

Basic Theory from G2M31 2nd year course

Subgroups

Definition: Let G be a group. Then $H \subseteq G$ is a subgroup of G if H is itself a **group** with the same *operation* as G . **Alternative Definitions.** (a) (i) $H \subseteq G$, (ii) If $a, b \in H \Rightarrow ab \in H$, (iii) If $a \in H \Rightarrow a^{-1} \in H$. I.e. H is *closed* w.r.t. products and inverses. The **other** group properties will follow for H . In particular, if $a \in H$ then $a^{-1} \in H$ and $aa^{-1} = 1 \in H$ giving the *same identity* for H & G . (b) (i) $H \subseteq G$, (ii) If $a, b \in H \Rightarrow ab^{-1} \in H$ (**Notes:** $b \in H \Rightarrow bb^{-1} = 1 \in H$, $1, b \in H \Rightarrow 1 \cdot b^{-1} = b^{-1} \in H$, $a, b \in H \Rightarrow a \cdot b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$).

Examples: (1) In $\mathbf{Z}_5^* = \{1, 2, 3, 4\}$, $H = \{1, 4\}$ forms a *subgroup* since “ $4^2 = 1$ ”. (2) The identity $\{1\}$ **always** forms a subgroup. (3) In S_3 the set $\{I, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$ forms a *subgroup* (see Cayley table).

Cyclic Groups

A *cyclic group* is one in which **every** element can be written as a *power* of one element “ a ” called **a generator** i.e. $G = \{x: x = a^r, r \in \mathbf{Z}\}$ (including *negative* powers). **Notes:** (1) The generator is not in general *unique* e.g. $\mathbf{Z}_5^* = \{1, 2, 3, 4\}$ is *generated* by 2 (see earlier) or by 3. Note that in **both** cases $2^4 \equiv 3^4 \equiv 1$ where 4 is the *order* of the group. If we look at the elements generated by 4 we obtain the **subgroup** $\{1, 4\}$.

(2) For any group G the *powers* of any element “ a ” $H = \{x: x = a^r, r \in \mathbf{Z}\}$ form a **subgroup** (*cyclic*) of G since (i) $H \subseteq G$, (ii) If $x = a^r, y = a^s \in H$, then $xy^{-1} = a^r(a^s)^{-1} = a^r a^{-s} = a^{r-s} \in H$ e.g. in S_3 the powers of $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ generates the *subgroup* $\{I, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$. (3) Any *cyclic group* $G = \{x: x = a^r, r \in \mathbf{Z}\}$ is **Abelian** since $a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r$.

(4) If n is the *smallest positive integer* s.t. $a^n = 1$ (i.e. the **order** of a) then $G = C_n = \{1, a, a^2, \dots, a^{n-1}\}$ is of finite order n . (There are precisely n *distinct elements* here since if $a^r = a^s$, $0 \leq s < r < n$ then $a^{r-s} = 1$ with $0 < (r-s) < n$). If there is **no such** n then $G = C_\infty = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$ is an *infinite cyclic group* e.g. \mathbf{Z} with the binary operation of “*addition*” is generated by 1 with identity 0 and is **infinite** cyclic group.

(5) If $x \in C_n = \{1, a, \dots, a^{n-1}\}$ then $x^n = 1$ for all $x \in C_n$ since $x = a^r$ for some $r < n$, $x^n = (a^r)^n = (a^n)^r = 1^r = 1$. **Example:** Consider $C_6 = \{1, a, a^2, \dots, a^5\}$ ($a^6 = 1$), then $a^5 = b$ is *also* a generator for C_6 since $b^0 = 1$ (by definition), $b = a^5$, $b^2 = a^{10} = a^6 \cdot a^4 = a^4$, $b^3 = a^{15} = a^3$, $b^4 = a^{20} = a^2$, $b^5 = a^{25} = a$ (modular arithmetic on the *powers*). On the **other** hand $c = a^2$ just generates the *cyclic subgroup* of even powers of a ($c^0 = 1, c = a^2, c^2 = a^4, c^3 = a^6 = 1$ i.e. $\{1, a^2, a^4\}$).

Theorem: The cyclic group $C_n = \{1, a, a^2, \dots, a^{n-1}\}$ ($a^n=1$) is generated by a^r iff $\gcd(n,r) = 1$ (Relatively prime). Proof: (i) If $\gcd(n,r) = 1$ there exists p, q s.t. $pn+qr = 1$ then $(a^r)^q = a^{rq} = a^{1-pn} = a^1(a^n)^{-p} = a^1 \cdot 1 = a$. Now (a^r) generates a cyclic subgroup of C_n and since this subgroup **contains** a ($= (a^r)^q$) it includes all powers of a .

