

# Math 551 – Algebra – Fall 2002

Richard Lyons  
Rutgers University  
New Brunswick, New Jersey, USA

## A. Groups

### 1. Definition and examples.

#### 1a. Definition and rudimentary properties

**Definition.** A group  $(G, \cdot)$  is a set  $G$  together with a binary operation  $\cdot : G \times G \rightarrow G$ , written for simplicity as multiplication, such that

- (1) The operation is associative:  $g(hk) = (gh)k$  for all  $g, h, k \in G$ ;
- (2) There exists  $1 \in G$  such that  $g1 = 1g = g$  for all  $g \in G$ ;
- (3) For every  $g \in G$  there is  $g^{-1} \in G$  such that  $gg^{-1} = g^{-1}g = 1$ .

(If (3) is dropped, we have the definition of “monoid”. If (2) and (3) are dropped, we have the definition of “semigroup”. If  $gh = hg$  for all  $g, h \in G$ , then  $G$  is said to be abelian. In this case, and only in this case, additive notation  $g + h$  may be used for the product  $gh$ , and 0 instead of 1, and  $-g$  instead of  $g$ .)

**Proposition.** Let  $G$  be a group. Then

- 1) 1 is the only identity element of  $G$ ; indeed it is the unique right identity element of  $G$  and the unique left identity element.
- 2) For each  $x \in G$ ,  $x^{-1}$  is the unique inverse of  $x$ ; indeed it is the unique right inverse and the unique left inverse.
- 3) If  $g, h \in G$  then the equation  $gx = h$  has a unique solution in  $G$ , namely  $x = g^{-1}h$ ; likewise  $xg = h$  has the unique solution  $x = hg^{-1}$ .
- 4) If  $n \geq 3$  and  $x_1, \dots, x_n \in G$ , then any two associations of  $x_1 \dots x_n$  represent the same element of  $G$ .
- 5) If  $x, y \in G$  then  $(xy)^{-1} = y^{-1}x^{-1}$  and  $(x^{-1})^{-1} = x$ .

**Proof.** 1) If  $e$  is a right identity then  $1_G = 1_G e = e$ , and similarly for left identity elements.

2) If  $y$  is a right inverse then  $x^{-1} = x^{-1}1_G = x^{-1}(xy) = (x^{-1}x)y = 1_G y = y$ . Similarly for left inverses.

3) Trivial

4) Induction on  $n$ , starting with  $n = 3$ , where it is the associative law. Show that the element represented by any association of  $x_1 \dots x_n$  equals the element represented by the standard association  $[x_1 \cdots x_n] = x_1(x_2(x_3(\cdots(x_{n-1}x_n)\cdots)))$ . Namely any association equals a product of associations of  $x_1, \dots, x_k$  and  $x_{k+1}, \dots, x_n$ , so equals  $[x_1 \cdots x_k][x_{k+1} \cdots x_n]$  by induction. This equals

$$(x_1[x_2 \cdots x_k])[x_{k+1} \cdots x_n] = x_1([x_2 \cdots x_k][x_{k+1} \cdots x_n]) = x_1[x_2 \cdots x_n] = [x_1 \cdots x_n],$$

the three steps by associativity, induction and definition, respectively.

5)  $(y^{-1}x^{-1})xy = 1$  and  $x^{-1}x = 1$ ; now use the first statement of 3). QED

### 1b. Some examples

**Ex. A.** Let  $X$  be any set. A permutation of  $X$  is a bijection  $\sigma : X \rightarrow X$ , i.e., a mapping on  $X$  which is one-to-one and onto  $X$ . Let

$$\Sigma_X = \{\sigma : X \rightarrow X \mid \sigma \text{ is a permutation of } X\}.$$

For  $\sigma, \tau \in \Sigma_X$  define  $\sigma\tau = \sigma \circ \tau$ , the composite of  $\sigma$  and  $\tau$ . Also let  $1_X$  be the identity mapping  $1_X(x) = x$ ,  $x \in X$ , and for each  $\sigma \in \Sigma_X$ , let  $\sigma^{-1}$  be the inverse mapping:  $\sigma^{-1}(x) = y \iff \sigma(y) = x$ . Then  $\Sigma_X$  is a group.

Remarks: Composition of mappings is always associative, whether or not the mappings are injective or surjective.

If  $X$  is finite, then  $|\Sigma_X| = |X|!$ .

We write mappings on the left, so  $\sigma \circ \tau(x) = \sigma(\tau(x))$ .

**Ex. B.** Let  $V$  be a vector space (of any dimension) over a field  $k$ . Then  $GL(V)$ , the set of all invertible linear transformations from  $V \rightarrow V$ , is a group, under composition of mappings.

Related to this, for a given natural number  $n$  and field (indeed any commutative ring)  $k$ , is the group  $GL_n(k)$  of all invertible  $n \times n$  matrices with entries in  $k$ , under the operation of matrix multiplication.

**Ex. C.** Let  $G$  be a group. A subset  $H$  of  $G$  which is itself a group with respect to the same operation is a subgroup of  $G$ . (Notation:  $H \leq G$ ; if also  $H \neq G$  we write  $H < G$ .)

For instance, if  $G = \Sigma_X$  and  $x \in X$ , then  $G_x = \{\sigma \in \Sigma_X \mid \sigma(x) = x\}$  is a subgroup of  $G$ .

Also if  $n$  is a natural number and  $k$  is a commutative ring, then we define  $SL_n(k) = \{A \in GL_n(k) \mid \det(A) = 1\}$  and have that  $SL_n(k) \leq GL_n(k)$ .

Trivially, in any group  $G$ ,  $\{1\}$  (written 1) and  $G$  itself are both subgroups.

**Proposition.** *If  $G$  is a group and  $H \subseteq G$ , then  $H \leq G$  if and only if  $H$  is nonempty and closed under multiplication and inversion. In that case  $1_H = 1_G$  and for  $x \in H$ ,  $x^{-1}$  has the same meaning in both  $H$  and  $G$ .*

**Proof.** Left to reader. QED

**Ex. D.** Let  $X$  be any set, and  $\Phi$  a structure on  $X$ . An automorphism of  $\Phi$  is a bijection  $X \rightarrow X$  preserving  $\Phi$ . The set  $\text{Aut}(\Phi)$  of all automorphisms of  $\Phi$  is a group, indeed a subgroup of  $\Sigma_\Phi$ .

