{A_i}| = k_i p^{e_i}$, $k_i | k$, $e_i \leq n$. $\frac{|G|}{|G_{A_i}|} = \left(\frac{k}{k_i}\right) p^{n-e_i}$. If each $e_i < n$, $n-e_i>0 \Rightarrow$ RHS $\equiv 0 \pmod p$, LHS $\equiv k \not\equiv 0 \pmod p$.

This is a contradiction $\therefore$ at least one $G_{A_i} = k_i p^n$, $k_i \leq k$. If $k_i = k$, A_i is a fixed point $\Rightarrow$ contradiction, so $k_i < k$.

Now G_{A_i} is a subgroup of $G \Rightarrow |G_{A_i}| = k_i p^n$ where $k_i<k$. By induction, G_{A_i} has a subgroup H, $|H| = p^n$. Hence $H \leq G_{A_i} \leq G$,

and H is also a subgroup of $G \Rightarrow G$ has a subgroup of order p^n // q.e.d.

22 February 2013
Prof FEA Johnson.
Roberts 106.

We will get to (Sylow's theorems: II). If N_p = number of groups of order p^n, then $N_p \equiv 1 \pmod p$, after some more background –

Let G be a group, $K \triangleleft G$ i.e. ($\forall g \in G\ \forall k \in K$, $gkg^{-1} \in K$. Define <u>quotient group</u> $G/K = \{gK : g \in G\}$. (rule of equality: $g_1K = g_2K \Leftrightarrow g_2^{-1}g_1 \in K$). In general, G/K is a set.

[Proposition] If $K \triangleleft G$, then G/K is "naturally a group", i.e. the multiplication $* : G/K \times G/K \to G/K$, $(g_1K) * (g_2K) = g_1g_2K$ is well-defined.

Proof – NTP: if $g_1K = h_1K$ and $g_2K = h_2K$, then $g_1g_2K = h_1h_2K$. Suppose $g_1K = h_1K$, $g_2K = h_2K$, then $h_1^{-1}g_1$, $h_2^{-1}g_2 \in K$. Then we see that

$(h_1h_2)^{-1}(g_1g_2) = h_2^{-1}h_1^{-1}g_1g_2 = h_2^{-1}(g_2g_2^{-1})h_1^{-1}g_1g_2 = (h_2^{-1}g_2)[g_2^{-1}(h_1^{-1}g_1)g_2]$. Then $h_1^{-1}g_1 \in K$ so $(g_2^{-1})(h_1^{-1}g_1)(g_2^{-1})^{-1} \in K$ by normality of K. Also $h_2^{-1}g_2 \in K$.

Hence, $(h_1h_2)^{-1}(g_1g_2) \in K \Rightarrow (g_1g_2)K = (h_1h_2)K$ // q.e.d.

Note: This only works because when $h_1^{-1}g_1 \in K$, $g_2^{-1} \in G$, $g_2^{-1}(h^{-1}g_1)g_2 \in K$, using fact that $K \triangleleft G$. If K is not normal, proof breaks down.

NTP: The above well-defined product gives a group multiplication on G/K. Let $(g_1K) * (g_2K) = g_1g_2K$.

- $*$ is associative: $(g_1K * g_2K) * g_3K = g_1g_2K * g_3K = (g_1g_2)g_3K = g_1(g_2g_3)K = g_1K * (g_2g_3K) = g_1K * (g_2K * g_3K)$
- G/K has identity element in $*$, namely $K = 1\cdot K$ $\because$ $(g\cdot K) * (1 \cdot K) = (g \cdot 1)K = (1 \cdot g)K = (1\cdot K) * (g \cdot K)$.
- G/K has inverses in $*$: $(gK) * (g^{-1}K) = (gg^{-1})K = K = (g^{-1}g)K = (g^{-1}K) * gK$.

So if $K \triangleleft G$, G/K is "naturally" a group // q.e.d.

Notice that the mapping $\natural : G \to G/K$, $\natural(g) = gK$ is a group homomorphism: $\natural(g_1g_2) = \natural(g_1)\natural(g_2)$, $\mathrm{Ker}(\natural) = K$.

Unfinished business from earlier –
(Noether's Zeroth Isomorphism Theorem).

[Proposition] Let $\varphi : G \to H$ be a group homomorphism and let $\varphi_* : G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$ be $\varphi_*(g\,\mathrm{Ker}(\varphi)) = \varphi(g)$. Then $\varphi_* : G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$ is a group homomorphism.

Proof – We have earlier already shown that φ_* is a well-defined bijection. Only need to check that φ_* is a homomorphism. Let $K = \mathrm{Ker}(\varphi)$

$\varphi_* : G/K \to \mathrm{Im}(\varphi)$, $\varphi_*(gK) = \varphi(g)$. $\varphi_*(g_1K * g_2K) = \varphi_*(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi_*(g_1K)\varphi_*(g_2K)$

So if $\varphi : G \to H$ is a group homomorphism, $G/\mathrm{Ker}(\varphi) \xrightarrow{\cong} \mathrm{Im}(\varphi)$.

Note: In MATH1201, this was presented alternatively as the Rank-Nullity theorem. If $T : V \to W$ is a linear map, $T_* : V/\mathrm{Ker}(T) \xrightarrow{\cong} \mathrm{Im}(T)$, i.e.

$\dim(V) - \dim \mathrm{Ker}(T) = \dim \mathrm{Im}(T)$.

[Ex] Let $G = D_6 = \langle x, y \mid x^3 = y^2 = 1, yx = x^2y \rangle$. Show that G/K is naturally a group but G/H is not, where $K = \{1, x, x^2\}$, $H = \{1, y\}$

Soln. $K \triangleleft G$, so G/K is well-defined, $G/K \cong C_2$ // q.e.d. H is not normal in G, so G/H is not naturally a group. // q.e.d.

[Ex] Let $G = Q(8) = \{1, -1, i, -i, j, -j, k, -k\}$ $i^2 = j^2 = k^2 = 1$, $ij = -ji = k$. Find $Q(8)/\{\pm 1\}$.

Soln. Put $K = \{1, -1\}$, then $K \triangleleft Q(8)$. So $Q(8)/\{\pm1\}$ is a well-defined group of order 4: either C_4 or $C_2 \times C_2$.

To check, we see that $Q(8)/K = \{K, iK, jK, \underset{(iK)(jK)}{kK}\}$. Every element has order 2, so $Q(8)/\{\pm 1\} \cong C_2 \times C_2$ //.

<u>Noether's First Isomorphism Theorem</u>

[Definition] Suppose P, Q are subgroups of G. We say that P <u>normalises</u> Q when $\forall p \in P\ \forall q \in Q$, $pqp^{-1} \in Q$.

[Proposition] Suppose P, Q are subgroups of G. P normalises $Q \Rightarrow PQ = \{pq : p \in P, q \in Q\}$ is a subgroup of G and $Q \triangleleft PQ$.

Proof – Let $p_1q_1 \in PQ$, $p_2q_2 \in PQ$. Then $(p_1q_1)(p_2q_2) \in PQ$. $(p_1q_1)(p_2q_2) = (p_1p_2)(p_2^{-1}q_1p_2)q_2$. $p_1p_2 \in P$ and $p_2^{-1}q_1p_2 \in Q$ (P normalises Q) so $p_2^{-1}q_1p_2q_2 \in Q$.

Then $(p_1q_1)(p_2q_2) = \underset{P}{(p_1p_2)}\underset{Q}{(p_2^{-1}q_1p_2q_2)}$. If $q \in Q$, $p_1q_1 \in PQ$. $(p_1q_1)q(p_1q_1)^{-1} = p_1[q_1qq_1^{-1}]p_1^{-1}$. $q_1qq_1^{-1} \in Q$, $q, q_1 \in Q$.

$p_1[q_1qq_1^{-1}]p_1^{-1} \in Q$. P normalises Q. So $Q \triangleleft PQ$ // q.e.d.

$\boxed{\text{Theorem}}$ (Noether's First Isomorphism theorem).

P, Q are subgroups of G and P normalises Q. Then $PQ/Q \cong P/P\cap Q$.

Proof - Define $c: P \to (PQ)/Q$ by $c(p) = pQ$. We claim that (1) c is a homomorphism (2) c is surjective (3) $\mathrm{Ker}(c) = P\cap Q$.

(1) By definition, $c(p_1p_2) = p_1p_2Q$. $c(p_1)c(p_2) = (p_1Q)(p_2Q) = p_1(Qp_2)Q$. [$P$ normalises Q, so $Qp_2 = p_2Q$] so $= (p_1p_2)QQ = p_1p_2Q$.

(2) c is surjective: If $p_1q_1Q \in PQ/Q$, then $p_1q_1Q = p_1Q$, $q_1 \in Q$. So $p_1q_1Q = c(p_1)$ // q.e.d.

(3) $\mathrm{Ker}(c) = \{p \in P, pQ = Q\}$. Q = identity in PQ/Q. Now $pQ = Q \Leftrightarrow p \in Q$. But $p \in P$, so $p \in P\cap Q$. $\mathrm{ker}(c) = P\cap Q$.

So by Noether's zeroth isomorphism, $\mathrm{Im}(c) \cong P/P\cap Q = P/\mathrm{Ker}(c)$. But $\mathrm{Im}(c) = PQ/Q$ so $PQ/Q \cong P/P\cap Q$ // q.e.d.

26 February 2013.
Prof Frank EA JOHNSON.

Recall - (Sylow's Theorems: II) Let G be a finite group, $|G| = kp^n$ with p prime, $\gcd(k,p) = 1$. Let N_p be the number of subgroups of order p^n. Then $N_p \equiv 1$ (p). Roberts Gob.

Proof - Let $S = \{H : H \text{ is a subgroup of } G, |H| = p^n\}$. Then $N_p = |S|$. By Sylow Part I, $S \neq \phi$, so let $P \in S$, i.e. P is a specific subgroup of G, $|P| = p^n$.