(ii) If C_n is generated by a^r then since $a \in C_n$ for some q , $(a^r)^q = 1$. Hence $rq \equiv 1 \pmod{n}$ i.e. $rq = 1 + \lambda n$ i.e. $rq + (-\lambda)n = 1$. Hence $\gcd(n,r) = 1$. **Corollary:** The number of *distinct possible generators* of C_n is $\phi(n)$ since $\phi(n)$ is the number of numbers **between** 1 and n which are relatively prime to n .

Theorem: If p is a prime then $Z_p^* = \{1, 2, \dots, (p-1)\}$ is a cyclic group of order $(p-1)$ [under multiplication modulo p]. **Examples:** $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ is a cyclic of order 6 by the above. We search for a generator. Note: a generator must be of order 6 since we need $a^6=1$. 3 is a generator: $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 4 \pmod{7}$, $3^5 \equiv 5 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$. The **other** generators are of the form 3^r where $\gcd(r,6) = 1$. The only possibility is $r=5$, $3^5 \equiv 5$ ($\phi(6) = \phi(2 \times 3) = 2$)

Homomorphisms between Groups

Definition: (1) A group *homomorphism* is a function $\phi: G_1 \rightarrow G_2$ (G_1, G_2 are groups) such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G_1$. (2) A *bijective* group homomorphism is called an isomorphism denoted by $G_1 \cong G_2$ (Isomorphic groups are in effect **identical** as groups).

Notes: If $\phi: G_1 \rightarrow G_2$ is a group homomorphism then (a) If e_1 & e_2 are the respective identities in G_1 and G_2 then $\phi(e_1) = e_2$. Proof: $\phi(e_1) \cdot \phi(e_1) = \phi(e_1 e_1) = \phi(e_1) = e_2 \cdot \phi(e_1)$. Multiply both sides by $(\phi(e_1))^{-1}$ to obtain the result. (b) $\phi(x^{-1}) = (\phi(x))^{-1}$ for all $x \in G_1$. Proof: $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(e_1) = e_2 = \phi(e_1) = \phi(x^{-1}x) = \phi(x^{-1})\phi(x)$.

The result follows by the *uniqueness* of $(\phi(x))^{-1}$. (c) $\phi(G_1) = \{g_2: g_2 = \phi(g_1) \text{ some } g_1 \in G_1\}$ is a **subgroup of G_2** . Proof: (i) $\phi(G_1) \subseteq G_2$. ✓. (ii) If $a, b \in \phi(G_1)$ then $a = \phi(x)$, $b = \phi(y)$ for some $x, y \in G_1$ and $ab^{-1} = \phi(x)(\phi(y))^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \phi(G_1)$. ✓.

Example: Let $G_1 = C_4 = \{1, a, a^2, a^3\}$ where $a^4=1$ and let $G_2 = C_2 = \{1, b\}$ where $b^2 = 1$. Define $\phi: G_1 \rightarrow G_2$ by $1 \rightarrow 1$ and $a^2 \rightarrow 1$, a and $a^3 \rightarrow b$. Then this gives a group **homomorphism**.

G_1	1	a^2	a	a^3		G_2	1	b
1	1	a^2	a	a^3		1	1	b
a^2	a^2	1	a^3	a		1	1	b
a	a	a^3	a^2	1		b	b	1
a^3	a^3	a	1	a^2		b	b	1

Cosets

Definition: Let G be a group and S a subgroup of G . Let $g \in G$ and put $gS = \{x \in G: x=gs, \text{ some } s \in S\}$. We call gS a *left coset* of S in G (we can also form right cosets). **Notes:** (1) gS is **not usually** a subgroup, (2) $g \in gS$ since $g=g \cdot 1$ where $1 \in S$.

Theorem: The *left cosets* of S in G form a partition of G . **Proof:** Define the relation \sim on G by $g \sim h \Leftrightarrow gS = hS, g, h \in G$. (i) Reflexive $g \sim g$ since $gS = gS$. (ii) Symmetric: If $g \sim h \Rightarrow gS = hS \Rightarrow hS = gS \Rightarrow h \sim g$. (iii) Transitive. If $g \sim h$ and $h \sim t$ then $gS = hS$ and $hS = tS, \Rightarrow gS = tS \Rightarrow g \sim t$. Hence \sim is an equivalence relation as required.