### 1c. Isomorphisms, homomorphisms, representations

**Definition.** Let  $G$  and  $H$  be groups. An isomorphism from  $G$  to  $H$  is a mapping  $\phi : G \rightarrow H$  such that

- 1)  $\phi(xy) = \phi(x)\phi(y)$  for all  $x, y \in G$ .
- 2)  $\phi$  is a bijection.

In 1), the products  $xy$  and  $\phi(x)\phi(y)$  are in  $G$  and  $H$ , respectively.

If 2) is omitted, we have the definition of homomorphism.

**Proposition.** Let  $\phi : G \rightarrow H$  be a homomorphism. Then  $\text{im}(\phi) = \phi(G) \leq H$ , and  $\ker(\phi) = \phi^{-1}(1) \leq G$ . Moreover  $\phi$  is injective if and only if  $\ker(\phi) = 1$ . In this case  $\phi$  induces an isomorphism from  $G$  to  $\phi(G)$ .

**Proof.** Left to reader. QED

We write  $G \cong H$  if and only if there exists an isomorphism from  $G$  to  $H$ .

The relation  $\cong$  is then reflexive, symmetric and transitive on the class of all groups. Indeed one sees quickly from the definition of isomorphism that

- 1) For any  $G$ ,  $\text{id}_G : G \rightarrow G$  is an isomorphism;
- 2) If  $\phi : G \rightarrow H$  is an isomorphism, then  $\phi^{-1} : H \rightarrow G$  is an isomorphism; and
- 3) If  $\phi : G \rightarrow H$  and  $\psi : H \rightarrow K$  are isomorphisms, then  $\psi \circ \phi : G \rightarrow K$  is an isomorphism.

and these facts imply respectively that  $\cong$  is reflexive, symmetric and transitive. Consequently (ignoring set-theoretic difficulties) the class of all groups is partitioned into “isomorphism classes” or “isomorphism types”.

As an example of isomorphism, let  $X$  be a set,  $x \in X$ ,  $G = \Sigma_X$  and  $G_x$  the stabilizer of  $x$  in  $G$ , as above. Then  $G_x$  is isomorphic to  $\Sigma_{X-\{x\}}$ , via the isomorphism  $G_x \rightarrow \Sigma_{X-\{x\}}$  taking  $\sigma \mapsto \sigma|_{(X-\{x\})}$ .

For another example of isomorphisms, let  $X$  and  $Y$  be sets and suppose that there exists a bijection  $f : X \rightarrow Y$ . Define  $\phi_f : \Sigma_X \rightarrow \Sigma_Y$  by  $\phi_f(\sigma) = f \circ \sigma \circ f^{-1}$ . Notice that the right side is a composite of bijections so is a bijection, and maps  $Y$  to  $Y$ . Then  $\phi_f$  is an isomorphism. Indeed  $\phi_f(\sigma\tau) = (f\sigma f^{-1})(f\tau f^{-1}) = f\sigma\tau f^{-1}$ . Moreover,  $\phi_f\phi_{f^{-1}} : \Sigma_Y \rightarrow \Sigma_Y$  takes  $\sigma$  to  $\phi_f(f^{-1}\sigma f^{-1}) = f f^{-1}\sigma f^{-1} f^{-1} = \sigma$ , so  $\phi_f\phi_{f^{-1}} = 1_{\Sigma_Y}$ , and similarly  $\phi_{f^{-1}}\phi_f = 1_{\Sigma_X}$ . Hence  $\phi_f$  is a bijection (with inverse  $\phi_{f^{-1}}$ ).

Thus if  $X$  and  $Y$  are two sets of the same cardinality, then  $\Sigma_X \cong \Sigma_Y$ .

We write  $\Sigma_n$  for  $\Sigma_{\{1,2,\dots,n\}}$ . Thus for any finite  $X$ ,  $\Sigma_X \cong \Sigma_n$  where  $n = |X|$ . However, there are (as long as  $n > 2$ ) many such isomorphisms, for a given  $X$ .

Yet another example of isomorphism is obtained by taking an  $n$ -dimensional vector space  $V$  over a field  $k$ , and choosing an ordered basis  $B$  of  $V$ . For each linear transformation  $T : V \rightarrow V$ , let  $[T]_B$  be the matrix of  $T$  with respect to  $B$ . The mapping

$$GL(V) \rightarrow GL_n(k), \quad T \mapsto [T]_B$$

is an isomorphism. Thus there are many isomorphisms between these two groups, (at least) one for each choice of  $B$ .

If  $\phi : G \rightarrow H$  is an isomorphism, and  $\phi(1_G) = h$ , then  $h^2 = \phi(1_G)\phi(1_G) = \phi(1_G^2) = \phi(1_G) = h$ , so  $h = 1_H$ . Likewise for any  $x \in G$ ,  $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1_G) = 1_H$  and vice-versa, so  $\phi(x^{-1}) = \phi(x)^{-1}$ . Indeed these properties hold for any homomorphism  $\phi$ .

We shall consider isomorphic groups to be the “same”, and group theory is the study of those properties of groups which are invariant under isomorphism. Representation theory, on the other hand, is the study, for a given group  $G$ , of structures  $\Phi$  and homomorphisms  $G \rightarrow \text{Aut}(\Phi)$ .

If  $G$  is a group, then  $\text{Aut}(G)$ , the set of all isomorphisms from  $G$  to itself, is again a group.

**Exercise.** If  $G \cong H$  then  $\text{Aut}(G) \cong \text{Aut}(H)$ .

Representations of any group  $G$  are not hard to find. We give three important examples.

1. For each  $g \in G$  define  $\text{Int}(G) : G \rightarrow G$  by  $\text{Int}(g)(x) = gxg^{-1}$ . Then  $\text{Int}(g) \in \text{Aut}(G)$ , and the mapping

$$i : G \rightarrow \text{Aut}(G), \quad g \mapsto \text{Int}(g)$$

is a homomorphism. In general this homomorphism is not surjective; its image is called  $\text{Inn}(G)$  and an automorphism is called inner if and only if it lies in  $\text{Inn}(G)$ . Likewise in general this homomorphism is not injective; its kernel is

$$Z(G) = \{g \in G \mid gxg^{-1} = x \ \forall x \in G\} = \{g \in G \mid gx = xg \ \forall x \in G\}.$$

At one extreme, if  $G$  is abelian, i.e., satisfies the commutative law

$$gh = hg \ \forall g, h \in G$$

then  $Z(G) = G$  and  $\text{Inn}(G) = 1$ . At the other extreme, if  $Z(G) = 1$ , then  $G \cong \text{Inn}(G)$ .