Let P act on S by $P\times S \to S$, $p * Q = pQp^{-1}$. We calculate S^P, the fixed point set. So suppose $Q \in S^P$. i.e. $\forall p \in P$, $pQp^{-1} = Q$.

So P normalises Q, and PQ is a subgroup of G. We need to calculate $|PQ|$. We know that $PQ/Q \cong P/P\cap Q$.

So $|PQ| = |PQ/Q||Q| = \underbrace{|P/P\cap Q||Q|}_{-(*)}$. $|P| = p^n \Rightarrow P\cap Q$ is a subgroup of P, so $|P\cap Q| = p^m$ for some m $(0 \le m \le n)$.

So $|P| = |P/P\cap Q||P\cap Q| \Rightarrow p^n = |P/P\cap Q|p^m \Rightarrow |P/P\cap Q| = p^e$ where $m+e=n$, $0 \le e \le n$. From $(*)$, $|PQ| = p^e|Q| = p^ep^n$.

$\Rightarrow |PQ| = p^{n+e}$. But PQ is a subgroup of G, and p^n is the highest power of p dividing G. By Lagrange's Theorem, $e = 0 \Rightarrow$

$|PQ| = p^n$. But $P \subset PQ$, $|P| = |PQ|$ so $P = PQ$. Also, $Q \subset PQ$, $|Q| = |PQ| = p^n$. so $Q = PQ$. $\therefore P = Q$.

so $\underset{\in S}{P}$ is the unique fixed point under the action. $|P| = p^n$. then $|S| \equiv |S^P| \pmod p \Rightarrow N_p \equiv 1 \pmod p$ // q.e.d.

We will not further investigate the proofs for Sylow's Theorems III and IV, which are beyond the scope of our course.

This marks the end of the formal group theory component of the course, and we now look at RING THEORY. (the other part of the course).

Ring theory

Consider the mapping $(X, *)$. $*: X\times X \to X$ with $(x,y) \mapsto x*y$. We normally put down some restrictions:

(I) Associativity: $x*(y*z) = (x*y)*z$. A set X with an associative multiplication $*$ is called a <u>semigroup</u>.

(II) Identity element: $\exists 1 \in X$ s.t. $\forall x \in X$, $x*1 = 1*x = x$.

$(X,*)$ satisfying (I) and (II) is called a <u>monoid</u>.

(III) Inverses: $\forall x \in X$, $\exists x^{-1} \in X$ s.t. $x * x^{-1} = x^{-1} * x = 1$.

A set $(X,*)$ satisfying (I), (II), (III) is, as we know, called a group. We have developed a substantial amount of theory for groups.

We can also add a fourth axiom to restrict our concerns to <u>abelian groups</u>.

(IV) Commutativity: $\forall x,y \in X$, $x*y = y*x$. Abelian groups are simpler structures than general groups — there are no real problems left unsolved in the discipline.

We now consider sets with two operations —

$\boxed{\text{Definition}}$ By a <u>ring</u> R we mean $R = (R, +, 0, \cdot, 1)$ where

i) R is a set, $0 \in R$, $1 \in R$, $1 \neq 0$.

ii) $(R, +, 0)$ is an additive abelian group.

iii) $(R, \cdot, 1)$ is a multiplicative monoid (i.e. it is associative, with 1 as the identity)

iv) $\forall a,b,c \in R$, $(a+b)\cdot c = a\cdot c + b\cdot c$, $c\cdot(a+b) = c\cdot a + c\cdot b$. (Distributive axioms)

$\boxed{\text{Ex}}$ Show that $\overset{(1)}{\mathbb{Z}} = (\mathbb{Z}, +, 0, \cdot, 1)$ is a ring. Likewise $\overset{(2)}{\mathbb{Q}} = \{\frac{m}{n} : m,n \in \mathbb{Z}, n \neq 0.$ $\overbrace{\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow mn' = m'n}^{\text{(rule of equality)}}\}$

Soln. (1) $(a\cdot b)\cdot c = a\cdot(b\cdot c)$, $(a+b)\cdot c = a\cdot c + b\cdot c$, etc... so $\mathbb{Z}$ is a ring

(2) $\mathbb{Q}$ is also a ring. It is not typical as it has properties that also make it a field; that of multiplicative inverses:

$\forall x \in \mathbb{Q}$, $x \neq 0$ $\exists x^{-1} \in \mathbb{Q}$. $xx^{-1} = 1 = x^{-1}x$. A ring satisfying multiplicative inverses is called a <u>division ring</u>.

$\boxed{\text{Definition}}$ A field $\mathbb{F}$ is a division ring whose multiplication is also commutative.

For example, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. As an example of a non-commutative division ring (by contrast) take $\mathbb{H} = \{x_0\cdot 1 + x_1\cdot i + x_2 j + x_3 k \,;\, x_i \in \mathbb{R}\}$.

This is the set of <u>Hamiltonian quartenions</u> (or <u>hypercomplex numbers</u>). $\dim_{\mathbb{R}} \mathbb{H} = 4$ with unit basis $1, i, j, k$ with $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$.

$\underset{\sim}{x} = x_0\cdot 1 + x_i\cdot i + x_2 j + x_3 k$, $\|x\| = \sqrt{x_0^2 + x_1^2 + x_2^2 + x_3^2}$. $\bar{\underset{\sim}{x}} = x_0\cdot 1 - x_i i - x_2 j - x_3 k$. $x\bar{x} = \|x\|^2 \Rightarrow x^{-1} = \frac{\bar{x}}{\|x\|^2}$.

A typical non-commutative ring is $M_n(\mathbb{F}) = \{n\times n$ matrices over field $\mathbb{F}\}$. Here, $1 = I_n$, $0 =$ zero matrix.

Unless explicitly stated otherwise, through the length of this course rings will be assumed to be commutative: $\forall x,y \in R,\ x\cdot y = y\cdot x$.

$\boxed{\text{Definition}}$ Let R be a commutative ring. We say that R is an <u>integral domain</u> when $xy=0 \Rightarrow x=0$ or $y=0$.

For example: $\mathbb{Z}$, any $\mathbb{F}$ are integral domains. $\mathbb{F}[x]$, the ring of polynomials over $\mathbb{F}$ in one variable x is an integral domain. A polynomial over $\mathbb{F}$ in x is a formal expression:
$a(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$. $a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{F}$. Multiplication and addition of polynomials occur as per expectation: $\begin{cases} x^m x^n = x^{m+n} \\ 1\cdot x^n = x^n \end{cases}$

Note: Polynomials here are simply formal expressions — we are not considering them as functions!

Rule of Equality for polynomials: $\left.\begin{matrix} a(x) = a_n x^n + \dots + a_1 x + a_0 \\ b(x) = b_n x^n + \dots + b_1 x + b_0 \end{matrix}\right\}$ $a(x) = b(x) \Leftrightarrow \forall i,\ a_i = b_i$. $\mathbb{F}[x] = \{$polynomials over $\mathbb{F}$ in $x\}$.

$\boxed{\text{Proposition}}$ $\mathbb{F}[x]$ is an integral domain.

Proof – Suppose $a(x) = a_n x^n + \dots + a_1 x + a_0$ is a polynomial of order n (i.e. $a_n \neq 0$). $b(x) = b_m x^m + \dots + b_1 x + b_0$ (i.e. $b_m \neq 0$).

Then $a(x)b(x) = a_n b_m x^{n+m} +$ (terms in x^r, with $r < n+m$). If $a_n, b_m \neq 0$, $a_n, b_m \in \mathbb{F}$ so $a_n b_m \neq 0$ so $a(x)b(x) \neq 0$.

i.e. $(a(x)\neq 0) \wedge (b(x) \neq 0) \Rightarrow (a(x)b(x) \neq 0)$. In the contrapositive, $a(x)b(x) = 0 \Rightarrow (a(x)=0) \vee (b(x)=0) \Rightarrow \mathbb{F}[x]$ is an integral domain // q.e.d.

$\mathbb{F}[x]$ behaves very much like $\mathbb{Z}$.

<u>Ideals and Quotient Rings</u>

Let R be a commutative ring. By an <u>ideal</u> $I \subset R$ we mean (i) I is an additive subgroup of R, and (ii) $\forall x \in I\ \forall \lambda \in R,\ \lambda x \in I$.

$\boxed{\text{Ex}}$ Let R be a commutative ring, $a \in R$. Define $\boxed{(a) = \{\mu a : \mu \in R\}}$. [Proposition]: Show that (a) is an ideal in R.

Soln. Let $x, y \in (a)$, so $x = \mu_1 a$, $y = \mu_2 a$; where $\mu_1, \mu_2 \in R$. Then $x + y = (\mu_1 + \mu_2)a$, $-x = (-\mu_1)a$, $0 = 0\cdot a \Rightarrow (a)$ is additive subgroup.

If $x = \mu a \in (a)$ and $\lambda \in R$, $\lambda x = (\lambda\mu)a \in (a)$, so (a) is an ideal in R // q.e.d.

Note: In the context of ring theory, we write $I \trianglelefteq R$ when I is an ideal in R. In general, an ideal does not contain 1.

For instance, take $R = \mathbb{Z}$. Then $(2) = \{2x : x \in \mathbb{Z}\} = \{$even integers$\}$. $(n) = \{nx : x \in \mathbb{Z}\} = \{$multiples of $n\}$.

Quotient Construction:

Let R be a commutative ring and $I \trianglelefteq R$. We form $R/I = \{x + I : x \in R\}$ as an additive coset. We apply rule of equality for additive cosets: $\boxed{x+I = x'+I \Leftrightarrow x - x' \in I}$

We also have addition on R/I: $(x+I)+(y+I) = x+y+I$. So R/I is a group under addition.

Likewise we have multiplication on R/I: define $(x+I)(y+I) = xy + I$

$\boxed{\text{Proposition}}$ The above multiplication is well-defined if $I \trianglelefteq R$.

Proof – NTP: If $x + I = x' + I$, $y + I = y' + I$; then $xy + I = x'y' + I$. We begin by evaluating $xy - x'y' = x(y-y') + (x-x')y = x(y-y') + y(x-x')$.