Note: If X is a *left coset* of S in G and $g \in X$ then since $g \in gS$ and the cosets *partition* G , $X = gS$. **Example:** Let $G = U(\mathbb{Z}_{12}^*) = \{1, 5, 7, 11\}$ and $S = \{1, 5\}$ ($5^2=1$). $1 \cdot S = \{1 \cdot 1, 1 \cdot 5\} = \{1, 5\} = S = 5S$ (Check: $5S = \{5 \cdot 1, 5 \cdot 5\} = \{5, 1\}$. OK). **And** $7 \cdot S = \{7 \cdot 1, 7 \cdot 5\} = \{7, 11\} = 11S$. Thus $U(\mathbb{Z}_{12}^*)$ is partitioned into 2 cosets $1, 5 \mid 7, 11$.

Example: Let $G = S_3 = \{I, (123), (132), (12), (13), (23)\}$ and let $S = \{I, (123), (132)\}$ ($=A_3$). We compute the *cosets* of S in G . $I \cdot S = \{I, (123), (132)\} = (123)S = (132)S$. **Now** $(12)S = \{(12)I, (12)(123), (12)(132)\} = \{(12), (23), (13)\}$ (looking at the S_3 table) $= (23)S = (13)S$. Thus S_3 is partitioned into *two left cosets* by S : $I, (123), (132)$ and $(12), (23), (13)$.

Example: Let $G = S_3$ and $S = \{I, (12)\}$ ($((12)^2=I)$). Find the *left cosets* of S in G and give the partition of G they produce. Now $I \cdot S = \{I, (12)\} = (12)S$. **And** $(123) \cdot S = \{(123)I, (123)(12)\} = \{(123), (13)\} = (13)S$. **And** $(132)S = \{(132)I, (132)(12)\} = \{(132), (23)\} = (23)S$. Thus S_3 is partitioned into 3 *left cosets* by S : $I, (12)$; $(123), (13)$ and $(132), (23)$.

Lagrange's Theorem

If S is a *subgroup* of a finite group G then the order of S *divides* the order of G i.e. $|S| \mid |G|$ (**Cardinality** of S divides **cardinality** of G). **Proof.** The *left cosets* of S form a partition of G . We show that every coset has the same number of elements as S . For a fixed $g \in S$ defined $f_g: S \rightarrow gS$ by $f_g(x) = gx$ for all $x \in S$. *Clearly*, by definition f is surjective i.e. $f(S) = gS$. Suppose $f_g(x_1) = f_g(x_2) \Rightarrow gx_1 = gx_2 \Rightarrow g^{-1}gx_1 = g^{-1}gx_2 \Rightarrow x_1 = x_2$, f is *injective*. By the Pigeon Hole principle, $|f(S)| = |S|$ i.e. $|gS| = |S|$.

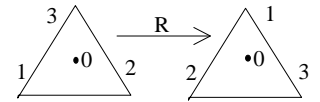
Corollary 1: If G is a finite group of *order* n and $x \in G$ is of order s ($x^s=1$) then $s \mid n$. **Proof:** x generates the *cyclic subgroup* $\{1, x, x^2, \dots, x^{s-1}\}$ with s elements. **Corollary 2:** If G is a finite group of order n then $x^n = 1$ for *all* $x \in G$. **Note:** we are not saying x is of order n since the order of x is the smallest power of s for which $x^s=1$. **Proof:** By corollary 1 if x is of *order* s then $s \mid n$ i.e. $n=rs$ for some r , $x^n = x^{rs} = (x^s)^r = 1^r = 1$.

Corollary 3: If the *order* of G is a prime p , then G is a **cyclic** group of order p , C_p . **Proof:** If $x \in G$ and $x \neq 1$ then x generates a *cyclic* subgroup whose order divides p . But p is prime (only factors are 1 and p) i.e. this *subgroup* is G itself.

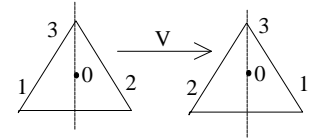
Symmetry Groups

The *symmetries* of regular geometrical figures form a group.

Example 1: Equilateral Triangle. Let R be a rotation about O through $2\pi/3$ which replaces 1 by 2; 2 by 3 and 3 by 1. As a permutation of the vertices R is equivalent to $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (1\ 2\ 3)$. Then $R^2 = \text{rotation through } 4\pi/3$, equivalent to $(1\ 3\ 2)$ and $R^3 = I$ so R will not generate any further symmetries.