**Exercise.** If  $X$  is a set, what is  $Z(\Sigma_X)$ ?

2. If  $G$  is a group, consider the symmetric group  $\Sigma_G$  (the set of all permutations of  $G$ , disregarding their effect on the group structure, i.e. whether or not they are automorphisms). For each  $g \in G$  define  $\lambda_g : G \rightarrow G$

$$\lambda_g(x) = gx, \ \forall x \in G.$$

Then

$$\lambda_g \circ \lambda_h(x) = g(hx) = (gh)x = \lambda_{gh}(x) \ \forall x \in G \tag{1A}$$

and of course  $\lambda_1 = id_G$  is the identity function on  $G$ .

Consequently  $\lambda_g \lambda_{g^{-1}} = \lambda_1 = id_G = \lambda_{g^{-1}} \lambda_g$ , so each  $\lambda_g \in \Sigma_G$  and then (1A) shows that the mapping

$$\lambda : G \rightarrow \Sigma_G, g \mapsto \lambda_g$$

is a homomorphism. If  $\lambda_g = \lambda_h$  then  $g = \lambda_g(1) = \lambda_h(1) = h$  so  $\lambda$  is injective. We have proved Cayley's Theorem:

**Theorem.** *Every group  $G$  is isomorphic to a subgroup of  $\Sigma_G$  (via  $\lambda$ ).*

This is generally not very useful, except for philosophical reasons: groups are inherently groups of permutations, or can be viewed as such. Moreover one can try to “decompose” this representation.

One can also define  $\rho_g : G \rightarrow G$  by  $x \mapsto xg$ , and we get the possibly different representation  $\rho : G \rightarrow \Sigma_G$  defined by  $\rho(g) = \rho_{g^{-1}}$ .

**Exercise.** *Let  $G$  be a group. For any subgroup  $H \leq G$ , define  $C_G(H) = \{g \in G \mid gh = hg \forall h \in H\}$ . Show that  $C_G(H) \leq G$ . Show also that  $C_{\Sigma_G}(\rho(G)) = \lambda(G)$  and  $C_{\Sigma_G}(\lambda(G)) = \rho(G)$ .*

3. For any group  $G$ , let  $V$  be a vector space over  $\mathbf{R}$  (or any field  $k$ ) with basis  $G$ . Thus  $V$  is the set of formal linear combinations  $\sum_{x \in G} \alpha_x x$  such that  $\alpha_x \in k$  for all  $x \in G$  and almost all  $\alpha_x$  are 0 (i.e.  $\alpha_x \neq 0$  for only finitely many elements  $x$  of  $G$ ). The vector space operations on  $V$  are the obvious formal operations. For each  $g \in G$  there is a linear transformation  $\Lambda_g : V \rightarrow V$  defined by

$$\Lambda_g \left( \sum_x \alpha_x x \right) = \sum_x \alpha_x gx = \sum_{y \in G} \alpha_{g^{-1}y} y,$$

and the mapping  $\Lambda : G \rightarrow GL(V)$ ,  $g \mapsto \Lambda_g$  is a homomorphism. It is easily checked that  $\Lambda$  is injective, so we get a matrix version of Cayley's Theorem above. In particular: Every group  $G$  of finite cardinality  $|G| = n$  is isomorphic to a subgroup of  $GL_n(k)$  for any field  $k$ .

The decomposition of this “regular” representation is crucial for the representation theory of finite groups.

**Remark.** An element  $\sum \alpha_x x$  of  $V$  is really just an array of coefficients  $(\alpha_x)$  indexed by  $G$ , that is, a function  $f : G \rightarrow k$  (namely the one such that  $f(x) = \alpha_x$  for every  $x \in G$ ). Regarding elements of  $V$  this way we find that

$$\Lambda_g(f)(y) = f(g^{-1}y), \quad f \in V, \quad g, y \in G.$$

Note the  $g^{-1}$  (not  $g$ ), so that  $\Lambda_g \Lambda_h = \Lambda_{gh}$  (not  $\Lambda_{hg}$ ).

**Ex. E.** An example similar to, but different from,  $GL_2(\mathbf{C})$  is the group of fractional linear transformations of the complex plane, that is, the group  $LF(2, \mathbf{C})$  of all permutations

$\sigma$  of the extended complex plane (Riemann sphere)  $\mathbf{C} \cup \{\infty\}$  of the form

$$\sigma(z) = \frac{az + b}{cz + d}$$

such that  $a, b, c, d$  are complex constants for which  $ad - bc \neq 0$ . This last condition prevents  $\sigma$  from being a constant mapping, so is actually redundant. We may write  $\sigma = \sigma_A$ , where  $A$  is the “matrix of coefficients”

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

It is then easy to check that

$$LF(2, \mathbf{C}) = \{\sigma_A \mid A \in GL_2(\mathbf{C})\}, \text{ and } \sigma_A \sigma_B = \sigma_{AB} \forall A, B \in GL_2(\mathbf{C}).$$

However, the homomorphism

$$\phi : GL_2(\mathbf{C}) \rightarrow LF(2, \mathbf{C}) \text{ defined by } \phi(A) = \sigma_A,$$

is not an isomorphism, because it fails to be injective. In fact  $\sigma_{cA} = \sigma_A$  for every  $A$  and for every  $c \in \mathbf{C}^\times$ .

**Exercise.** Show that for any  $A, B \in GL_2(\mathbf{C})$ , we have  $\sigma_A = \sigma_B$  if and only if  $B = cA$  for some  $c \in \mathbf{C}^\times$ . Explain why this assertion is essentially the same as the assertion that  $\ker \phi = \{cI \mid c \in \mathbf{C}^\times\}$ , where  $I$  is the  $2 \times 2$  identity matrix.

**Exercise.** Let  $G$  be a group and  $\alpha \in \text{Aut}(G)$ . Set

$$C_G(\alpha) = \{g \in G \mid \alpha(g) = g\} \text{ and } I_G(\alpha) = \{g \in G \mid \alpha(g) = g^{-1}\}.$$

Show that  $C_G(\alpha) \leq G$ , but that  $I_G(\alpha)$  need not be a subgroup of  $G$ . Show that if  $I_G(\alpha) = G$ , then  $G$  is abelian. Show that if  $G$  is finite and  $|C_G(\alpha)| > |G|/2$ , then  $C_G(\alpha) = G$ . Show that if  $G$  is finite and  $|I_G(\alpha)| > |G|/2$ , then  $\alpha^2 = 1$ . Finally show that if  $G$  is finite and  $|I_G(\alpha)| > 3|G|/4$ , then  $G$  is abelian and  $I_G(\alpha) = G$ .