$y - y' \in I \Rightarrow x(y-y') \in I$. $x - x' \in I \Rightarrow y(x-x') \in I$, so $xy - x'y' \in I$, i.e. $xy + I = x'y' + I$ // q.e.d.

$\boxed{\text{Proposition}}$ If $I \trianglelefteq R$, then R/I is naturally a ring.

Proof – R/I has addition and multiplication. $\times$ is associative: $(x+I)[(y+I)(z+I)] = (x+I)(yz+I) = x(yz)+I = (xy)z + I = [(x+I)(y+I)](z+I)$.

We check easily that distributive axioms hold // q.e.d.

For example, $R = \mathbb{Z}$, $I = (3) =$ multiples of 3. There are three distinct cosets $\mathbb{Z}/(3)$; namely (3) itself, $(3) = \{3\lambda : \lambda \in \mathbb{Z}\}$. In addition, it has
$1 + (3) = \{3\lambda + 1 : \lambda \in \mathbb{Z}\}$, $2 + (3) = \{3\lambda + 2 : \lambda \in \mathbb{Z}\}$. We write $[0] = (3)$, $[1] = \{3\lambda+1 : \lambda \in \mathbb{Z}\}$, $[2] = \{3\lambda + 2 : \lambda \in \mathbb{Z}\}$

We also get the multiplication table as on the right: $[2][2] = 2\cdot 2 + (3) = 4 + (3) = 1 + 3 + (3) = 1 + (3)$ $\because 3 \in (3)$ $= [1]$

•	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1].

$\mathbb{Z}/(3)$ is the field $\mathbb{F}_3$, with 3 elements.

1 March 2013.
Prof FEA JOHNSON.
Roberts 106.

Consider $\mathbb{Z}/(5)$. $(5) = \{5m : m \in \mathbb{Z}\}$. Then $\mathbb{Z}/(5)$ has 5 elements: (5), $1+(5)$, $2+(5)$, $3+(5)$, $4+(5)$, where (say) $2+(5) = \{5\lambda + 2 : \lambda \in \mathbb{Z}\}$.

The elements of $\mathbb{Z}/5$ simply correspond to possible remainders mod 5: 0, 1, 2, 3, 4. The practical way to compute on $\mathbb{Z}/5$ is to add and multiply as usual, but set $5 \equiv 0$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3.

We also create the multiplication table of $\mathbb{Z}/(5)$, as shown. Thus, we observe that $\mathbb{Z}/(5)$ is a field.

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Then, we try $\mathbb{Z}/(4)$ ($\cong \mathbb{Z}/4$). We leave out the zero rows as they are trivial. Then, we get:

•	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1.

Clearly, $\mathbb{Z}/4$ is not a field. It is not an integral domain: $2 \neq 0$, but $2\cdot 2 = 0$.

In summary, we have seen that $\mathbb{Z}/3, \mathbb{Z}/5$ are fields but $\mathbb{Z}/4$ is not.

In effect, this gives us a statement about $\mathbb{Z}/(n)$ being an integral domain:

Proposition $\mathbb{Z}/(n)$ is an integral domain $\Leftrightarrow$ n is prime.

Proof – Let n be composite, then we can factorise $n=ab$, $1<a<n$, $1<b<n$. Let $[a]=a+(n)$, $[b]=b+(n)$ (additive cosets). Then we have $[a][b]=(a+(n))(b+(n))=ab+(n)=n+(n)=(n)=[0]$. $[a][b]=[0]$ but $[a],[b]\neq 0 \Rightarrow \mathbb{Z}/(n)$ is not an integral domain // q.e.d.

Conversely, let n be prime. $[a][b]=0 \Rightarrow ab=kn$ for some k. Since n is prime, by uniqueness of prime factorisation, $n|a$ or $n|b$.

Hence, $[a][b]=0 \Rightarrow a=kn$ or $b=kn \Rightarrow a=0$ or $b=0 \Rightarrow \mathbb{Z}/(n)$ is an integral domain // q.e.d.

Proposition Let A be a finite integral domain. Then A is a field.

Proof – Let $a\in A$, $a\neq 0$. NTP: $\exists a^{-1}\in A: aa^{-1}=1$. Consider the mapping $\lambda_a: A\to A: \lambda_a(x)=ax$. Claim that λ_a is injective: suppose $\lambda_a(x)=\lambda_a(y) \Rightarrow ax=ay \Rightarrow a(x-y)=0$. By hypothesis, $a\neq 0$. Since A is an integral domain, $x-y=0 \Rightarrow x=y$. Since $\lambda_a: A\to A$ is injective, finiteness of $A \Rightarrow \lambda_a$ is surjective.

Hence, $\exists x\in A$ s.t. $\lambda_a(x)=1$, $ax=1$, $a=x^{-1}$ // q.e.d.

Corollary $\mathbb{Z}/n$ is a field $\Leftrightarrow$ n is prime.

Proof – Trivial.

Usual notation: We write $\mathbb{F}_p=\mathbb{Z}/(p)$ iff p is prime. Note that $\mathbb{F}_4\neq\mathbb{Z}/(4)$! Beware...

<u>The field of 4 elements, $\mathbb{F}_4$.</u>

Begin construction with the ring $\mathbb{F}_2[x]$. Then $\mathbb{F}_2[x]=\{a_nx^n+\dots+a_1x+a_0: a_i\in\mathbb{F}_2\}$. Consider $\mathbb{F}_2[x]/(x^2+x+1)$, where we have $(x^2+x+1)=\{a(x)\cdot(x^2+x+1): a(x)\in\mathbb{F}_2[x]\}$. We represent the cosets in $\mathbb{F}_2[x]/(x^2+x+1)$ by possible remainders after dividing by x^2+x+1.

If we divide a polynomial with degree ≥ 2 by x^2+x+1, in general we will get polynomials of degree ≤ 1 as possible remainders.

After dividing by x^2+x+1, we get 4 possible remainders: $\{0,1,x,x+1\}$. We do up the multiplication table:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x.

$x\cdot x=x^2$, which is not on list. Set $x^2+x+1\equiv 0$, then $x^2\equiv -x-1\equiv x+1$. Hence, we replace x^2 by $x+1$. $x(x+1)=x^2+x=x+1+x=2x+1=1$.

Clearly, this generates a field with 4 elements — developed by Galois in 1829.

Definition Let R be a group. The <u>unit group</u> R^* (or $U(R)$) with $R^*=\{a\in R: \exists b\in R \text{ s.t. } ab=1\}$.

It is the group of invertible elements under multiplication.

Ex Show that $\mathbb{F}_2[x]/(x^2+1)$ is not a field.

Soln. Represent cosets by polynomials of degree ≤ 1. $(x+1)(x+1)=x^2+2x+1=x^2+1=0$. However, $x+1\neq 0$, so $\mathbb{F}_2[x]$ is not an integral domain $\Rightarrow$ not a field.

We know that for the field $\mathbb{Z}$, the set of quotients $\mathbb{Z}/n$ is a field $\Leftrightarrow$ n is prime. By intuitive analogy: for the field $\mathbb{F}[x]$, the set of quotients $\mathbb{F}[x]/p(x)$ is a field $\Leftrightarrow$ $p(x)$ is irreducible

This will be formally proven later on.

Recall that if $p(x)\in\mathbb{F}[x]$, $p(x)\neq 0$; $p(x)$ is irreducible on $\mathbb{F}$ $\Leftrightarrow$ we cannot write $p(x)=a(x)b(x)$ where $\deg(a)<\deg(p)$ and $\deg(b)<\deg(p)$.

For instance, if $\mathbb{F}=\mathbb{R}$, consider $\mathbb{R}[x]/p(x)$. x^2+1 is irreducible over $\mathbb{R}$. Then $\mathbb{R}[x]/(x^2+1)$: we can represent elements as polynomials of degree ≤ 1.

$(a+bx)(c+dx)=ac+(bd)x^2+(ad)(bc)x$. But $x^2+1\equiv 0 \Rightarrow x^2=-1$. Then $(ac-bd)+(ad+bc)x$. Since $x^2=-1$, write $x=i$!

Then $(a+bi)(c+di)=(ac-bd)+(ad+bc)x \Rightarrow \mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$.

5 March 2013.
Prof FEA JOHNSON.
Roberts G06.

Consider $\mathbb{F}[x]/(p(x))$, where $\mathbb{F}$ is a field, $p(x)$ is a polynomial over $\mathbb{F}$. Assume $\deg(p)\geq 2$ for sake of non-triviality:

$(p(x))=\{c(x)p(x): c(x)\in\mathbb{F}[x]\}$. An element of $\mathbb{F}[x]/(p(x))$ is a coset $a(x)+(p(x))$.

Rule of equality: $a(x)+(p(x))=b(x)+(p(x)) \Leftrightarrow a(x)-b(x)=c(x)p(x)$ for some $c(x)$. i.e. $a(x)-b(x)$ is divisible by $p(x)$.

Recall the division algorithm for polynomials: If $A(x)\in\mathbb{F}[x]$, and $\deg A(x)\geq\deg p(x)$, then $A(x)=q(x)p(x)+r(x)$ where $\deg r<\deg p$. ($q(x), r(x)$ uniquely determined by $A(x)$, $p(x)$).

So the coset $A(x)+(p(x))$ is identical to the coset $r(x)+(p(x)) \Rightarrow$ every coset in $\mathbb{F}[x]/(p(x))$ can be represented uniquely in the form $r(x)+(p(x))$, where $\boxed{\deg r(x)<\deg p(x)}$.

Corollary $\exists$ natural 1-1 correspondence $\mathbb{F}[x]/(p(x)) \longleftrightarrow$ polynomials on $\mathbb{F}[x]$ with degree $<\deg p$.

Evidently $\mathbb{F}[x]/(p(x))$ is a vector space over $\mathbb{F}$, $p(x)=c_nx^n+\dots+c_1x+c_0$, $c_n\neq 0$. Elements of $\mathbb{F}[x]/(p(x))$ look like $a(x)=a_nx^{n-1}+\dots+a_1x+a_0+(p(x))$.

