Algebra I

陳信睿

January, 2023

Abstract

這份筆記主要是在寒假時因爲興趣加上有很多時間可以讓我讀書，所以我決定來讀 Jacobson 所寫的 Basic Algebra 第一冊。這篇筆記的進行方式是我先閱讀該書的內容，之後把覺得重要的內容抄進來，除非必要，我會盡量用跟原作者一樣的句子來寫，一方面是這樣有助於我練習用英文寫證明，另一方面可以讓我更熟習書中的內容。(簡單來說，我就是在抄書，只是我是用打字的。)

Contents

1 Monoids and Groups

1.1 Monoids of Transformations and Abstract Monoids

Definition 1.1 (Monoid)**.** A monoid is a triple $(M, p, 1)$ in which M is a non-vacuous set, p is an associative binary composition (or product) in M, and 1 is an element of M such that $p(1, a) = a = p(a, 1)$ for all $a \in M$.

If we drop the hypothesis that p is associative we obtain a system which is sometimes called a *monad*. On the other hand, if we drop the hypothesis on 1 and so have just a set together with an associative binary composition, then we have obtain a *semigroup* (M, p). We shall now abbreviate $p(a, b)$, the product under p of a and b, to the customary ab (or $a \cdot b$). An element 1 in (M, p) such that $a1 = a = 1a$ for all $a \in M$ is called a unit in (M, p). If $1'$ is another such element then $1'1 = 1$ and $1'1 = 1'$, so $1' = 1$. Hence, if a unit exists it is unique, and so we may speak of *the* unit of (M, p).

If M is a monoid, a subset N of M is called a *submonoid* of M if N contains 1 and N is closed under the product in M, that is, $n_1n_2 \in N$ for every $n_i \in N$.

1.2 Groups of Transformations and Abstract Groups

An elements u of a monoid M is said to be *invertible* if there exists a v in M such that

$$uv = 1 = vu. \tag{1}$$

If v' also satisfies $uv' = 1 = v'u$ then $v' = (vu)v' = v(uv') = v$. Hence v satisfying (1) is unique. We call this *the inverse* of u and write $v = u^{-1}$. It is clear also that u^{-1} is invertible and $(u^{-1})^{-1} = u$. We now give the following

Definition 1.2 (Group)**.** A group G (or $(G, p, 1)$) is a monoid all of whose elements are invertible.

We shall call a submonoid of a monoid M (in particular, of a group) a *subgroup* if, regarded as a monoid, it is a group. Since the unit of a submonoid coincides with that of M it is clear that a subset G of M is a subgroup if and only if it has the following closure properies: $1 \in G$, $g_1g_2 \in G$ for every $g_i \in G$, every $g \in G$ is invertible, and $g^{-1} \in G$.

Let $U(M)$ denote the set of invertible elements of the monoid M and let $u_1, u_2 \in U(M)$. Then

$$(u_1u_2)(u_2^{-1}u_1^{-1}) = ((u_1u_2)u_2^{-1})u_1^{-1} = (u_1(u_2u_2^{-1}))u_1^{-1} = u_1u_1^{-1} = 1$$

and, similarly, $(u_2^{-1}u_1^{-1})(u_1u_2) = 1$. Hence, $u_1u_2 \in U(M)$. We saw also that if $u \in U(M)$ then $u^{-1} \in U(M)$, and clearly $1 \cdot 1 = 1$ shows that $1 \in U(M)$. Thus we see that $U(M)$ is a subgroup of M. We shall call this the *group of units* or *invertible elements of M*.

We now consider the monoid $M(S)$ of transformation of a non-vacuous set S. What is the associated group of units? It is easy to see that a trasformation is invertible if and only if it is bijective. Hence our group is just the set of bijective transformations of S with the composition as the composite of maps and the unit as the identity map. We shall call $U(M(S))$ the *symmetric group of the set* S and denote it as Sym$S$. In particular, if $S = \{1, 2, \ldots, n\}$ then we shall write S_n for Sym$S$ and call this the symmetric group on n letters. We usually call the elements of S_n *permutations* of $\{1, 2, \ldots, n\}$. Perform induction on n show the following theorem.