## 1d. Powers; cyclic groups

**Definition.** Let  $G$  be any group and  $g \in G$ . Define  $g^n$  for  $n \in \mathbf{Z}$  as follows:  $g^0 = 1_G$  and  $g^{n+1} = g^n g$  for  $n \geq 0$ ;  $g^n = (g^{-n})^{-1}$  for  $n < 0$ . (In an abelian group with additive notation, we write  $ng$  instead of  $g^n$ .)

**Proposition.** Let  $g \in G$  and  $m, n \in \mathbf{Z}$ . Then  $g^m g^n = g^{m+n}$ , and  $(g^m)^{-1} = g^{-m}$ . Moreover  $(g^m)^n = g^{mn}$ .

This is a consequence of 4) of the Proposition above, when  $m$  and  $n$  have the same sign; otherwise, there are several cases, e.g. if  $n \geq |m|$  with  $m < 0$ , then  $g^n = g^{-m} g^{m+n}$ , so  $g^m g^n = g^m g^{-m} g^{m+n} = g^{m+n}$ . The remaining assertions are left to the reader to prove, as is the following elementary fact:

**Proposition.** If  $\phi : G \rightarrow H$  is a homomorphism and  $g \in G$ , then  $\phi(g^n) = (\phi(g))^n$  for every  $n \in \mathbf{Z}$ .

Given  $g \in G$ , the set  $\{g^n \mid n \in \mathbf{Z}\}$  is a subgroup of  $G$ , and is denoted by  $\langle g \rangle$ . A group arising in this way—as the powers of a single element—is called cyclic, and  $g$  is called a generator.

Examples of cyclic groups:  $\mathbf{Z}$ , the set of integers, with respect to addition. 1 is a generator, 0 is the identity element,  $-g$  is the inverse of  $g$ . Additive notation is customary. Also  $\mathbf{Z}_n$ , the integers mod  $n$  (here  $n$  is a positive integer), with elements  $[i]$ ,  $i \in \mathbf{Z}$ , and  $[i] = [j]$  if and only if  $i \equiv j \pmod{n}$ ;  $[i] + [j] = [i + j]$ . A generator is  $[1]$ .

**Theorem.** Every cyclic group  $G$  is isomorphic to exactly one of the groups  $\mathbf{Z}$ ,  $\mathbf{Z}_n$ ,  $n = 1, 2, \dots$ . Moreover if  $G = \langle g \rangle$ , then there is a unique isomorphism  $\mathbf{Z} \rightarrow G$  or  $\mathbf{Z}_n \rightarrow G$ , as the case may be, taking  $1 \mapsto g$  or  $[1] \mapsto g$ .

**Proof.** If  $g^n \neq 1$  for all  $n \neq 0$ , then the elements  $g^n$ ,  $n \in \mathbf{Z}$  are all different (for  $g^n = g^m$  implies  $g^{n-m} = g^n(g^n)^{-1} = 1$  and hence  $n - m = 0$ ). Map  $\mathbf{Z} \rightarrow G$  by  $n \mapsto g^n$ . This is clearly injective, surjective, and multiplicative.

If  $g^n = 1$  for some  $n \neq 0$ , then  $g^{-n} = (g^n)^{-1} = 1$ , so we may take  $n > 0$ . We may also assume that  $n$  is the smallest positive integer such that  $g^n = 1$ . Then the elements  $g^i$ ,  $0 \leq i < n$ , are all distinct, by a similar argument, and  $i \equiv j \pmod{n}$  implies  $g^i = g^j$ . The mapping  $\phi : \mathbf{Z}_n \rightarrow G$  taking  $[m] \mapsto g^m$ ,  $0 \leq m < n$  is then well-defined and injective. For any  $i \in \mathbf{Z}$  we may write  $i = qn + r$  with  $0 \leq r < n$ , so  $g^i = g^r$  and  $\phi$  is surjective. Finally  $g^m g^{m'} = g^{m+m'}$ , so  $\phi$  is an isomorphism.

The uniqueness of the isomorphism is clear since if  $1$  or  $[1]$  maps to  $g$ , then  $m = 1 + \dots + 1$  or  $[m] = [1] + \dots + [1]$  maps to  $g \dots g = g^m$  by repeated use of the multiplicativity of the isomorphism. QED

One corollary of this is that we can compute the structure of the automorphism group of a cyclic group, which we do below. As a simpler corollary we can define the order of an element.

**Definition.** Let  $G$  be a group and  $g \in G$ . The order of  $g$  is  $|g| = |\langle g \rangle|$ , the cardinality of  $\langle g \rangle$ .

Thus the order of  $g$  is a positive integer or  $\infty$ . The identity element has order 1. In a finite group, every element has finite order.

**Theorem.** Subgroups and homomorphic images of cyclic groups are cyclic.

**Proof.** The second statement means that if  $G$  is cyclic and  $\phi : G \rightarrow H$  is a homomorphism, then  $\phi(G)$  is cyclic. But if  $G = \langle g \rangle$ , then every element of  $\phi(G)$  has the form  $\phi(g^n) = (\phi(g))^n$  for some  $n \in \mathbf{Z}$ , so  $\phi(G) = \langle \phi(g) \rangle$  is cyclic.

For the first statement, we know that  $G \cong \mathbf{Z}$  or  $\mathbf{Z}_n$  for some  $n > 0$ , so it is sufficient to prove the statement for  $\mathbf{Z}$  and  $\mathbf{Z}_n$ . We prove a stronger statement:

**Theorem.** *The distinct subgroups of  $\mathbf{Z}$  are the subgroups  $\langle n \rangle$ ,  $n > 0$ . The distinct subgroups of  $\mathbf{Z}_n$  are the subgroups  $\langle [m] \rangle$ ,  $m > 0$ ,  $m$  dividing  $n$ ; the subgroup  $\langle [m] \rangle$  has order  $n/m$  if  $m$  divides  $n$ . Consequently a cyclic group of order  $n$  has a subgroup of order  $m$  if and only if  $m$  divides  $n$ .*

Obviously the listed subgroups are indeed subgroups. In  $\langle n \rangle \leq \mathbf{Z}$ ,  $n$  is the least positive element. Moreover if  $m > 0$  divides  $n$ , then  $[m]$  has order  $n/m$  in  $\mathbf{Z}_n$ . These facts imply that the claimed subgroups are distinct.