Proposition $\dim_{\mathbb{F}}(\mathbb{F}[x]/(p(x)))=\deg p(x)$.

Proof – By simple counting // q.e.d.

Ex Let $\mathbb{F}_2$ be the field with 2 elements, $\{0,1\}$. Compute the multiplicative monoid of $\mathbb{F}_2[x]/(x^3+1)$.

Soln. As basis for $\mathbb{F}_2[x]/(x^3+1)$, we take $\{1,x,x^2\}$: dim $=3$. Hence $\mathbb{F}_2[x]/(x^3+1)$ has 8 elements: $0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1+(x^3+1)$.

We then compute the multiplicative monoid, with $x^3+1\equiv 0 \Rightarrow x^3\equiv -1\equiv 1$ ($\because -1\equiv 1$ in $\mathbb{F}_2$).

7202-1L.

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	1	$x+1$	x^2+1	x^2+x+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+1	x^2+x	$x+1$	0
x^2	0	x^2	1	x^2+1	x	x^2+x	$x+1$	x^2+x+1
x^2+1	0	x^2+1	$x+1$	x^2+x	x^2+x			
x^2+x	0	x^2+x	x^2+1	$x+1$	$x+1$			
x^2+x+1	0	x^2+x+1	x^2+x+1	0	x^2+x+1			x^2+x+1

Special calculations: $x^2 \cdot x = x^3 \equiv 1$. $(x+1)(x^2+1) = x^3+x^2+x+1 = x^2+x$

$(x^2+x+1)(x+1) = x^3+x^2+x+x^2+x+1 = x^3+1 = 0$.

$(x^2+x+1)(x^2+x+1) = x^4+x^3+x^2+x^3+x^2+x+x^2+x+1 = x^4+x^2+1 = x^2+x+1$

Clearly then, $\mathbb{F}_2[x]/(x^3+1)$ does not produce a field. The only invertible elements are $1, x, x^2$.

Multiplicative group is C_3.

Note: in this case, we do not get a field because $(x+1)(x^2+x+1) \equiv x^3+1 \equiv 0$ over $\mathbb{F}_2 \Rightarrow x^3+1$ is reducible in $\mathbb{F}_2$!

We will show the following –

$\boxed{\text{Theorem}}$ Let $\mathbb{F}$ be a field. Then if $p(x)$ is a polynomial with $\deg p \geq 1$, $\mathbb{F}[x]/(p(x))$ is a field $\Leftrightarrow$ $p(x)$ is irreducible over $\mathbb{F}$.

Proof – $\boxed{\text{Proposition}}$. We will first prove that $\mathbb{F}[x]/(p(x))$ is an integral domain $\Leftrightarrow$ $p(x)$ is irreducible over $\mathbb{F}$.

Proof:

Observe that if $p(x)$ is reducible over $\mathbb{F}$, then it has a proper factorisation: $p(x) = a(x)b(x)$, where $\deg(a), \deg(b) < \deg(p)$.

Write $[a]$ for coset of a: $[a] = a(x) + (p(x))$, and $[b]$ for coset of b: $[b] = b(x) + (p(x))$.

Then $[a][b] = a(x)b(x) + (p(x)) = p(x) + (p(x)) = (p(x)) = 0$. As $p(x) \neq 0$, then $a(x) \neq 0$, $b(x) \neq 0$. $\Rightarrow [a], [b] \neq 0$ but $[a][b] = 0$.

So $\mathbb{F}[x]/(p(x))$ is not an integral domain. Take contrapositive: $\mathbb{F}[x]/(p(x))$ integral domain $\Rightarrow$ $p(x)$ is irreducible.

Conversely suppose $p(x)$ is irreducible. Let $a(x), b(x) \in \mathbb{F}[x]$ and suppose $[a][b] = 0$ in $\mathbb{F}[x]/(p(x))$ i.e. $a(x)b(x) \in (p(x)) \Rightarrow a(x)b(x) = q(x)p(x)$ for some $q(x) \in \mathbb{F}[x]$. Write $a(x)$ as a product of irreducibles: $a(x) = a_1(x)a_2(x)\cdots a_m(x)$. Likewise $b(x) = b_1(x)b_2(x)\cdots b_k(x)$, $a_i(x)$, $b_j(x)$ irreducible.

Then $a_1(x)\cdots a_m(x)b_1(x)\cdots b_k(x) = p(x)\cdot q(x)$. Since $p(x)$ is irreducible, by uniqueness of factorisation into irreducibles, either $\overset{1)}{a_i(x)} = Ap(x)$, A const., or $\overset{2)}{b_j(x)} = Bp(x)$, B const. for some i, j. If 1) $a(x) \in (p(x))$ so $[a] = 0$; if 2) $b(x) \in (p(x))$ so $[b] = 0$ $\Rightarrow$ $[a][b] = 0$ means $[a] = 0$ or $[b] = 0$.

Hence, $\mathbb{F}[x]/(p(x))$ is an integral domain // q.e.d.

$\boxed{\text{Proposition}}$

Let A be a commutative integral domain, and suppose $\overset{(i)}{A}$ contains a subring $\mathbb{F}$ which is a field, and $\overset{(ii)}{\dim_{\mathbb{F}}} A$ is finite. Then A is a field.

Proof:

Let $a \in A$, $a \neq 0$. Need to produce $b \in A$ st. $ab = 1$. Let $\lambda_a : A \to A$ be the mapping $\lambda_a(x) = ax$. λ_a is linear over $\mathbb{F} \subset A$.

$\because$ $\lambda_a(x+y) = \lambda_a(x) + \lambda_a(y)$, $\lambda_a(\xi x) = a(\xi x) = (a\xi)x = (\xi a)x = \xi(ax) = \xi\lambda_a(x)$ $\forall \xi \in \mathbb{F}$. $\dim_{\mathbb{F}} A$ is finite, so we have

$\dim \operatorname{Ker} \lambda_a + \dim \operatorname{Im} \lambda_a = \dim A$. $\operatorname{Ker} \lambda_a = \{0\}$ $\because$ $\lambda_a(y) = 0 \Rightarrow ay = 0$. $a \neq 0 \Rightarrow y = 0$ $\because$ A is an integral domain. $\Rightarrow \dim \operatorname{Ker} \lambda_a = 0$

$\Rightarrow \dim \operatorname{Im} \lambda_a = \dim A$. $\operatorname{Im} \lambda_a \subset A$, so $\operatorname{Im} \lambda_a = A$. Hence, λ_a is surjective. $\therefore$ $\exists b \in A$ s.t. $\lambda_a(b) = 1 \Rightarrow ab = 1$ // q.e.d.

Beware: Proposition is false if $\dim A = +\infty$ e.g. $A = \mathbb{F}[x]$ is an integral domain, $\mathbb{F} \subset \mathbb{F}[x]$. $\dim \mathbb{F}[x] = +\infty$, $\mathbb{F}[x]$ is not a field.

Collecting our results: we get our theorem.

Alternative statement: Let $\mathbb{F}$ be a field, $p(x) \in \mathbb{F}[x]$, $\deg p \geq 1$. Then the following statements are equivalent:

(i) $\mathbb{F}[x]/(p(x))$ is a field, (ii) $\mathbb{F}[x]/(p(x))$ is an integral domain (iii) $p(x)$ is irreducible over $\mathbb{F}$.

(i) $\Rightarrow$ (ii) trivial, (ii) $\Leftrightarrow$ (iii) shown.

Proof – only remains to show (ii) $\Rightarrow$ (i): $\mathbb{F}[x]/(p(x))$ contains field $\mathbb{F}$ as cosets of constant polynomials. Also, $\dim \mathbb{F}[x]/(p(x)) = \deg p(x)$, which is finite.

$\therefore$ $\mathbb{F}[x]/(p(x))$ is a field // q.e.d.

So, to construct fields $\mathbb{F}[x]/(p(x))$, we need to know which $p(x) \in \mathbb{F}[x]$ are irreducible.

For instance, if $\mathbb{F} = \mathbb{R}$, the irreducible polynomials are (1) all polynomials of degree ≤ 1 and (2) $p(x) = x^2+bx+c$ where $b^2-4c < 0$.

If $\mathbb{F} = \mathbb{C}$, $p(x) \in \mathbb{C}[x]$, then the only irreducible polynomials $p(x)$ are those of degree 1: this is the Fundamental Theorem of Algebra. (first stated by d'Alembert).

Suppose $p(x) \in \mathbb{R}[x]$, we can factorise over $\mathbb{C}$: $p(x) = K(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_N)$. Since $p(x) \in \mathbb{R}[x]$, $p(x) = \overline{p(x)} \Rightarrow \bar{\lambda}_1 \in \{\lambda_1, \dots, \lambda_N\}$.

We can rewrite: $p(x) = K\underbrace{(x-\mu_1)(x-\bar{\mu}_1)\cdots(x-\mu_m)(x-\bar{\mu}_m)}_{\text{real quadratic}}(x-\nu_1)\cdots(x-\nu_k)$, $\nu_i \in \mathbb{R}$. This gives the result above for $\mathbb{F} = \mathbb{R}$.

We found earlier that x^2+1 is irreducible over $\mathbb{R}$, so $\mathbb{R}[x]/x^2+1$ is a field, specifically $\mathbb{C}$. $\mathbb{R}[x]/(x^2+1) = \{a+bx : a, b \in \mathbb{R}\}$. $x^2+1 \equiv 0 \Rightarrow x^2 \equiv -1$.

We also showed that $(a+bi)(c+di) = (ac-bd) + (ad+bc)x$.

Irreducibles over $\mathbb{Q}$:

Consider $\mathbb{Q}[x]/(x^2-2)$, x^2-2 is irreducible over $\mathbb{Q}$ (credit to Pythygoras). Irreducibles over $\mathbb{Q}$ are very complicated: the study of $\mathbb{Q}[x]/(p(x))$ is Algebraic Number Theory.