Theorem 1.1. *The order of S_n is $n!$.*

We shall now consider a general construction of monoids and groups out of given monoids and groups called the direct product. Let $M_1, M_2, \ldots, M_n$ be given monoids and put $M = M_1 \times M_2 \times \cdots \times M_n$. We introduce a product in M by

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$$

where $a_i, b_i \in M_i$ and put

$$1 = (1_1, 1_2, \ldots 1_n)$$

1_i, the unit of M_i. It is easy to check that M is a monoid. M is called the *direct product of $M_1 \times M_2 \times \cdots \times M_n$ of the monoids M_i*. If, In addition, each M_i is a group G_i, then $G_1 \times G_2 \times \cdots \times G_n$ is a group and is called the *direct product of the groups G_i*.

1.3 Isomorphism. Cayley's Theorem

Definition 1.3 (Isomorphism)**.** Two monoids $(M, p, 1)$ and $(M', p', 1')$ are said to be isomorphic if there exists a bijective map η of M to M' such that

$$\eta(1) = 1', \qquad \eta(xy) = \eta(x)\eta(y), \qquad x, y \in M. \tag{2}$$

The fact that M is isomorphic to M' will be indicated by $M \cong M'$. The map η satisfying the conditions (2) is called an isomorphism of M onto M'. Actually, the first condition in (2) is superfluous. For, if η satisfies the second condition, then we have $\eta(x)\eta(1) = \eta(x) = \eta(1)\eta(x)$. Since η is surjective, this shows that $\eta(1)$ acts as teh unit $1'$ in M', and since we know that the unit is unique, we have $\eta(1) = 1'$. It is clear that isomorphism is an equivalence relation. We shall now prove the result due to Cayley.

Theorem 1.2 (Cayley's Theroem for monoids and groups)**.**

1. *Any monoid is isomorphic to a monoid of transformation.*

2. *Any group is isomorphic to a transformation group.*

Proof.

1. Let $(M, p, 1)$ be a monoid. Then we shall set up an isomorphism of $(M, p, 1)$ with a monoid of transformations of the set M itself. For any $a \in M$, we define the map $a_L : x \to ax$ of M into M. We call a_L the left translation defined by a. It is easy to see that $M_L = \{a_L : a \in M\}$ is a monoid of transformation and

$$\eta : M \to M_L$$
$$a \mapsto a_L$$

   is an isomorphism.

2. Now let $(G, p, 1)$ be a group. Then, everything follows from the proof of (1) since G_L is clearly a group of transformations.

□

It should be noted that if M (or G) is finite then M_L acts in the finite set M. In particular, if $|G| = n$, then G_L is a subgroup of S_n, the symmetric group on a set of n elements. Hence we have

Corollary. Any finite group of order n is isomorphic to a subgroup of the symmetric group S_n.

1.4 Commutativity

If $ab = ba$ in M then a and b are said to *commute* and if this happens for all a and b in M then M is called a *commutative monoid.* Commutative groups are generally called *abelian groups* after Niels Hendrik Abel, a great Norwegian mathematician of the early nineteenth century.

If $a \in M$ we define the centralizer $C(a)$ —or $C_M(a)$ if we need to indicate M —as the subset of M of the elements b which commute with a. This is a submonoid of M. Also, if $M = G$ is a group then $C(a)$ is a subgroup.

It is immediate that if $\{M_\alpha\}$ is a set of submonoids of a monoid then $\cap M_\alpha$ is a submonoid. Similarly, the intersection of any set of subgroups of a group is a subgroup.

If A is a subset of M we define the *centralizer* of A as $C(A) = \bigcap_{a \in A} C(a)$. Clearly this is a submonoid and it is a subgroup if M is a group. The submonoid $C(M)$ is called the *center* of M.