It remains to show that every subgroup is one of them. Let  $H \leq \mathbf{Z}$ . Then either  $H = 0$  or  $H$  contains a positive integer  $m$  (since  $H$  is closed under inversion). Similarly if  $H \leq \mathbf{Z}_n$ , then either  $H = 0$  or  $H$  contains  $[m]$  for some  $0 < m < n$ . Let  $m$  be the least such integer, in either case. Then  $H$  contains  $\langle m \rangle$  or  $\langle [m] \rangle$  respectively, and we argue that  $H$  in fact equals that cyclic group. For if  $k \in H$  (or  $[k] \in H$ ) we may write  $k = qm + r$  with  $0 \leq r < m$ . Then  $r = k - qm \in H$  (or  $[r] \in H$ ). By minimality of  $m$ ,  $r = 0$  so  $k = qm \in H$  (or  $[k] = q[m] \in H$ ). Hence  $H = \langle m \rangle$  or  $\langle [m] \rangle$ . QED

**Exercise.** *If  $g \in G$  and  $g^n = 1$  for some integer  $n \neq 0$ , then the order of  $g$  is finite and divides  $n$ .*

**Exercise.** *If  $g \in G$  has finite order  $n$ , and  $\phi : G \rightarrow H$  is a homomorphism, then  $\phi(g)$  has finite order dividing  $n$ .*

To determine the automorphism group of a cyclic group  $G$ , observe first that  $G \cong \mathbf{Z}$  or  $\mathbf{Z}_n$ , so  $\text{Aut}(G) \cong \text{Aut}(\mathbf{Z})$  or  $\text{Aut}(\mathbf{Z}_n)$ . Thus it suffices to consider the groups  $G = \mathbf{Z}$  and  $\mathbf{Z}_n$ ,  $n > 0$ . Accordingly let  $g = 1$  or  $[1]$ . If  $\phi \in \text{Aut}(G)$  then  $G = \phi(G) = \langle \phi(g) \rangle$ , so  $\phi(g)$  is also a generator of  $G$ . Indeed for each generator  $h$  of  $G$  there exists by the above theorem a unique  $\phi \in \text{Aut}(G)$  such that  $\phi(g) = h$ . Hence the mapping

$$\phi \mapsto \phi(g)$$

is a bijection between  $\text{Aut}(G)$  and the set of all generators of  $G$ .

Now if  $G = \mathbf{Z}$  it is easy to see that the only generators of  $G$  are 1 and  $-1$ . Hence  $\text{Aut}(\mathbf{Z})$  consists of two elements, the identity mapping and inversion, and  $\text{Aut}(\mathbf{Z}) \cong \mathbf{Z}_2$ .

On the other hand if  $G = \mathbf{Z}_n$  then (exercise) the only generators of  $G$  are the elements  $[m]$  such that  $\gcd(m, n) = 1$ . Thus for each such  $[m]$  there exists a unique  $\phi_{[m]} \in \text{Aut}(\mathbf{Z}_n)$  such that  $\phi_{[m]}([1]) = [m]$ . Moreover

$$\phi_{[m]} \circ \phi_{[m']}([1]) = \phi_{[m]}([m']) = \phi_{[m]}(m'[1]) = m'\phi_{[m]}([1]) = m'[m] = [mm'],$$

so  $\phi_{[m]} \circ \phi_{[m']} = \phi_{[mm']}$ . Thus if we let  $S$  be the set of all generators of  $G$ , and use the multiplication in the ring  $\mathbf{Z}/n\mathbf{Z}$  as the operation on  $S$ , then  $\text{Aut}(G) \cong S$  (and  $S$  is a group).

**Exercise.**  *$S$  is the group of multiplicative units in the ring  $\mathbf{Z}/n\mathbf{Z}$ .*

These results imply:

**Theorem.**  $\text{Aut}(\mathbf{Z}) \cong \mathbf{Z}_2$ , and for  $n > 0$ ,  $\text{Aut}(\mathbf{Z}_n)$  is isomorphic to the multiplicative group of units in the ring  $\mathbf{Z}/n\mathbf{Z}$ .

## 1e. Generation

**Lemma.** The intersection of any collection of subgroups of a group  $G$  is a subgroup of  $G$ .

**Proof.** Left to reader. QED

**Definition.** Let  $G$  be a group and  $S$  any subset of  $G$ . The intersection of all subgroups of  $G$  containing  $S$  ( $G$  is one of them) is a subgroup of  $G$  called  $\langle S \rangle$ , the subgroup of  $G$  generated by  $S$ .

**Proposition.**  $\langle S \rangle = \{s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} \mid n \geq 0, s_i \in S \text{ and } \epsilon_i = \pm 1 \forall i\}$ .

The expressions on the right are called “words in  $S \cup S^{-1}$ ”. Here if  $n = 0$ , the empty product is interpreted as  $1_G$ .

**Proof.** Since  $(xy)^{-1} = y^{-1}x^{-1}$  and  $(x^{-1})^{-1} = x$ , the right side  $H$  is obviously a subgroup of  $G$ , and  $S \subseteq H$  via words of length 1. Therefore  $\langle S \rangle \leq H$ . On the other hand  $\langle S \rangle$  contains each  $s^{\pm 1}$ ,  $s \in S$ , and hence contains all the elements of  $H$ , as it is closed under inversion and products. QED

Though the situation is nice for cyclic groups, those generated by one element, it quickly becomes intractable for groups generated by two or more elements.

**Exercise.**  $\Sigma_n$  is generated by two elements.

Hint: Every permutation is the composition of “transpositions”, i.e., interchanges of pairs of objects. The transposition  $(12)$  and the cycle  $(12 \cdots n)$  generate a subgroup containing all transpositions and hence generate  $\Sigma_n$ .

Furthermore, it can be shown that  $\lim_{n \rightarrow \infty} P(\langle x, y \rangle = \Sigma_n) = 1$ , for  $x$  and  $y$  chosen (uniformly) randomly and independently in  $\Sigma_n$ .

Another example of this is

$$SL_2(\mathbf{Z}) = \left\langle \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \right\rangle.$$

Taking matters to larger extremes, Burnside proposed the following problem a hundred years ago.

Let  $m$  and  $n$  be positive integers. Let  $G$  be a group such that  $g^n = 1$  for all  $g \in G$ , and  $G = \langle S \rangle$  for some set of cardinality  $m$ . Is  $G$  necessarily finite?

The answer, which remained unknown for 50 years, turns out to be “no” in general, although for some very small values of  $n$ , it is “yes”. Of course it is “yes” for  $m = 1$ . It

is not known for all values of  $m$  and  $n$ , and in particular the case  $(m, n) = (2, 5)$  remains open.