$\forall n$ $\exists \infty$ many irreducibles over $\mathbb{Q}$ of degree n.

$\boxed{\text{Theorem}}$ (Eisenstein's criterion).

Let $a(x) \in \mathbb{Z}[x]$ (integral polynomial), i.e. $a(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, $a_i \in \mathbb{Z}$.

Suppose there is a prime p such that: 1) $a_n \not\equiv 0 \bmod p$, 2) $a_r \equiv 0 \bmod p$, $0 \leq r < n$, 3) $a_0 \not\equiv 0 \bmod p^2$.

Then $a(x)$ is irreducible over $\mathbb{Q}$.

For instance, $2x^5+9x^4+27x^2+81x+6$ is irreducible over $\mathbb{Q}$: $p=3$. Likewise, $x^{10^{10}}+41x+41$ is irreducible etc.

Proof – will follow later.

8 March 2013.
Prof FEA Johnson
Roberts 106.

Ex Evaluate whether $2x^{10}+15x^5+25x^2+20x+15$ is reducible in $\mathbb{Q}$.

soln. It is irreducible by Eisenstein's criterion, by taking $p=5$.

Consider $f(x)\in\mathbb{Z}[x]$. Let $b\in\mathbb{Z}$. Then $f(x+b)$ is still a polynomial in x with integral coefficients i.e. $f(x+b)\in\mathbb{Z}[x]$.

Proposition Let $f(x)\in\mathbb{Z}[x]$, $b\in\mathbb{Z}$. Then $f(x)$ is irreducible $\Leftrightarrow$ $f(x+b)$ is irreducible.

Proof – Suppose $f(x+b)$ is reducible, $f(x+b)=g(x)h(x)$, so $f(x)=g(x-b)h(x-b)\Rightarrow f(x)$ is reducible. Proof is symmetric, replacing b by $-b$.

Ex Let $f(x)=x^7+7x^6+21x^5+35x^4+35x^3+21x^2+7x+38$. Show that this is irreducible over $\mathbb{Q}$.

soln. Set $g(x)=x^7+37$. Irreducible by Eisenstein's criterion. Then $g(x+1)=(x+1)^7+37=f(x)$ is irreducible as well // q.e.d.

Ex Consider $f(x)=x^4+x^3+x^2+x+1$. Show that $f(x)$ is irreducible in $\mathbb{Q}$.

soln. $f(x+1)=(x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1=x^4+4x^3+6x^2+4x+1+x^3+3x^2+3x+1+x^2+2x+1+\cancel{x}\,x+1+1=x^4+5x^3+10x^2+10x+5$

This satisfies Eisenstein's criterion, so $f(x)$ is irreducible // q.e.d.

We can generalise Eisenstein's criterion to cyclotomic polynomials:

Let p be a prime. Define the p^{th} cyclotomic polynomial as $C_p(x)=x^{p-1}+x^{p-2}+\dots+x+1=\sum_{r=0}^{p-1}x^r$.

Proposition $C_p(x)$ is irreducible over $\mathbb{Q}$.

Proof – Observe that $x^p-1=(x-1)C_p(x)$. Then $C_p(x)=\frac{x^p-1}{x-1}$. Replace x by $x+1$, then $C_p(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=\left[x^p+\sum_{r=1}^{p-1}\binom{p}{r}x^r+1-1\right]\cdot\frac{1}{x}$.

Then $C_p(x+1)=x^{p-1}+\sum_{r=2}^{p-1}\binom{p}{r}x^{r-1}+p$. We know $\binom{p}{r}\equiv 0 \pmod p$ for $2\le r\le p-1$. Hence, $C_p(x+1)$ satisfies Eisenstein's criterion $\Rightarrow C_p(x)$ irreducible // q.e.d.

We now prove Eisenstein's criterion – in two steps: first bit produced by him, second part filled in by Gauss.

Definition Let $f(x)\in\mathbb{Z}[x]$, $\deg(f)\ge 2$. By a proper factorisation of f, we mean $f(x)=g(x)\cdot h(x)$ where both $\deg(g),\deg(h)<\deg(f)$. $g(x),h(x)\in\mathbb{Z}[x]$.

(Observe that this implies $\deg(g),\deg(h)>0$).

Theorem (Eisenstein's lemma?)

Let p be a prime and $a(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0\in\mathbb{Z}[x]$ where (i) $a_n\not\equiv 0 \pmod p$, (ii) $a_r\equiv 0\pmod p$ $0\le r\le n-1$, (iii) $a_0\not\equiv 0\pmod{p^2}$.

Then $a(x)$ has no proper factorisation in $\mathbb{Z}[x]$.

Proof – Suppose $a(x)=b(x)c(x)$ is a proper factorisation of $a(x)$ where $b(x)=b_kx^k+\dots+b_1x+b_0$, $b_i\in\mathbb{Z}$, $b_k\ne 0$ and $c(x)=c_mx^m+\dots+c_1x+c_0$, $c_j\in\mathbb{Z}$, $c_m\ne 0$.

Compare constant terms: $a_0=b_0c_0$. So $a_0\equiv 0\pmod p$, $a_0\not\equiv 0\pmod{p^2}\Rightarrow$ either $b_0\equiv 0\pmod p$, $c_0\not\equiv 0\pmod p$ (or vice versa). WLOG, assume $b_0\not\equiv 0\pmod p$, $c_0\equiv 0\pmod p$. Compare coefficients of x: $a_1=b_1c_0+b_0c_1$. We know $p\mid a_1$, $p\mid c_0$, so $p\mid b_0c_1\Rightarrow c_1\equiv 0\pmod p$

By induction on j, we claim that all $\{c_j\}_{j=0,1,\dots,m}\equiv 0\pmod p$. Let $P(r)$ be the statment that $\forall r, 0\le r\le m$, $c_r\equiv 0\pmod p$.

Suppose $P(0),P(1),\dots P(r-1)$ are true, $r\le m$, $r-1<m$. NTP: $P(r)$ is true. $a_r=\sum_{t=0}^{r}b_{r-t}c_t$. Since $P(0),\dots P(r-1)$ are true, $c_0\equiv c_1\equiv\dots\equiv c_{r-1}\equiv 0 \pmod p\Rightarrow b_0c_r\equiv 0\pmod p$. $b_0\not\equiv 0\pmod p\Rightarrow c_r\equiv 0\pmod p\Rightarrow P(r)$ is true. Then coefficient of x^n is $a_n=b_kc_m$, and $c_m\equiv 0\pmod p$ $\Rightarrow a_n\equiv 0\pmod p\Rightarrow$ contradiction. Hence, $a(x)$ has no proper factorisation in $\mathbb{Z}[x]$ // q.e.d.

12 March 2013.
Prof FEA Johnson.
Roberts G06.

We would like to convert this result into one over the rationals: i.e. there is no factorisation $a(x)=b(x)c(x)$ where $b(x),c(x)\in\mathbb{Q}[x]$.

This gap was filled by Gauss.

Definition Let $a(x)=a_nx^n+\dots+a_1x+a_0\in\mathbb{Z}[x]$. The content of $a(x)$ is $C(a)=\mathrm{hcf}(a_0,a_1,\dots,a_n)$

Lemma (Gauss's lemma).

Let $b(x),c(x)\in\mathbb{Z}[x]$. Then $C(bc)=C(b)C(c)$.

Proof – We prove the special case where $C(b)=C(c)=1$. In practical terms, this means that if p is a prime, then $\exists k,m$ s.t. $p\nmid b_k$ and $p\nmid c_m$.

NTP: if $a(x)=b(x)c(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$, then $\exists l$ s.t. $p\nmid a_l$. Let p be prime. Define $k=\min\{r: p\nmid b_r\}$. i.e. $s<k\Rightarrow p\mid b_s$.

Define $m=\min\{r: p\nmid c_r\}$ i.e. $t<m\Rightarrow p\mid c_t$. We claim that $p\nmid a_{k+m}$. $a(x)=b(x)c(x)$ s.t. $a_{k+m}=b_kc_m+\sum_{s<k}b_sc_{m+k-s}+\sum_{t<m}b_{m+k-t}c_t$.

By definition of k,m: $\sum_{s<k}b_sc_{m+k-s}\equiv 0\pmod p$ $\because p\mid b_s$. Likewise $\sum_{t<m}b_{m+k-t}c_t\equiv 0\pmod p$ $\because p\mid c_t$. $\therefore a_{k+m}\equiv b_kc_m\pmod p$.

However, $p\nmid b_k$ and $p\nmid c_m$, so $p\nmid a_{k+m}$. This is true for all primes p. i.e. $\forall p$ prime, $\exists l$ s.t. $p\nmid a_l\Rightarrow C(a)=1$ // q.e.d.

For the general case, if $b(x)=b_mx^m+\dots+b_1x+b_0\in\mathbb{Z}[x]$, $C(b)=\mathrm{hcf}(b_m,\dots,b_0)$. Then define $b'(x)$ s.t. $b'_r=\frac{b_r}{C(b)}\in\mathbb{Z}$. Then $C(b')=1$.

Likewise, define $c'_r=\frac{c_r}{C(c)}\Rightarrow c(x)=C(c)c'(x)$ s.t. $C(c')=1$. $b(x)c(x)=C(b)C(c)b'(x)c'(x)\Rightarrow$ since $C(b'c')=1$ from above, $C(bc)=C(b)C(c)$ // q.e.d.

7202-19.

Corollary If $a(x) \in \mathbb{Z}[x]$ has a proper factorisation $a(x) = B(x)D(x)$ where $B(x), D(x) \in \mathbb{Q}[x]$, then it also has a proper factorisation $a(x) = b(x)d(x) \in \mathbb{Z}[x]$.