1.5 Submonoids and Subgroups Generated by a Subset. Cyclic Groups

Given a subset S of a monoid M or of a group G, one often needs to consider the "smallest" submonoid of M or subgroup G containing S. What we want to have is a submonoid (or subgroup) containing the given set and contained in every submonoid (subgroup) containing this set. If such an object exists it is unique, for the stated property imply that if $H(S)$ and $H'(S)$ both satisfy the conditions then we have $H(S) \subset H'(S)$ and $H(S) \supset H'(S)$. Hence $H(S) = H'(S)$. Existence can also established immediately in the following way. Let S be a given subset of a monoid M (or a group G) and let $\{M_\alpha\}$ ($\{G_\alpha\}$) be the set of all submonoids of M (subgroup of G) which contain the set S. Form the intersection $\langle S\rangle$ of all these M_α (G_α). This is a submonoid (subgroup) since the intersection of submonoids (subgroups) is a submonoid (subgroup). Of course, $\langle S\rangle \supset S$. Moreover, if N is any submonoid of M (or subgroup of G) containing S, then N is one of the M_α (G_α). We shall call $\langle S\rangle$ the *submonoid (subgroup) generated by* S. If S is a finite set, say, $S = \{s_1, s_2, \ldots, s_r\}$, then we write $\langle s_1, s_2, \ldots, s_r\rangle$ in place of the more cumbersome $\langle\{s_1, s_2, \ldots, s_r\}\rangle$. An important situation occurs when $\langle S\rangle = M$ (or G). In this case we say that the monoid M (group G) is generated by the subset S, or S is the generators for M (or G).

We now shall show the constructive defintion of $\langle S\rangle$. We consider first the case of monoids. Since $\langle S\rangle$ is a submonoid containing S, clearly $\langle S\rangle$ contains 1 and every product of the form $s_1 s_2 \cdots s_r$ where s_i are elements of S (which need not be distinct.) Thus

$$\langle S\rangle \supset \langle S\rangle' \equiv \{1, s_1 s_2 \cdots s_r : s_i \in S\}. \tag{3}$$

Here the notation indicates that $\langle S\rangle'$ is the subset of the given monoid M consisting of 1 and every product of a finite number of elements of S. Now we claim that, in fact, $\langle S\rangle = \langle S\rangle'$. To see this we observe that $\langle S\rangle'$ contains S, since we are allowing $r = 1$ in (3). Also $\langle S\rangle'$ contains the unit, and the product of any two elements of the form $s_1 \cdots s_r$, $s_i \in S$, is again an element of this form. Hence $\langle S\rangle'$ is a submonoid of M and since $\langle S\rangle' \supset S$ we have $\langle S\rangle' \supset \langle S\rangle$. Since previously we had $\langle S\rangle \supset \langle S\rangle'$, $\langle S\rangle = \langle S\rangle'$. Thus a constructive definition of $\langle S\rangle$ is that this just the subset of M consisting of 1 and all finite products of elements of the set S.

In the group case we let $\langle S\rangle'$ be the subset of the given group G consisting of 1 and all finite products of elements of S or the inverses of elements of S. In other words,

$$\langle S\rangle \supset \langle S\rangle' \equiv \{1, s_1 s_2 \cdots s_r : s_i \text{ or } s_i^{-1} \in S\}. \tag{4}$$

It is immediate that $\langle S\rangle \supset \langle S\rangle'$, that $\langle S\rangle' \supset S$ and $\langle S\rangle'$ is a subgroup. Hence $\langle S\rangle' = \langle S\rangle$.

We now restrict our attention to groups, and we consider the simplest possible groups —those with a single generator. We have $G = \langle a\rangle$, and we call G *cyclic* with generator a. We now consider the map

$$n \mapsto a^n$$

of $\mathbb{Z}$ into $\langle a\rangle$. Since $\langle a\rangle = \{a^k\}$ this map is surjective. Also we have

$$m + n \mapsto a^{m+n} \quad \text{and} \quad 0 \mapsto 1.$$

Hence if our map is injective it will be an isomorphism. Now suppose $n \mapsto a^n$ is not an isomorphism. Then, $a^n = a^m$ for some $n \neq m$. We may assume $n > m$. Then, $a^{n-m} = a^n a^{-m} = a^m a^{-m} = 1$; so there exist positive integers p such that $a^p = 1$. Let r be the least such positive integer. Then we claim that

$$\langle a \rangle = \{1, a, a^2, \dots, a^{r-1}\} \tag{5}$$

and the elements listed in (5) are distinct, so $|\langle a \rangle| = r$. Let a^m be any element of $\langle a \rangle$. By the division algorithm for integers, we can write $m = rq + p$ where $0 \leq p < r$. Then we have $a^m = a^{rq+p} = (a^r)^q a^p = 1^q a^p = a^p$. Hence $a^m = a^p$ is one of the elements displayed in (5). Next we note that if $k \neq l$ are in the range $0, 1, \dots, r-1$, then $a^k \neq a^l$. Otherwise, taking $l > k$ we obtain $a^{l-k} = 1$ and $0 < l - k < r$ contrary to the choice of r. We now see that if $n \mapsto a^n$ is not an isomorphism, then $\langle a \rangle$ is a finite group. Accordingly, any infinite cyclic group is isomorphic to $(\mathbb{Z}, +, 0)$ and so any two infinite cyclic subgroups are isomorphic.