On the other hand, some non-finitely-generated groups can be very tractable. The additive group  $\mathbf{Q}^+$  of rational numbers, for instance, is “locally cyclic”: every finitely generated subgroup is cyclic, even though  $\mathbf{Q}^+$  itself is not cyclic (or finitely generated). The better behavior is largely due to the fact that  $\mathbf{Q}^+$  is abelian.

## 1f. Abelian groups

**Exercise.** If  $G$  is abelian then  $(xy)^m = x^m y^m$  for all  $x, y \in G$  and  $m \in \mathbf{Z}$ . Moreover if  $G$  is abelian and generated by elements  $x_1, \dots, x_r$  and  $x_i^n = 1$  for all  $i$ , then  $G$  is finite and its cardinality is at most  $n^r$ .

Examples of abelian groups are cyclic groups, the additive group of the rationals, reals, complexes (or any field), the multiplicative group of nonzero rationals, reals, complexes (or any field), the multiplicative group of all roots of unity in  $\mathbf{C}$  (or in any field), and the matrix group

$$U = \left\{ \left[ \begin{array}{cc} 1 & c \\ 0 & 1 \end{array} \right] \mid c \in \mathbf{C} \right\}.$$

**Exercise.** Subgroups and homomorphic images of abelian groups are abelian.

**Definition.** A periodic group (torsion group) is one all of whose elements have finite order. The exponent of a torsion group is the least common multiple of the orders of its elements (or  $\infty$ , if there is no such common multiple). The exponent of a non-torsion group is  $\infty$ .

**Exercise.** Suppose that  $G = \langle S \rangle$ . If  $G$  is abelian, then the exponent of  $G$  is the least common multiple of the orders of the elements of  $S$ . Moreover, the hypothesis of commutativity cannot be dropped.

**Exercise.** A group of exponent 2 is necessarily abelian. There exist nonabelian groups of exponent 3.

## 1g. Dihedral groups

Let  $n > 2$  be an integer and let  $D_{2n}$  be the group of symmetries of the regular  $n$ -gon. Thus  $D_{2n}$  contains rotations through integer multiples of  $2\pi/n$ , which form a cyclic subgroup of cardinality  $n$ , generated by (say) rotation  $\sigma$  through  $2\pi/n$ . In addition there are the reflections about an axis of symmetry; there are exactly  $n$  of these as well. Notice that if  $\tau$  is one such reflection, then  $\sigma^i \tau$  is also a reflection. There are no other symmetries, so  $D_{2n} = \{\sigma^1, \sigma^2, \dots, \sigma^n, \sigma^1 \tau, \dots, \sigma^n \tau\} = \{\sigma^i \tau^j \mid 0 \leq i < n, 0 \leq j \leq 1\}$ . The multiplication is determined by the following compact rules:

$$\sigma^n = 1, \tau^2 = 1, \tau \sigma \tau = \sigma^{-1}.$$

For these imply that  $\tau\sigma^n\tau = \text{Int}(\tau)(\sigma^n) = \text{Int}(\tau)(\sigma)^n = \sigma^{-n}$ , and then

$$\sigma^i\tau^j\sigma^k\tau^\ell = \begin{cases} \sigma^{i+k}\tau^\ell & \text{if } j = 0 \\ \sigma^{i-k}\tau^{1+\ell} & \text{if } j = 1 \end{cases}$$

Notice however that  $D_{2n} = \langle \tau, \sigma\tau \rangle$ , and both of these elements have order 2.

## 1h. Direct products

**Definition.** Let  $G$  and  $H$  be groups. The (external) **direct product**  $G \times H$  is the group based on the set which is the Cartesian product  $\{(g, h) \mid g \in G, h \in H\}$  and with multiplication  $(g, h)(g', h') = (gg', hh')$ .

Then  $G \times H$  has subgroups  $G_1 = \{(g, 1) \mid g \in G\}$  isomorphic to  $G$  and  $H_1 = \{(1, h) \mid h \in H\}$  isomorphic to  $H$ , every element of  $G$  is the product of an element of  $G_1$  and one of  $H_1$ , and  $g_1h_1 = h_1g_1$  for all  $g_1 \in G_1, h_1 \in H_1$ . But any nonabelianness of  $G$  and  $H$  is preserved.

Indeed if  $\{G_i \mid i \in I\}$  is a family of groups indexed by the set  $I$ , then  $\prod_{i \in I} G_i$  is the set of all functions  $f : I \rightarrow \cup G_i$  such that  $f(i) \in G_i$  for all  $i$ ; multiplication is pointwise:  $(ff')(i) = f(i)f'(i)$ . Within this is the restricted direct product, the subgroup consisting of all elements  $f$  such that  $f(i) = 1_{G_i}$  for all but finitely many  $i \in I$ .

We shall see that every finite (or even finitely generated) abelian group is isomorphic to the direct product of finitely many cyclic groups. But nothing like this is true for infinitely generated groups or for finite nonabelian groups.

A naturally occurring example of direct products is as follows:

Let  $G = \Sigma_X$  and let  $Y$  be a subset of  $X$ ,  $\emptyset \neq Y \neq X$ . Let  $G_{[Y]} = \{\sigma \in G \mid \sigma(Y) = Y\}$ . Then  $G_{[Y]} \leq G$ . Moreover, the mapping

$$G_{[Y]} \cong \Sigma_Y \times \Sigma_{X-Y}$$

via the isomorphism  $\sigma \mapsto (\sigma|_Y, \sigma|(X-Y))$ . Checking this boils down to the following evident statements: a) composition of mappings is preserved upon restriction to a subset left invariant by the mappings in question; b) every permutation of  $X$  leaving  $Y$  invariant is made up of a permutation of  $Y$  and one of  $X-Y$ , and every such pair conversely together form a permutation of  $X$ .

**Exercise.** Develop an analogue of the previous example for  $GL(V)$  and  $GL_n(k)$ .

**Exercise.** Show that  $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$ , but  $\mathbf{Z}_4 \not\cong \mathbf{Z}_2 \times \mathbf{Z}_2$ . Generalize.