Proof – Suppose $a(x) = B(x)D(x)$ where $B(x) = \sum_{r=0}^{k} B_r x^r$, $D(x) = \sum_{r=0}^{m} D_r x^r$, $B_k \neq 0$, $D_m \neq 0$. Let $a(x) = a_n x^n + \dots + a_1 x + a_0$, $a_i \in \mathbb{Z}$, $a_0 \neq 0$.

then $B_i, D_j \in \mathbb{Q}$ and $k<n$, $m<n$. Suppose also the special case that $C(a) = 1$ (special case). We then clear fractions in B, D.

Write $B(x) = \frac{1}{K}\beta(x)$, $D(x) = \frac{1}{L}\delta(x)$ s.t. $K, L \in \mathbb{Z}$; $\beta(x), \delta(x) \in \mathbb{Z}[x]$. So now, $a(x) = \frac{1}{K}\beta(x)\frac{1}{L}\delta(x)$. Then $KL \cdot a(x) = \beta(x)\delta(x)$.

Here $\deg(\beta) = \deg B = k$, $\deg(\delta) = \deg(D) = m$. We write $\beta(x) = C(\beta)\, b(x)$ where $b(x) \in \mathbb{Z}[x]$, $C(b) = 1$. $\delta(x) = C(\delta)\, d(x)$ where $d(x) \in \mathbb{Z}[x]$, $C(d) = 1$.

so $KL\, a(x) = C(\beta)C(\delta)\, b(x)d(x)$. But $C(a) = 1$ so content of LHS $= KL$. $C(b) = C(d) = 1 \Rightarrow$ RHS $= C(\beta)C(\delta)$ so $a(x) = b(x)d(x)$.

$\deg(b) = k < n$, $\deg(d) = m < n$. $b(x)d(x) \in \mathbb{Z}[x]$. In general if $C(a) \neq 1$, write $a(x) = C(a)\,\alpha(x)$, $C(\alpha) = 1$. If $a(x) = B(x)D(x)$, $\alpha(x) = \frac{1}{C(a)}B(x)D(x)$.

so $\alpha(x) = \beta(x)d(x)$ for some $\beta, d \in \mathbb{Z}[x]$. so $a(x) = b(x)d(x) \Rightarrow b(x) = C(a)\beta(x)$.

In the contrapositive, we obtain:

Theorem Let $a(x) \in \mathbb{Z}[x]$. If $a(x)$ has no proper factorisation over $\mathbb{Z}$, then $a(x)$ is irreducible over $\mathbb{Q}$.

Proof – By contrapositive.

so now, we get the full Eisenstein-Gauss criterion (proven)

Cyclotomic polynomials.

We know that $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$. If p is prime, this is the complete factorisation of $x^p - 1$ into $\mathbb{Q}$-irreducibles. Then, we now consider $x^n - 1$ where n is not necessarily prime.

First approximation: We can factorise $x^n - 1$ completely over $\mathbb{C}$: Put $\zeta = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. $\zeta^n = \cos(2\pi) + i\sin(2\pi) = 1$ by de Moivre's theorem.

Then $\zeta^r = \cos\left(\frac{2\pi r}{n}\right) + i\sin\left(\frac{2\pi r}{n}\right)$, and $x^n - 1 = \prod_{r=0}^{n-1}(x - \zeta^r)$ is the complete factorisation over $\mathbb{C}$ – each ζ^r satisfies $(\zeta^r)^n - 1 = 0$.

The set of n^{th} roots of 1, $\{1, \zeta, \zeta^2, \dots \zeta^{n-1}\}$ forms a subgroup of $\mathbb{C}^*$ (multiplicative group of $\mathbb{C}$). Then $\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\} \cong C_n$.

The orders of the elements $\{1, \zeta, \dots, \zeta^{n-1}\}$ are precisely the divisors of n. So suppose $d | n$. Define $C_d(x) = \prod_{\mathrm{ord}(\zeta^r) = d}(x - \zeta^r)$. Then $x^n - 1 = \prod_{d|n} C_d(x)$.

It is not immediately clear that $C_d(x)$ is an integral polynomial. In fact, each $C_d(x) \in \mathbb{Z}[x]$, and is irreducible over $\mathbb{Q}$.

How to compute $C_d(x)$: Consider $x^n - 1 = \prod_{d|n} C_d(x)$.

$n=1$: $C_1(x) = x - 1$

$n=2$: $x^2 - 1 = C_1(x)C_2(x) = (x-1)C_2(x)$, so $C_2(x) = x + 1$

$n=3$: $x^3 - 1 = C_1(x)C_3(x) = (x-1)C_3(x) \Rightarrow C_3(x) = x^2 + x + 1$, irreducible over $\mathbb{Q}$.

$n=4$: $x^4 - 1 = C_1(x)C_2(x)C_4(x)$. $C_1(x)C_2(x) = (x-1)(x+1) = x^2 - 1$, so $C_4(x) = x^2 + 1$

$n=5$: $x^5 - 1 = C_1(x)C_5(x) = (x-1)C_5(x) \Rightarrow C_5(x) = x^4 + x^3 + x^2 + x + 1$

$n=6$: $x^6 - 1 = C_1(x)C_2(x)C_3(x)C_6(x) = (x^3 - 1)C_2(x)C_6(x) \Rightarrow C_2(x)C_6(x) = x^3 + 1$. $C_2(x) = x + 1 \Rightarrow C_6(x) = (x^3+1)/(x+1) = x^2 - x + 1$

To show that $C_6(x)$ is irreducible, note that if $g(x) = x^2 - x + 1$, $g(x-1) = (x-1)^2 - (x-1) + 1 = x^2 - 2x + 1 - x + 1 + 1 = x^2 - 3x + 3$. Set $p = 3$, irreducible by Eisenstein's criterion.

Ex Factorise $x^{12} - 1$ completely over $\mathbb{Q}$.

Soln. $x^{12} - 1 = C_1(x)C_2(x)C_3(x)C_4(x)C_6(x)C_{12}(x)$. We know that $x^6 - 1 = C_1(x)C_2(x)C_3(x)C_6(x)$, so $x^{12} - 1 = (x^6 - 1)(x^6 + 1) \Rightarrow C_4(x)C_{12}(x) = x^6 + 1$.

$C_{12}(x) = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1$. Hence, $x^{12} - 1 = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)$.

How do we factorise $x^n + 1$?

Ex Factorise $x^{10} + 1$ completely into irreducibles over $\mathbb{Q}$.

Soln. We use a trick: $x^{10} + 1 \mid x^{20} - 1 \Rightarrow x^{20} - 1 = (x^{10} - 1)(x^{10} + 1)$. If we can factorise $x^{10} - 1$ and $x^{20} - 1$, we can factorise $x^{10} + 1$. $x^{10} - 1 = C_1(x)C_2(x)C_5(x)C_{10}(x)$.

$x^{10} - 1 = (x^5 - 1)C_2(x)C_{10}(x) \Rightarrow C_2(x)C_{10}(x) = x^5 + 1 \Rightarrow C_{10}(x) = \frac{x^5+1}{x+1} = x^4 - x^3 + x^2 - x + 1$. $x^{20} - 1 = C_1(x)C_2(x)C_4(x)C_5(x)C_{10}(x)C_{20}(x) \Rightarrow x^{20} - 1 = (x^{10} - 1)C_4(x)C_{20}(x)$.

Then $C_4(x)C_{20}(x) = x^{10} + 1 \Rightarrow C_{20}(x) = \frac{x^{10}+1}{x^2+1} = x^8 - x^6 + x^4 - x^2 + 1$. Thus, $x^{10} + 1 = \frac{x^{20} - 1}{x^{10} - 1} = \frac{C_1(x)C_2(x)C_4(x)C_5(x)C_{10}(x)C_{20}(x)}{C_1(x)C_2(x)\quad C_5(x)C_{10}(x)} = C_4(x)C_{20}(x) = (x^{10}+1) = (x^2+1)(x^8 - x^6 + x^4 - x^2 + 1)$

15 March 2013.
Prof FEA JOHNSON
Roberts 106.

Today, we will retreat into Graph theory to deliberate upon something: $\mathrm{Aut}(C_p) \cong C_{p-1}$.

Proposition If m, n are coprime, then $C_m \times C_n \cong C_{mn}$.

Proof – We'll prove in additive form first: If m, n are coprime, $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$. If $x \in \mathbb{Z}$, let $[x]_k$ denote the congruence class of $x \pmod k$. This gives us a well-defined homomorphism: $\natural: \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$. $\natural([x]_{mn}) = ([x]_m, [x]_n)$. $\natural$ is injective, as if we let $[x]_{mn} \in \mathrm{Ker}(\natural)$, i.e.

$\natural([x]_{mn}) = ([x]_m, [x]_n) = (0, 0) \Rightarrow x \equiv 0 \pmod m$, $x \equiv 0 \pmod n$. $\Rightarrow x = km = \ell n \Rightarrow x$ is a common multiple of $m, n \Rightarrow x = \lambda\, \mathrm{lcm}(m,n) = \lambda \frac{mn}{\gcd(m,n)}$

$\gcd(m,n) = 1 \Rightarrow \mathrm{lcm}(m,n) = \lambda mn \Rightarrow x \equiv 0 \pmod{mn} \Rightarrow [x]_{mn} = 0$. $\natural([x]_{mn}) = (0,0) \Rightarrow [x]_{mn} = 0$, $\mathrm{Ker}(\natural)$ is trivial $\Rightarrow \natural$ is injective.

$|\mathbb{Z}/mn| = |\mathbb{Z}/m \times \mathbb{Z}/n|$, so $\natural$ is injective $\Rightarrow \natural$ is bijective. This proves the additive notation. Clearly $C_k \cong \mathbb{Z}/k$, so $\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn$

$\Rightarrow C_m \times C_n \cong C_{mn}$ q.e.d.

Theorem Let $\mathbb{F}$ be a field. Let $G \subset \mathbb{F}^*$ be a finite subgroup of the multiplicative group $\mathbb{F}^*$. Then G is cyclic.