We shall now show next that any two finite cyclic groups of the same order are isomorphic. Suppose $\langle b \rangle$ has order r. Then, as in the case of $\langle a \rangle$, we have $\langle b \rangle = \{1, b, \dots, b^{r-1}\}$, where r is the smallest positive integer such that $b^r = 1$. We now observe that if h is any integer such that $a^h = 1$, then r is a divisor of h. We have $h = qr + s$, $0 \leq s < r$, so $1 = a^{qr+s} = (a^r)^q a^s = 1^q a^s = a^s$. Since r was the least positive integer satisfying $a^r = 1$ we must have $s = 0$ and so $h = qr$. We now claim that if m and n are any two integers such that $a^m = a^n$ then also $b^m = b^n$. For, $a^m = a^n$ gives $a^{m-n} = 1$; hence $m - n = qr$. Then $b^{m-n} = (b^r)^q = 1^q = 1$ and $b^m = b^n$. By symmetry, $b^m = b^n$ implies $a^m = a^n$. It is now clear that we have a 1-1 correspondence between $\langle a \rangle$ and $\langle b \rangle$ pairing a^n and b^n. Since $a^m a^n = a^{m+n}$ is paired with $b^{m+n} = b^m b^n$, $a^n \mapsto b^n$ is an isomorphism of $\langle a \rangle$ and $\langle b \rangle$.

Our analysis has proved the following

Theorem 1.3. *Any two cyclic groups of the same order (finite or infinite) are isomorphic.*

We can use the notion of a cyclic group to obtain a classification of the elements of any group G. If $a \in G$ we say that a is of *infinite order* or of *finite order* r according as the subgroup $\langle a \rangle$ is infinite of finite of order r. In the first case $a^m \neq 1$ for $m \neq 0$. In the second case we have $a^r = 1$ and r is the least positive integer having this property. Also, if $a^m = 1$ then m is a multiple of r. We shall denote the order of a by $o(a)$ (finite or infinite). It is clear that if $o(a) = r = st$ where s and t are positive integers then $o(a^s)$ is t. More generally, one sees easily that if $o(a) = r < \infty$ then $o(a^k)$ for any integer $k \neq 0$ is $[r, k]/k = r/(r, k)$, where as usual $[,]$ denotes the l.c.m. and $(,)$ denotes the g.c.d.

Cyclic groups are the simplest kind of groups. It is therefore not surprising that most questions on groups are easy to answer for this class. For example, one can determine all the subgroups of a cyclic group. This is generally an arduous task for most groups. We shall now prove

Theorem 1.4. *Any subgroup of a cyclic group $\langle a\rangle$ is cyclic. If $\langle a\rangle$ is infinite, the subgroups not equal to $\{1\}$ are infinite and $s \mapsto \langle a^s\rangle$ is a bijective map of $\mathbb{N}$ with the set of subgroups of $\langle a\rangle$. If $\langle a\rangle$ is finite of order r, then the order of every subgroup is a divisor of r, and for every positive divisor q of r there is one and only one subgroup of order q.*

Proof. Let H be a subgroup of $\langle a\rangle$. If $H = 1 := \{1\}$ then $H = \langle 1\rangle$. Now let $H \neq 1$. Then there exists an $n \neq 0$ in $\mathbb{Z}$ such that $a^n \in H$. Since also $a^{-n} = (a^n)^{-1} \in H$ we may assume $n > 0$. Now let s be the smallest positive integer such that $a^s \in H$. Then we claim $H = \langle a^s\rangle$. Let $a^m \in H$ and write $m = qs + t$ where $0 \leq t < s$. Then $a^t = a^m(a^s)^{-q} \in H$, and, since s was the least positive integer such that $a^s \in H$, we must have $t = 0$. Then $a^m = (a^s)^q \in \langle a^s\rangle$. Since a^m was any element of H we have $H = \langle a^s\rangle$, which proves the first statement of the theorem.