Let V be **reflection** in line O3. As a permutation of vertices V is equivalent to $(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$ or $(1\ 2)$. $V^2=I$ so we cannot generate any further symmetries using V alone. There are two other reflections (in O1 and O2)

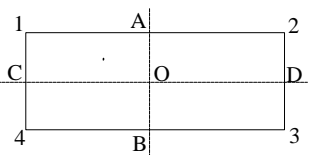


and we can express these in terms of R and V. **VR** (R first) gives the diagram on the left, resulting in a reflection in O1. Equivalently in terms of permutations $(1\ 2)(1\ 2\ 3) = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (2\ 3)$. **VR²** gives reflection in O2 or equivalently permutation $(1\ 3)$.

The other possible combinations of V & R are RV and R²V. However, RV gives $(1\ 2\ 3)(1\ 2) = (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}) = (1\ 3) = VR^2 = VR^{-1}$. Similarly $R^2V = VR$. Thus group of symmetries {I, R, R², V, VR, VR²} is **isomorphic** to S₃ (the same “as a group”) with $R^3 = I = V^2$ and $RV = VR^2 = VR^{-1}$.

Example 2: In general a regular n-sided polygon gives all symmetries as combinations of rotation R through $2\pi/n$ and a reflection V. Then group is {I, R, R², ..., Rⁿ⁻¹, V, VR, VR², ..., VRⁿ⁻¹} of order 2n called the *Dihedral Group* D_n where $R^n = I = V^2$ and $RV = VR^{n-1} = VR^{-1}$. **Example 3:** Regular Tetrahedron (3 dim.) The symmetries give all possible permutations of vertices 1,2,3,4 i.e. the group S₄.

Example 4: Rectangle (not a square). R = rotation through π , $(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}) = (1\ 3)(2\ 4)$. R² = I. V = reflection in line AOB $(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{smallmatrix}) = (1\ 2)(3\ 4)$. V² = I. Now RV = $(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}) = (1\ 4)(3\ 2) = \text{reflection COD}$. VR = RV. Thus group is {I, R, V, VR} where R² = V² = I and VR = RV. This is **Klein's 4-group**, a subgroup of S₄.



Group Presentation

Definition: A group presentation consists of a set of generators and relations between them. These define a group consisting of all possible **distinct** products of the generators. E.g., Examples 1, 2 and 4 above with R and V as generators and relations as **given**. The cyclic groups C_n is generated by “a” where aⁿ = 1 i.e. C_n = {a: aⁿ=1} = {1, a, a², ..., aⁿ⁻¹}

Direct Products of Groups

Definition: The direct product of groups G and H is the set of ordered pairs $G \times H = \{(g,h): g \in G, h \in H\}$ with multiplication defined by $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ where the multiplication of the g_i and h_i take place in G and H respectively. With this definition $G \times H$ is a group with identity (I_G, I_H) (I_G identity of G , I_H identity of H) and the inverse of (g,h) in $G \times H$ is (g^{-1}, h^{-1}) .

Example: $G = C_2 \times C_2$. Take $C_2 = \{1, a\}$, $a^2 = 1$ and $C_2 = \{1, b\}$, $b^2 = 1$ to avoid confusion. Then $G = \{(1,1), (1,b), (a,1), (a,b)\}$ with Cayley table as shown on the right. Note that $(1,b)^2 = (1,1) = (a,1)^2$ and $(1,b)(a,1) = (a,b) = (a,1)(1,b)$. The correspondence $I \Leftrightarrow (1,1)$; $R \Leftrightarrow (1,b)$ and $V \Leftrightarrow (a,1)$ shows that $C_2 \times C_2$ is isomorphic to Klein's 4 group.

	(1,1)	(1,b)	(a,1)	(a,b)
(1,1)	(1,1)	(1,b)	(a,1)	(a,b)
(1,b)	(1,b)	(1,1)	(a,b)	(a,1)
(a,1)	(a,1)	(a,b)	(1,1)	(1,b)
(a,b)	(a,b)	(a,1)	(1,b)	(1,1)

Example: $C_2 \times C_3 \simeq C_6$ (isomorphic). Take $C_2 = \{1, a\}$ ($a^2=1$); $C_3 = \{1, b, b^2\}$ ($b^3=1$). Then $C_2 \times C_3 = \{(1,1), (1,b), (a,1), (a,b), (a,b^2), (1,b^2)\}$. Further, $(a,b)^2 = (a^2, b^2) = (1, b^2)$; $(a,b)^3 = (a, 1)$; $(a,b)^4 = (1, b)$; $(a,b)^5 = (a, b^2)$; $(a,b)^6 = (1, 1)$. Hence $C_2 \times C_3$ is cyclic of order 6 with generator (a,b) .