Proof – Begin with special case, $|G| = p^n$, p prime. If $x \in G$, $\mathrm{ord}(x) \mid p^n \Rightarrow \mathrm{ord}(x) = p^m$, $m \leq n$. Define $e = \max\{m : \exists x \in G \ \mathrm{ord}(x) = p^m\}$.

so $\exists x \in G$, $\mathrm{ord}(x) = p^e$. Also, if $g \in G$, $g^{p^e} = 1$ ($\mathrm{ord}(g) = p^m$, $m \leq e$). Evidently, $e \leq n$. Then consider equation $y^{p^e} - 1 = 0$.

As $\mathbb{F}$ is a field, $\deg(y^{p^e}) = p^e \Rightarrow$ equation has at most p^e solutions. But $\forall g \in G$, $g^{p^e} - 1 = 0$ is a solution $\Rightarrow$ equation has at least p^n solutions.

$\Rightarrow e = n$ and $\exists x \in G$, $\mathrm{ord}(x) = p^n \Rightarrow$ since $|G| = p^n$, $G \cong C_{p^n}$, x is a generator.

For the general case, apply Sylow's theorem: Write $|G| = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, with $p_1, p_2, \dots, p_m$ distinct primes. By Sylow's theorem

$\exists$ subgroup $G(i)$ of G, $|G(i)| = p_i^{e_i}$. By above, $G(i) = C_{p_i^{e_i}}$ is cyclic. For each $1 \leq r \leq m$, define $H(r) = G(1) \cdot G(2) \cdots G(r)$.

i.e. $H(r) = \{x_1 x_2 \cdots x_r : x_i \in G(i)\}$. G is abelian, so each $H(r)$ is a subgroup. $H(2) = G(1) \cdot G(2)$. $G_1 \cap G_2 = \{1\}$, so by recognition criterion,

$H(2) \cong G(1) \rtimes_h G(2) \cong G(1) \times G(2)$ (abelian). $|H(2)| = p_1^{e_1} p_2^{e_2}$. Suppose proved $|H(r)| = p_1^{e_1} \cdots p_r^{e_r}$. $H(r+1) = H(r)\, G(r+1)$.

$H(r) \cap G(r+1) = \{1\}$ (coprime orders) $\Rightarrow H(r+1) \cong H(r) \times G(r+1) \cong G(1) \times G(2) \times \cdots \times G(r) \times G(r+1)$, $|H(r+1)| = p_1^{e_1} \cdots p_{r+1}^{e_{r+1}}$.

so $H(m) \cong G(1) \times \cdots \times G(m)$, $|H(m)| = p_1^{e_1} \cdots p_m^{e_m} = |G|$. But each $G(i)$ is cyclic (special case), so $G \cong C_{p_1^{e_1}} \times \cdots \times C_{p_m^{e_m}}$.

Clearly thus, $p_i^{e_i}$ is coprime with $p_j^{e_j}$, $i \neq j \Rightarrow G$ is cyclic // q.e.d.

Corollary Let p be a prime. Then $\mathbb{F}_p^* \cong C_{p-1}$. (recall: $\mathbb{F}_p^* = \{x \in \mathbb{F}_p : x \neq 0\}$).

Proof – $\mathbb{F}_p^\times$ is a finite group of $\mathbb{F}_p^*$, so it is cyclic. $|\mathbb{F}_p^*| = p-1$ // q.e.d.

Corollary If p is prime, then $\mathrm{Aut}(C_p) \cong C_{p-1}$.

Proof – We know that $\mathrm{Aut}(C_p) \cong \{\varphi_a : 1 \leq a \leq p-1\}$ where $\varphi_a(x) = x^a$. So the map $\mathbb{F}_p^\times \to \mathrm{Aut}(C_p)$; $a \mapsto \varphi_a$ is an isomorphism.

However, $\mathbb{F}_p^* \cong C_{p-1}$ so $\mathrm{Aut}(C_p) \cong C_{p-1}$ // q.e.d.

19 March 2013.
Prof FEA JOHNSON.
Roberts G06.

Product of Rings

Definition Let R, S be rings. The product ring $R \times S$ is defined (i) as a set by $R \times S = \{(r,s) : r \in R, s \in S\}$.

- addition: $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$,
- multiplication $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$
- zero $(0,0)$
- multiplicative identity $(1,1)$.

If R is a ring, we define $R^* = \{r \in R : \exists r^{-1} \in R,\ r r^{-1} = r^{-1} r = 1\}$, the unit group of invertible elements.

Proposition If R, S are rings, then $(R \times S)^* = R^* \times S^*$.

Proof – $(r_1, s_1)(r_2, s_2) = (1,1) \iff r_1 r_2 = 1$ and $s_1 s_2 = 1$. $(r,s) \in (R \times S)^* \iff r \in R^*$ and $s \in S^*$ // q.e.d.

Ex If m, n are coprime then $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$.

Proof – Recall the isomorphism of abelian groups $\natural : \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$. $\natural([x]_{mn}) = ([x]_m, [x]_n)$. $\natural$ is an additive isomorphism.

But also $\natural([xy]_{mn}) = ([xy]_m, [xy]_n) = ([x][y], [x][y]) = ([x]_m [x]_n)([y]_m [y]_n) = \natural[x]\,\natural[y]$. So $\natural$ is multiplicative and also $\natural[1] = ([1],[1])$.

Identity maps to identity, so $\natural$ is a ring isomorphism //

Let $n \in \mathbb{Z}$, $n \geq 2$. Write $n = p_1^{e_1} \cdots p_m^{e_m}$ where $p_1, \dots, p_m$ are distinct primes, $e_1, \dots, e_m \geq 1$. If $m \geq 2$, write $n' = (p_1^{e_1}, \dots, p_{m-1}^{e_{m-1}})$ so

$n = n' p_m^{e_m}$ and n', $p_m^{e_m}$ are coprime. So by above, $\mathbb{Z}/n \cong \mathbb{Z}/n' \times \mathbb{Z}/p_m^{e_m}$. Inductively, $\mathbb{Z}/n \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_m^{e_m}$, $n = p_1^{e_1} \cdots p_m^{e_m}$. So,

Corollary $(\mathbb{Z}/n)^* \cong (\mathbb{Z}/p_1^{e_1})^* \times \cdots \times (\mathbb{Z}/p_m^{e_m})^*$.

So to compute units on $\mathbb{Z}/n$, it is enough to compute units in $\mathbb{Z}/p^e$ (p prime). We know $(\mathbb{Z}/p)^* \cong C_{p-1}$, p prime. We want to know what happens for $(\mathbb{Z}/p^e)^*$, $e \geq 2$.

Nilpotent Trick

Let $a \in R$ (R ring). We say that a is nilpotent when $a^N = 0$ for some $N \geq 1$.

Proposition If $a \in R$ is nilpotent, then $1 + a \in R^*$.

Proof – $1 - a^N = (1-a)(1 + a + a^2 + \cdots + a^{N-1})$. If $a^N = 0$, then $1 - a^N = 1$. Hence $1 - a \in R^*$ with inverse $1 + a + \cdots + a^{N-1}$. Equally $(1+a)(1 - a + a^2 + \cdots (-1)^{N+1} a^{N+1}) = 1 + a^N = 1$.

Hence, $1 + a \in R^*$ with inverse $1 - a + a^2 + \cdots + (-1)^{N+1} a^{N+1}$ // q.e.d.

Corollary $1 + p^k$ is a unit in $\mathbb{Z}/p^e$.

Proof – $(p^k)^e \equiv (p^e)^k \equiv 0$ in $\mathbb{Z}/p^e$, so p^k is nilpotent // q.e.d.

Corollary Suppose $1 \leq r \leq p-1$. Then $r + ap^k$ is a unit in $\mathbb{Z}/p^e$.

Proof – To begin, calculate mod p (not mod p^e). Then $\exists s : 1 \leq s \leq p-1$ s.t. $rs \equiv 1 \pmod p$. Then we consider this mod p^e: $rs = 1 + bp^d$ for some

d. Multiplying $u = r + ap^k$ by s, $us = rs + sap^k = 1 + bp^d + sap^k = 1 + \lambda p^\mu$ for some power μ. $\therefore$ us is a unit with inverse v (i.e.

$us \in (\mathbb{Z}/p^e)^*$ with inverse v) $\Rightarrow usv = 1 \Rightarrow u \in (\mathbb{Z}/p^e)^*$ with inverse sv // q.e.d.

7202-20.

Corollary $(\mathbb{Z}/p^e)^* = \{r + ap^k : 1 \le r \le p-1,\ 1 \le k \le e-1\}$.

Proof – By above, all such elements are units. The remaining elements are not units $\because$ $0 + ap^k$ are nilpotent : $(ap^k)^e = 0$. $\Rightarrow$ ap^k cannot have an inverse u, since if it

~~Proposition~~ did, $u(ap^k) = 1 \Rightarrow (uap^k)^e = 1$ but $u^e(ap^k)^e = 0 \Rightarrow 1 = 0$, contradiction, q.e.d.

Proposition Let p be a prime, then $|(\mathbb{Z}/p^e)^*| = (p-1)p^{e-1}$.

e.g. $p=5$, $e=2$. $|(\mathbb{Z}/5^2)^*| = |\{1,2,3,4,\ 6,7,8,9,\ 11,12,13,14,\ 16,17,18,19,\ 21,22,23,24\}| = 20 = (5-1)5^{2-1}$.

Proof – We get p^{e-1} blocks of $(p-1)$ units. The blocks are of form $r + ap^k$, $1 \le r \le p-1$, $1 \le k \le e$, q.e.d.

How many residues are invertible mod n? This proposition above gives us a value, which we call the ~~Euler's totient function~~, $\Phi(n) = |(\mathbb{Z}/n)^*|$.