If $\langle a\rangle$ is infinite we saw that for distinct integers m and n, $a^m \neq a^n$. Hence for any positive s, the elements a^{ms}, $m = 0, \pm 1, \pm 2, \dots$ are distinct, so $\langle a^s\rangle$ is an infinite group. Moreover, s is the smallest positive integer such that $a^s \in \langle a^s\rangle$. Thus every subgroup not equal to $\{1\}$ is infinite and we have the 1-1 correspondence $s \mapsto \langle a^s\rangle$ between the set of positive integers and the set of subgroups not equal to $\{1\}$ of $\langle a\rangle$.

Now suppose $\langle a\rangle$ is of finite. order r, so $\langle a\rangle = \{1, a, \dots, a^{r-1}\}$. We have seen that if H is a subgroup not equal to $\{1\}$ of $\langle a\rangle$, then $H = \langle a^s\rangle$ where s is the smallest positive integer such that $a^s \in H$. We claim that $s \mid r$. For, writing $r = qs + t$ with $0 \leq t < s$, we have $1 = a^r = (a^s)^q a^t$, so $a^t = (a^s)^{-q} \in H$. The minimality of s then forces $t = 0$ and so $r = qs$. We can now list the elements of H as

$$\{1, a^s, \dots, a^{(q-1)s}\} \tag{6}$$

and $a^{sq} = a^r = 1$. This implies to $H = 1$ if we take $s = r$. In this way we obtain a bijective map $s \mapsto \langle a^s\rangle$ of the set of positive divisors s of r onto the set of subgroups of $\langle a\rangle$. The order of the subgroup $\langle a^s\rangle$ corresponding to s is $q = r/s$ and as s runs through the positive divisors of r, so does q. Hence the order of every subgroup is a divisor of r and for every positive $q \mid r$ we have one and only one subgroup of this order. This completes the proof. □

We note that again the subgroup of order q of the finite cyclic group $\langle a\rangle$ of order r can be displayed as in (6). There is another characterization of this subgroup which is often useful, namely:

Corollary. If $\langle a\rangle$ has order $r < \infty$, then the subgroup H of order $q \mid r$ is the set of elements $b \in \langle a\rangle$ such that $b^q = 1$.

Proof. Any element of H has the form a^{ks} where $s = r/q$. Then $(a^{ks})^q = a^{kr} = 1$. Conversely, let $b = a^m$ satisfy $b^q = 1$. Then $a^{mq} = 1$ and hence $mq = kr$. Then $m = ks$ so $b = (a^s)^k \in H$. □

After cyclic group the next simplest type of groups are the finitely generated abelian ones, (that is, abelian groups with a finite number of generators). These include the finite abelian groups. We shall determine the structure of this class of groups in Section 3, obtaining a complete classification by means of numerical invariants. Independently of the structure theory, we shall now derive a criterion for a finite abelian group to be cyclic. This result will be needed to prove an important theorem on fields (Theorem 2.18). To state our criterion we require the concept of the *exponent*, $\exp G$, of a finite group G, which we define to be the smallest positive integer e such that $x^e = 1$ for all $x \in G$.

Theorem 1.5. *Let G be a finite abelian group. Then G is cyclic if and only if* $\exp G = |G|$.

The proof will be based on two lemmas that are of independent interest.

Lemma 1. Let g and h be elements of an abelian group G having finite relatively prime orders m and n respectively (that is, $(m, n) = 1$). Then $o(gh) = mn$.

Proof. Suppose $(gh)^r = 1$. Then $k = g^r = h^{-r} \in \langle g \rangle \cap \langle h \rangle$. Then $o(k) \mid m$ and $o(k) \mid n$ and hence $o(k) = 1$. Thus $(gh)^r = 1 \implies a^r = 1 = h^r$. Then $m \mid r$ and $n \mid r$ and hence $mn = [m, n] \mid r$. On the other hand, $(gh)^{mn} = g^{mn}h^{mn} = 1$. Hence $o(gh) = mn$. □

Lemma 2. Let G be a finite abelian group, g an element of G of maximal order. Then $\exp G = o(g)$.