## 1i. Free products

If  $G$  and  $H$  are groups then  $G \times H$  is generated by the isomorphic copies  $G_1 = \{(g, 1) \mid g \in G\}$  of  $G$  and  $H_1 = \{(1, h) \mid h \in H\}$  of  $H$ . Moreover, every element of  $G_1$  commutes with

every element of  $H_1$ . Given  $G$  and  $H$  we may similarly search for a group containing – and generated by – two subgroups which are isomorphic copies of  $G$  and  $H$ , but with no additional equations (or “relations”) holding between elements of these subgroups. The free product  $G * H$  of  $G$  and  $H$  has the desired property. To describe it let us assume for simplicity that the groups  $G$  and  $H$  are disjoint except that they share an identity element (this assumption can easily be satisfied by replacing  $H$  by a suitable isomorphic copy of itself). Then the elements of  $G * H$  are (formal) finite words  $a_1 \cdots a_n$ ,  $n \geq 0$ , in which either all the odd  $a_i$  lie in  $G - \{1\}$  and all the even  $a_i$  lie in  $H - \{1\}$ , or vice-versa. We include the “empty word” of length  $n = 0$ . Multiplication is accomplished simply by juxtaposing words and carrying out the obvious reduction to a reduced word, using the multiplication in  $G$  (or  $H$ ) if two elements of  $G$  (or  $H$ ) end up adjacent, and removing identity elements whenever they appear in this reduction process. It is clear that multiplication is well-defined, the empty word is an identity element, and that inverses exist (reverse a word and replace every letter by its inverse). It also seems clear that associativity holds, although some thought shows that there is something to check: a triple product has two possible locations for reduction, and one must show that the result of reduction is independent of the choice of location at which to begin reduction. We shall verify this in a later section.

Free products have the following important mapping property:

**Proposition.** *Let  $\phi : G \rightarrow K$  and  $\psi : H \rightarrow K$  be group homomorphisms. Then there exists a unique group homomorphism  $\chi : G * H \rightarrow K$  such that  $\chi(g) = \phi(g)$  and  $\chi(h) = \psi(h)$  for all  $g \in G$  and  $h \in H$ .*

Here we identify  $g \in G$  with the one-letter word  $g \in G * H$ , and identify  $h \in H$  with the one-letter word  $h \in G * H$ .

The proposition has a trivial proof: for a word  $a_1 a_2 \cdots a_n \in G * H$  with  $a_1 \in G$ , the only possibility is to define

$$\chi(a_1 a_2 \cdots a_n) = \chi(a_1) \chi(a_2) \cdots \chi(a_n) = \phi(a_1) \psi(a_2) \psi(a_3) \cdots;$$

then  $\chi$  is well-defined and it is easy to check that it preserves multiplication. The fact that  $\phi$  and  $\psi$  are homomorphisms comes into play when checking  $\chi(xy) = \chi(x)\chi(y)$  in the case that the juxtaposition of  $x$  and  $y$  requires reduction.

**Exercise.** *Formulate and prove a similar proposition for the direct product  $G \times H$  instead of  $G * H$ . An extra hypothesis about the homomorphisms  $\phi$  and  $\psi$  will have to be added.*

**Exercise.** *If  $G$  and  $H$  are subgroups of a group  $K$  and  $K$  is generated by them (i.e.,  $K = \langle G \cup H \rangle$ , usually written  $K = \langle G, H \rangle$ ), then there is a surjective homomorphism  $G * H \rightarrow K$ .*

**Exercise.** *Let  $\langle a \rangle$  and  $\langle b \rangle$  be groups of order 2 and 3, respectively. Show that there is an injective homomorphism*

$$\phi : \langle a \rangle * \langle b \rangle \rightarrow LF(2, \mathbf{C}) \text{ such that } \phi(a) : z \mapsto \frac{-1}{z} \text{ and } \phi(b) : z \mapsto \frac{1}{1-z}.$$

Conclude that  $\mathbf{Z}_2 * \mathbf{Z}_3$  is isomorphic to the image of  $SL_2(\mathbf{Z})$  in  $LF(2, \mathbf{C})$ . (This image is usually called  $PSL_2(\mathbf{Z})$ .)

### 1j. Cosets and Lagrange's Theorem

Let  $G$  be a group and  $H$  a subgroup of  $G$ . We define an equivalence relation  $\sim_H$  on  $G$  as follows:

$$a \sim_H b \iff a^{-1}b \in H.$$

The facts that  $1 \in H$ ,  $H$  is closed under inversion, and  $H$  is closed under multiplication translate directly into the reflexivity, symmetry and transitivity of  $\sim_H$ . (Check this!) The equivalence classes of  $G$  are called the left cosets of  $H$  in  $G$ , and the set of all left cosets of  $G$  is denoted  $G/H$ . It is a partition of  $G$ , as is the set of equivalence classes for any equivalence relation. The cardinality of  $G/H$  is the “index” of  $H$  in  $G$  and is written  $|G : H|$ . Thus by definition,  $|G : H| = |G/H|$ .

**Lemma.** *The left coset of  $H$  containing the element  $a \in G$  is the set  $aH = \{ah \mid h \in H\}$ . Moreover  $|H| = |aH|$  for any  $a \in G$ .*

**Proof.** If  $a \sim_H b$ , then  $b = a(a^{-1}b) \in aH$ . Conversely if  $b \in aH$ , then  $b = ah$  for some  $h \in H$ , and  $a^{-1}b = h$ , so  $a \sim_H b$ . Finally the mapping  $h \mapsto ah$  is a bijection between  $H$  and  $aH$ . QED

**Lagrange's Theorem.** *If  $H \leq G$ , then  $|G| = |H||G : H|$ . If  $G$  is finite, then  $|G : H| = |G|/|H|$ .*

The first statement is actually true even if  $G$  is infinite, with cardinal multiplication. In any case for  $G$  finite, it is a trivial consequence of the previous lemma.

**Corollary.** *If  $H \leq G$  and  $G$  is finite, then  $|H|$  divides  $|G|$ , and  $|G : H|$  divides  $|G|$ .*

**Corollary.** *If  $g \in G$  and  $G$  is finite, then  $|g|$  divides  $|G|$ .*

**Corollary.** *A group of prime order is cyclic.*

**Proof.** Let  $G$  have order  $p$  and choose  $g \in G$  with  $g \neq 1$ . Then  $|g| > 1$ , so  $|g| = p$  by the previous corollary, and hence  $|\langle g \rangle| = p$ . Therefore  $G = \langle g \rangle$ . QED

**Proposition.** *If  $K \leq H \leq G$ , then*

$$|G : K| = |G : H||H : K|.$$

If  $G$  is finite this is immediate from Lagrange's theorem, by which  $|G : K| = |G|/|K|$  (and similarly for the other terms). But in general it remains true and can be proved as follows. Choose a “transversal”  $T$  for  $H$  in  $G$ , that is, a subset  $T$  of  $G$  containing exactly

one element from each coset in  $G/H$ . Thus  $|T| = |G : H|$ . Similarly choose a transversal  $U$  for  $K$  in  $H$ . Then we argue that

the elements  $tu$ ,  $t \in T$ ,  $u \in U$  are all distinct and form a transversal for  $K$  in  $G$ .