Normal Subgroups

(1) A subgroup S of group G is called **normal** iff $g^{-1}sg \in S$ for all $g \in G$ and for all $s \in S$. (2) A subgroup S is normal iff $g^{-1}Sg = S$ for all $g \in G$. (Recall that $g^{-1}Sg = \{g^{-1}sg: g \in G, s \in S\}$. These are equivalent. **Proof.** Clearly (2) \Rightarrow (1). Now assume (1). Fix $g \in G$. Then $g^{-1}Sg \subseteq S$. We must show that $S \subseteq g^{-1}Sg$.

Let $s \in S$ then $s = g^{-1}(gsg^{-1})g = g^{-1}(g^{-1}sg)^{-1}g$. Since by assumption $g^{-1}sg \in S$ and S is a subgroup, $(g^{-1}sg)^{-1} \in S$ i.e. S is of the form $g^{-1}s^*g \in g^{-1}Sg$ as required. **Natural Definition:** Let $f: G \rightarrow H$ be a group homomorphism, ($f(g_1 g_2) = f(g_1) f(g_2)$). Then the "Kernel" of f is **Ker $f = \{g \in G, f(g) = I_H\}$** . And Ker f is a **normal** subgroup of G .

Proof: (i) Let a & $b \in \text{Ker } f \subseteq G$ and $f(a) = f(b) = I_H$. Further, $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = I_H \cdot I_H = I_H$ i.e. $ab^{-1} \in \text{Ker } f$; Ker f is a subgroup. (ii) Let $g \in G$ and $s \in \text{Ker } f$ then $f(g^{-1}sg) = f(g^{-1})f(s)f(g) = (f(g))^{-1}I_H f(g) = I_H$ i.e. $g^{-1}sg \in \text{Ker } f$ as required.

Example: Consider $\phi: C_4 = \{1, a, a^2, a^3\} \rightarrow C_2 = \{1, b\}$ (with $a^4=1$ and $b^2=1$). Defined by $\phi: 1$ and a^2 go to 1; a and a^3 go to b . This is a **group homomorphism** with Kernel $\{1, a^2\}$, a normal subgroup of C_4 . (In fact, $\text{Ker } \phi = \{1, a^2\} \simeq C_2$ with generator a^2). It is clear from the definition that all subgroups of an **Abelian** group are normal, since $g^{-1}sg = g^{-1}gs = s$.

Quotient Groups (Factor Groups)

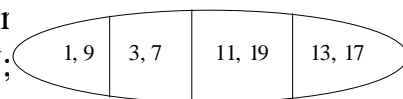
Recall that if N is a *normal* subgroup of G then the **left** cosets gN form a partition of G . Now define *multiplication* of cosets by $(aN)(bN) = \{g = g_1g_2: g_1 \in aN, g_2 \in bN\}$ then we show that **$(aN)(bN) = (ab)N$** for all $a, b \in G$. In particular, the *multiplication* of cosets gives another coset of N .

Proof: (i) $(aN)(bN) \subseteq (ab)N$. Let $g \in (aN)(bN)$ then $g = (an_1)(bn_2)$ for some $n_1, n_2 \in N$ i.e. $g = a(bb^{-1})n_1bn_2 = (ab)(b^{-1}n_1b)n_2$ where $b^{-1}n_1b \in N$ since N is **normal**. Thus we can write this expression as $(ab)n_3$ for some $n_3 \in N$, i.e. $g \in (ab)N$. (ii) $(ab)N \subseteq (aN)(bN)$. Let $g \in (ab)N$ then $g = (ab)n$ for some $n \in N$. $g = abn(b^{-1}b) = (a(bnb^{-1}))(b.1)$ where $bnb^{-1} = (b^{-1}nb)^{-1} \in N$ since N is a *normal* subgroup and $1 \in N$ i.e. $g \in (aN)(bN)$.