Proof. We have to show that $h^{O(g)} = 1$ for every $h \in G$. Write $o(g) = p_1^{e_1} \cdots p_s^{e_s}$, $o(h) = p_1^{f_1} \cdots p_s^{f_s}$, where the p_i are distinct primes and $e_i \geq 0$, $f_i \geq 0$. If $h^{o(g)} \neq 1$, then for some $f_i > e_i$ and we may assume $f_1 > e_1$. Put $g' = g^{p_1^{e1}}$, $h' = h^{p_2^{f_1} \cdots p_s^{f_s}}$. Then $o(g') = p_2^{e_2} \cdots p_s^{e_s}$ and $o(h') = p_1^{f_1}$. Hence, by Lemma 1, $o(g'h') = p_1^{f_1} p_2^{e_2} \cdots p_s^{e_s} > o(g)$. This contradicts the maximality of $o(g)$. □

We can now give the

Proof of Theorem 1.5. First suppose $G = \langle g \rangle$. Then $|G| = o(g)$ and hence $\exp G = |G|$. Conversely, let G be any finite abelian group such that $\exp G = |G|$. By Lemma 2 we have an element g such that $\exp G = o(g)$. Then $|G| = o(g) = |\langle g \rangle|$. Hence $G = \langle g \rangle$. □

1.6 Cycle Decomposition of Permutations

A permutation γ of $\{1, 2, \dots, n\}$ which permutes a sequence of elements $i_1, i_2, \dots, i_r$, $r > 1$, cyclically in the sense that

$$\gamma(i_1) = i_2, \quad \gamma(i_2) = i_3, \dots, \gamma(i_{r-1}) = i_r, \quad \gamma(i_r) = i_1, \tag{7}$$

and fixes (that is, leaves unchanged) the other numbers in $\{1, 2, \dots, n\}$ is called a *cycle* or an *r-cycle*. We denote this as

$$\gamma = (i_1 i_2 \cdots i_r). \tag{8}$$

It is clear that we can equally write

$$\gamma = (i_2 i_3 \cdots i_r i_1) = (i_3 i_4 \cdots i_r i_1 i_2), \text{ etc.}$$

The permutation γ^2 maps i_i into i_3, i_2 into i_4,..., i_r into i_2 etc., and, in general, for $1 \leq k \leq r$,

$$\begin{aligned} \gamma^k(i_j) &= i_{j+k} \qquad \text{if } j+k \leq r \\ \gamma^k(i_j) &= i_{j+k-r} \quad \text{if } j+k > r \end{aligned} \tag{9}$$

Clearly this shows that $\gamma^r = 1$ but $\gamma^k \neq 1$ if $1 \leq k < r$. Hence γ is of order r.

Two cycles γ and γ' are said to be *disjoint* if their symbols contain no common letters. In this case it is clear that any number moved by one of these transformations is fixed by the other. Hence if i is any number such that $\gamma(i) \neq i$ then $\gamma\gamma'(i) = \gamma(i)$, and since also $\gamma^2(i) \neq \gamma(i)$, $\gamma'\gamma(i) = \gamma(i)$. Similarly, if $\gamma'(i) \neq i$ then $\gamma'\gamma(i) = \gamma'(i) = \gamma\gamma'(i)$. Also if $\gamma(i) = i = \gamma'(i)$ then $\gamma\gamma'(i) = \gamma'\gamma(i)$. Thus $\gamma\gamma' = \gamma'\gamma$, that is, any two disjoint cycles commute. Let α be a product of disjoint cycles, that is,

$$\alpha = (i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s) \cdots (l_1 l_2 \cdots l_u). \tag{10}$$

Let m be the least common multiple of $r, s, \ldots, u$. Then we claim that m is the order of α. Putting $\gamma_1 = (i_1 i_2 \cdots i_r)$, $\gamma_2 = (j_1 j_2 \cdots j_s)$, $\ldots$, $\gamma_k = (l_1 l_2 \cdots l_u)$ we have $\alpha^m = \gamma_1^m \gamma_2^m \cdots \gamma_k^m = 1$. On the other hand, α permutes $i_1, \ldots, i_r$ and so do its powers and the restriction of α to $\{i_1, \ldots i_r\}$ is γ_1. Hence if $\alpha^n = 1$ then $\gamma_1^n = 1$ and so n is divisible by r. Similarly, n is divisible by $s, \ldots, u$ and so n is divisible by the least common multiple of $r, s, \ldots, u$. Hence the least common multiple of these numbers is the order of α.

It is convenient to extend the definition of cycles and the cycle notation to 1-cycles where we adopt the convention that for any i, (i) is the identity mapping. With this convention we can see that every permutation is a product of disjoint cycles.