Assuming this, we conclude that  $|G : K| = |T \times U| = |T||U| = |G : H||H : K|$  as desired.

To prove the displayed statement, let  $g \in G$ . Then  $gH = tH$  for some  $t \in T$  since  $T$  is a transversal. Hence  $g = th$  for some  $h \in H$ , and then  $hK = uK$  for some  $u \in U$  as  $U$  is a transversal. Therefore  $gK = thK = tuK$ . So every coset in  $G/K$  contains one of the listed elements. On the other hand if  $tuK = t'u'K$  for some  $t, t' \in T$  and  $u, u' \in U$  (for example if  $tu = t'u'$ ), then  $tH = tuH = tuKH = t'u'KH = t'u'H = t'H$ . Therefore  $t = t'$  since  $T$  is a transversal. But then  $tuK = t'u'K$  implies  $uK = u'K$ , so  $u = u'$  since  $U$  is a transversal, completing the proof.

**Exercise.** Show that if  $H \leq G$ ,  $K \leq G$  and both  $|G : H|$  and  $|G : K|$  are finite, then  $|G : H \cap K|$  is finite. (Hint. Show that if  $h, h' \in H$ , then  $h \sim_{H \cap K} h'$  if and only if  $h \sim_K h'$ .)

The definition of  $|G : H|$  may seem left-handed, but it is even-handed.

**Exercise.** If  $H \leq G$ , let  $H \backslash G$  be the set of all right cosets  $Hx$ ,  $x \in G$  (i.e. the set of equivalence classes under the relation  $a \sim b \iff ab^{-1} \in H$ ). Then  $|G/H| = |H \backslash G|$ . (Hint. Use the anti-isomorphism  $G \rightarrow G$  defined by  $x \mapsto x^{-1}$ .)

## 1k. Normal subgroups and quotients

In general if  $H \leq G$ , then the coset space  $G/H$  is **just a set** (endowed with an action of  $G$ , see the next section), but  $G/H$  **cannot be given the structure of a group in a reasonable way**<sup>†</sup>. The obvious attempt  $(xH) \cdot (yH) = (xy)H$  to define a binary operation on  $G/H$  fails to be well-defined. (Example: In  $G = \Sigma_3$ , let  $H = \langle (12) \rangle$ . Then  $(23)H \cdot (13)H = (123)H$  according to this definition and  $(132)H \cdot (13)H = (12)H$ . Unfortunately, the left sides are equal but the right sides are not:  $(23)H = (132)H$  but  $(12)H = H \neq (123)H$ .)

**Definition-Lemma.** Let  $H \leq G$ . Then  $H \triangleleft G$  ( $H$  is a normal subgroup of  $G$ ) if and only if the following equivalent conditions hold:

- a)  $Hx = xH$  for all  $x \in G$ ;
- b)  $xHx^{-1} = H$  for all  $x \in G$ ;
- c)  $xHx^{-1} \leq H$  for all  $x \in G$ .

**Proof.** a) and b) are equivalent by right multiplication by  $x^{-1}$ . Trivially b) implies c), and the converse holds by applying c) to  $x^{-1}$  in place of  $x$  and conjugating by  $x$ .

<sup>†</sup> “Reasonable” means that the mapping  $G \rightarrow G/H$ ,  $g \mapsto gH$ , should be a homomorphism.

**Example.** If  $\phi : G \rightarrow K$  is any homomorphism, then  $\ker \phi \triangleleft G$ . (By c): if  $\phi(g) = 1$  then  $\phi(xgx^{-1}) = \phi(x)\phi(x^{-1}) = 1$  for all  $x \in G$ . By a): for  $g \in G$ ,  $g^{-1}x \in H$  if and only if  $\phi(g) = \phi(x)$  if and only if  $gx^{-1} \in H$ . So  $xH = \phi^{-1}(\phi(x)) = Hx$ .)

**Theorem.** If  $H \triangleleft G$ , then the definition  $(xH) \cdot (yH) = xyH$  makes  $G/H$  a group, and the mapping  $x \mapsto xH$  is a surjective homomorphism  $\pi_H : G \rightarrow G/H$  with kernel  $H$ .

**Proof.** For any  $X, Y \subseteq G$  set  $XY = \{xy \mid x \in X, y \in Y\}$ . This is clearly a well-defined associative binary operation on the set of all subsets of  $G$ . If  $H \triangleleft G$ , then  $(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH) = (xy)H$ , which proves that the operation  $\cdot$  is well-defined. That the operation is associative,  $H$  is an identity element and  $(xH)^{-1} = x^{-1}H$  is easy to check, and the multiplicative property of  $\pi_H$  is trivial.

**Corollary.** Let  $H \leq G$ . Then  $H \triangleleft G$  if and only if there is a group  $K$  and a homomorphism  $\phi : G \rightarrow K$  such that  $\ker \phi = H$ .

**Examples.** a) Any subgroup of an abelian group is normal. b) Any subgroup of  $Z(G)$  is normal in  $G$ . c)  $\langle(123)\rangle \triangleleft \Sigma_3$ , but  $\langle(12)\rangle \not\triangleleft \Sigma_3$ . d)  $SL_n(k) = \{g \in GL_n(k) \mid \det g = 1\} \triangleleft GL_n(k)$ , since  $\det(gh) = \det(g)\det(h)$ , i.e.,  $\det : GL_n(k) \rightarrow k^\times$  is a homomorphism. Here  $k^\times$  is the group of all nonzero elements of  $k$ , under multiplication. e) If  $|G : H| = 2$ , then  $H \triangleleft G$ . (Proof: For  $x \in H$ ,  $xH = H = Hx$ . For  $x \notin H$ ,  $G = H \cup Hx = H \cup xH$  so  $xH = G - H = Hx$ .)

Warning: It is not the case that  $H \triangleleft K \triangleleft G$  implies  $H \triangleleft G$ . The group  $G = \Sigma_4$  has a normal abelian subgroup  $V$  of order 4 (consisting of 1 and the three elements  $(ab)(cd)$ ), and  $V$  has several normal subgroups  $H$  of order 2, but  $\Sigma_4$  has no normal subgroup  $H$  of order 2. (Such a subgroup would have to be contained in  $Z(\Sigma_4)$ , which is trivial.)