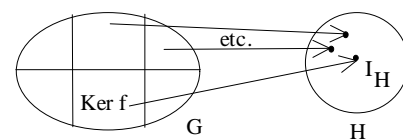
Theorem: The set of *left cosets* of N in G denoted by G/N form a group under coset multiplication. **Proof:** Closure. Already Proved. Associativity: Let $aN, bN, cN \in G/N$. $((aN)(bN))(cN) = ((ab)N)(cN) = (ab)cN = a(bc)N$ (since G is *associative*) $= (aN)((bc)N) = (aN)((bN)(cN))$. Identity: $I_{G/N} = N = 1.N$ since $(1N)aN = (1a)N = aN = (a.1)N = (aN)(1N)$. Inverse: $(aN)^{-1} = (a^{-1}N)$ since $(aN)(a^{-1}N) = (aa^{-1})N = 1.N = N = (a^{-1}a)N = (a^{-1}N)(aN)$.

Definition: We call G/N the *quotient* group of G by N (remember that N has to be a *normal* subgroup). **Example:** $G = U(\mathbf{Z}_{20}^*) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ with *multiplication* mod 20. This is an Abelian group so all subgroups are normal. Further, $9^2 \equiv 1 \pmod{20}$ so $N = \{1, 9\}$ is a *normal* subgroup of order 2 ($\simeq C_2$).

The *left cosets* of N are: $1.N = \{1, 9\} = 9.N$. $3.N = \{3, 3.9 \equiv 7\} = 7.N$. $11.N = \{11, 19\} = 19.N$. $13.N = \{13, 17\} = 17.N$. Thus G/N can be *represented* as in the diagram, where for example $\{3, 7\}\{11, 19\} = (3N)(11N) = (3.11 \equiv 13)N = \{13, 17\}$ (or $(7N)(19N) = 7.19 \equiv 13 = \{13, 17\}$). In fact, $(13N)^2 = (13.13)N = 9N$; $(13N)^3 = (13.9)N = 17N$; $(13N)^4 = (13.17)N = 1N$. So G/N is a *cyclic* group of order 4 **generated** by $13N$.



Theorem: Let $f: G \rightarrow H$ be a group *homomorphism* then $f(x) = f(y)$ iff x and y belong to the same coset of $G/\text{Ker } f$. **Proof:** (i) Assume $f(x) = f(y)$ then $f(x^{-1}y) = f(x^{-1})f(y) = (f(x))^{-1}f(y) = (f(y))^{-1}f(y) = I_H$ i.e. $x^{-1}y \in \text{Ker } f$.



Then *both* x and y belong to the **coset** $x\text{Ker } f$ (Clearly $x \in x\text{Ker } f$) since $y = x(x^{-1}y) \in x\text{Ker } f$. In fact, $x\text{Ker } f = y\text{Ker } f$. (ii) **Assume** x and $y \in x\text{Ker } f$ i.e. $y = xk$ for some $k \in \text{Ker } f$ (where $f(k) = 1$). **Then** $f(y) = f(xk) = f(x)f(k) = f(x)$.

The First Isomorphism Theorem

If $f: G \rightarrow H$ is a group *homomorphism* then $G/\text{Ker } f \simeq f(G)$. **Proof:** ($f(G)$ is a *subgroup* of H , $\text{Ker } f$ is a *normal subgroup* of G). Define a *function* $\theta: G/\text{Ker } f \rightarrow f(G)$ by $\theta(x\text{Ker } f) = f(x)$ for all *cosets* $x\text{Ker } f \in G/\text{Ker } f$. By the **previous** theorem this is a well defined *injective* function on $G/\text{Ker } f$. By the definition of $f(G)$ it is **surjective**.

It remains to show θ is a *group homomorphism*. $\theta((x\text{Ker } f)(y\text{Ker } f)) = \theta((xy)\text{Ker } f) = f(xy)$ by *definition* of $\theta = f(x)f(y) = \theta(x\text{Ker } f)\theta(y\text{Ker } f)$.

Example: Let \mathbf{Z} be the group of *integers* under addition and $\mathbf{Z}_m = \{0, 1, \dots, m-1\}$ the group of integers under *addition mod m*. Let $f: \mathbf{Z} \rightarrow \mathbf{Z}_m$ be defined by reducing each $n \in \mathbf{Z}$ to the unique *equivalent* in \mathbf{Z}_m (by *modulo m* operations). $\text{Ker } f = m\mathbf{Z}$ and by the first *Isomorphism Theorem* $\mathbf{Z}/\text{Ker } f$ i.e. $\mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}_m$.