Proposition If $n = p_1^{e_1} \cdots p_m^{e_m}$, $p_1, \dots, p_m$ are distinct primes, $\Phi(p_1^{e_1}) \cdots \Phi(p_m^{e_m})$

Proof – $(\mathbb{Z}/n)^* \cong (\mathbb{Z}/p_1^{e_1})^* \times \cdots \times (\mathbb{Z}/p_m^{e_m})^*$, q.e.d

We have seen that $\Phi(p_i^{e_i}) = (p_i - 1)p_i^{e_i - 1}$. $\Phi(p_i^{e_i}) = (1 - \frac{1}{p_i})p_i^{e_i}$. So now, if $n = p_1^{e_1} \cdots p_m^{e_m}$, with $p_1, \dots, p_m$ distinct primes, then $\Phi(n) = \prod_{i=1}^{m} (1 - \frac{1}{p_i}) p_i^{e_i}$

i.e. $\boxed{\Phi(n) = \left(\prod_{r=1}^{m} (1 - \frac{1}{p_r})\right) n}$. This is Euler's formula.

(NFE).
The group structures are $(\mathbb{Z}/p^e)^* \cong C_{p-1} \times C_{p^{e-1}}$ for p odd. For $p=2$, $(\mathbb{Z}/2)^* = \{1\}$, $(\mathbb{Z}/4)^* \cong C_2$, $(\mathbb{Z}/8)^* \cong C_2 \times C_2$.

However, $(\mathbb{Z}/16)^* \cong C_2 \times C_4$ is ~~a~~typical. $\mathbb{Z}/2^m \cong C_2 \times C_{2^{m-2}}$ for $m \ge 4$.

END OF SYLLABUS.

Practice Questions:

22 March 2013
Prof FEA JOHNSON
Roberts 106.

Q: Classify all groups of order 20.

$20 = 2^2 \times 5$, $|G| = 20$. By Sylow, $\exists$ $K \leq G$ with $|K| = 5$, and $\exists$ $Q \leq G$ with $|Q| = 4$.

Claim: $K \triangleleft G$. $N_5 \equiv 1 \pmod 5$ so $N_5 = 1$ or $N_5 \geq 6$.

Suppose $K_1, \dots, K_6$ are all subgroups with $|K_i| = 5$. Each $K_i \cong C_5$, so if $x \in K_i$ is non-trivial, x generates K_i.

If $i \neq j$, $x \in K_i \cap K_j$ then $x = 1$, otherwise x generates both K_i and K_j $\Rightarrow$ $K_i = K_j$.

So $K_i \cap K_j = \{1\}$. Then $|K_1 \cup \dots \cup K_6| = 6 \times (5-1) + 1 = 25 > 20$ $\Rightarrow$ contradiction. Hence $N_5 \equiv 1 \Rightarrow K \triangleleft G$.

$\because$ if $g \in G$, gKg^{-1} is also a subgroup of order $5 \equiv K$ (by uniqueness) $\Rightarrow$ $gK = Kg$ and $K \triangleleft G$.

G has a normal subgroup of order 5, $K \triangleleft G$, $K \cong C_5$. It also has $Q \leq G$, $|Q| = 4$.
Clearly $K \cap Q = \{1\}$ as orders are coprime. Also, $|G| = 20 = 5 \cdot 4 = |K|\,|Q|$.
} We can apply recognition criterion.

By recognition criterion for semi-direct products, $G \cong K \rtimes_h Q$ for some h i.e. $G \cong C_5 \rtimes_h Q$, $h: Q \to \mathrm{Aut}(C_5)$.

We know that there are only 2 groups of order 4: (a) C_4 or (b) $C_2 \times C_2$.

Case (a) $G \cong C_5 \rtimes_h C_4$

for some $h: C_4 \to \mathrm{Aut}(C_5) \cong C_4$

Let $K = C_5 = \{1, x, x^2, x^3, x^4\}$ $x^5 = 1$.

$Q = C_4 = \{1, y, y^2, y^3\}$ $y^4 = 1$

$\mathrm{Aut}(C_5) = \{\underset{\mathrm{Id}}{\underset{\shortparallel}{\varphi_1}}, \varphi_2, \varphi_3, \varphi_4\}$.

There are 4 possible homomorphisms:
$h_0(y) = \mathrm{Id}$, $h_1(y) = \varphi_2$, $h_2(y) = \varphi_3$, $h_3(y) = \varphi_4$.

$h_0 = \mathrm{Id}$: $\langle X, Y \mid X^5 = 1, Y^4 = 1, YXY^{-1} = X \rangle$
This is simply $C_5 \times C_4$.

$h_1 = \varphi_2$ $\langle X, Y \mid X^5 = 1, Y^4 = 1, YXY^{-1} = X^2 \rangle$
$h_2 = \varphi_3$ $\langle X, Y \mid X^5 = 1, Y^4 = 1, YXY^{-1} = X^3 \rangle$
$h_3 = \varphi_4$ $\langle X, Y \mid X^5 = 1, Y^4 = 1, YXY^{-1} = \underset{X^{-1}}{\underset{\uparrow}{X^4}} \rangle$.

This is $Q(20)$, or D_{10}^*.

The groups for h_1, h_2 are isomorphic: in h_1, put $Z = Y^3$.
Z still generates C_4:
$ZXZ^{-1} = Y^3XY^{-3} = Y^2(YXY^{-1})Y^{-2} = Y^2X^2Y^{-2}$
$= Y(YXY^{-1})^2Y^{-1} = YX^4Y^{-1} = (YXY^{-1})^4 = X^8 = X^3$.

So changing generator, $\underset{h_1}{YXY^{-1} = X^2} \longleftrightarrow \underset{h_2}{ZXZ^{-1} = X^3}$.

$h_3 \neq h_1$ or h_2., as h_1, h_2 have trivial centres, h_3 has centre $\{1, Y^2\}$.

h_1, h_2 produces a group called the affine group of $\mathbb{F}_5$, $\underset{\mathbb{F}_5 \rtimes (\mathbb{F}_5)^*}{\underset{\shortparallel}{\mathrm{Aff}(\mathbb{F}_5)}}$.

Case (b) $G \cong C_5 \rtimes_\psi (C_2 \times C_2)$.

for some $\psi: (C_2 \times C_2) \longrightarrow \mathrm{Aut}(C_5) \cong C_4$.

$C_5 = \{1, x, x^2, x^3, x^4\}$

$C_2 \times C_2 = \{1, s, t, st\}$. $s^2 = t^2 = 1$, $st = ts$.

$\mathrm{Aut}(C_5) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$.
ord: 1 4 4 2

φ_i is a homomorphism $\Leftrightarrow$ $\mathrm{ord}(\varphi_i) \mid \mathrm{ord}(g)$.
$\Rightarrow$ cannot attain φ_2, φ_3.

We get 4 homomorphisms:

ψ_0: $1 \mapsto \mathrm{Id}$, $s \mapsto \mathrm{Id}$, $t \mapsto \mathrm{Id}$, $st \mapsto \mathrm{Id}$.
ψ_1: $1 \mapsto \mathrm{Id}$, $s \mapsto \varphi_4$, $t \mapsto \mathrm{Id}$, $st \mapsto \varphi_4$
ψ_2: $1 \mapsto \mathrm{Id}$, $s \mapsto \mathrm{Id}$, $t \mapsto \varphi_4$, $st \mapsto \varphi_4$
ψ_3: $1 \mapsto \mathrm{Id}$, $s \mapsto \varphi_4$, $t \mapsto \varphi_4$, $st \mapsto \mathrm{Id}$

ψ_0: $\langle X, S, T \mid X^5 = S^2 = T^2 = 1, TS = ST, \underbrace{SXS^{-1} = X}_{SX = XS}, \underbrace{TXT^{-1} = X}_{TX = XT} \rangle$

This is abelian: $G \cong C_5 \times C_2 \times C_2$

ψ_1: $\langle X, S, T \mid X^5 = S^2 = T^2 = 1, TS = ST, SXS^{-1} = X^{-1}, \underbrace{TXT^{-1} = X}_{TX = XT} \rangle$

X and S generate D_{10}, which commutes with T.
$G \cong D_{10} \times C_2$.

ψ_2: $\langle X, S, T \mid X^5 = S^2 = T^2 = 1, TS = ST, SXS^{-1} = X, TXT^{-1} = X^{-1} \rangle$
This is isomorphic to ψ_1, where
$D_{10} \cong \langle X, T \rangle$, $C_2 \cong \langle S \rangle$.

ψ_3: Likewise for ψ_1, ψ_2, with $D_{10} \cong \langle X, S \rangle$, $C_2 \cong \langle ST \rangle$

Properties of $\mathrm{Aff}(\mathbb{F}_5)$.
Let $\mathbb{F}_5$ be the field of order 5: $\mathrm{Aff}(\mathbb{F}_5) = \mathbb{F}_5 \rtimes (\mathbb{F}_5)^*$.

$\therefore$ There are precisely 5 groups of order 20:
$C_5 \times C_4 \cong C_{20}$, $Q(20)$, $\mathrm{Aff}(\mathbb{F}_5)$, $C_5 \times C_2 \times C_2$, $D_{10} \times C_2$.

Q: Classify all groups of order 99.

$|G| = 3^2 \times 11$. Go for largest prime. $\exists K \triangleleft G$ s.t. $|K|=11$. $K \cong C_{11}$ is unique and normal; so $G \cong C_{11} \rtimes_h Q$ where $|Q| = 9 = 3^2$.

$\exists$ two groups of order 9: (I) C_9, (II) $C_3 \times C_3$.

(I)
But $\mathrm{Aut}(C_{11}) \cong C_{10}$. 10 is coprime to 9, $G \cong C_{11} \times C_9 \cong C_{99}$
h is trivial.

(II).
$\mathrm{Aut}(C_{11}) \cong C_{10}$. 10 is coprime to 3^2.
h is trivial, $G \cong C_{11} \times C_3 \times C_3 \cong C_{33} \times C_3$.

Theorem: there are precisely two groups of order 99, with are both abelian.

Or, more generally......

If $|G| = p^2 q$ s.t.

(i) $p^2 < q$

(ii) p, q are both odd primes, and

(iii) $\gcd(p-1, q) = 1$,

Then $\exists$ precisely two groups of order $p^2 q$, namely:

$$C_{p^2} \times C_q \quad \text{and} \quad C_p \times C_{pq},$$

which are both abelian.