In general, for any α we can begin with any number in $1, 2, \ldots, n$, say i_1, and form $\alpha(i_1) = i_2$, $\alpha(i_2) = i_3$, $\ldots$, until we reach a number that occurs previously in this list. The first such repetition occurs when $i_{r+1} = \alpha(i_r) = i_1$; for, we have $i_k = \alpha^{k-1}(i_1)$ and if $i_k = i_l$ for $l > k$ then $\alpha^{l-k}(i_1) = i_i$. Thus the sequence $i_1, i_2, \ldots, i_r$ is permuted cyclically by α. If $r < n$ we choose a j_1 not in $\{i_1, i_2, \ldots, i_r\}$. If $\alpha^m(j_1) = \alpha_q(i_1)$ then $j_1 = \alpha^{q-m}(i_1) \in \{i_1, i_2, \ldots, i_r\}$ contrary to our choice of j_1. Hence we obtain a new sequence of numbers $j_1, j_2, \ldots, j_s$ permuted cyclically by α and having no elements in common with the first. Continuing this way we ultimately exhaust the set $\{1, 2, \ldots, n\}$. It is clear, on comparing the images of any i under two maps α and $(l_1 l_2 \cdots l_u) \cdots (i_1 i_2 \cdots i_r)$ that

$$\alpha = (l_1 l_2 \cdots l_u) \cdots (i_1 i_2 \cdots i_r),$$

a product of disjoint cycles. The different cycles occurring in such a factorization commute and we may add or drop trivial one-cycles. Apart from order of the factors and inclusion or omission of 1-cycles this factorization is unique. For, if we have one which is essentially different from the one displayed above, then for some i, j, $i \neq j$, which occur in the order i followed by j in one of the cycles in (10), we have that this is not the case in the other one. The first factorization then shows that $\alpha(i) = j$ and the second that $\alpha(i) \neq j$. This contradiction proves our assertion.

A cycle of the form (ab) is called a *transposition*. It is easy to verify that

$$(i_1 i_2 \cdots i_r) = (i_1 i_r) \cdots (i_1 i_3)(i_1 i_2), \tag{11}$$

a product of $r-1$ transpositions. It follows that any $\alpha \in S_n$ is a product of transpositions. In fact, if α factors as a product of disjoints cycles as in (10), then α is a product of $(r-1)+(s-1)+\cdots+(u-1)$ transpositions. We denote this number, which is uniquely determined by α, as $N(\alpha)$. It is clear that $N(1) = 0$. There is no uniqueness of factorization of a permutation as a product of transpositions. However, we shall now show, there is one common feature of all the factorizations of a given α as a product of transpositions. The number of factors occurring all have the same parity: that is, their number is either always even or always odd. Our proof of this fact will be based on a simple formula, which is anyhow worth noting:

$$(ab)(ac_1 \cdots c_h b d_1 \cdots d_k) = (bd_1 \cdots d_k)(ac_1 \cdots c_h). \tag{12}$$

Here we are allowing h or k to be 0, meaning thereby that no c's or no d's occur. Comparing images of any i in $\{1, 2, \ldots, n\}$ shows that (12) holds. Since $(ab)^{-1} = (ab)$ multiplying both sides of (12) on the left by (ab) gives:

$$(ab)(bd_1 \cdots d_k)(ac_1 \cdots c_h) = (ac_1 \cdots c_h b d_1 \cdots d_k). \tag{13}$$

If N is defined as above, we have

$$N((ac_1 \cdots c_h b d_1 \cdots d_k)) = h + k + 1 \text{ and } N((bd_1 \cdots d_k)(ac_1 \cdots c_h)) = h + k.$$

It follows that $N((ab)(\alpha)) = N(\alpha) = 1$ if a and b occur in the same cycle in the decomposition of α into disjoint cycles and $N((ab)(\alpha)) = N(\alpha) + 1$ if a and b occur in different cycles. Hence if α is a product of m transpositions then, since $N(1) = 0$, $N(\alpha) = \sum_{i=1}^{m} \varepsilon_i$ where $\varepsilon_i = \pm 1$. Changing an $\varepsilon_i = -1$ to 1 amounts to adding 2 to the sum and so does not change the parity. If we make this change for every $\varepsilon_i = -1$ the final sum we obtain is m. Hence m and $N(\alpha)$ have the same parity. Hence the number of factors in any two factorizations of α as a product of transpositions have the same parity, namely, the parity of $N(\alpha)$.

We call α *even* or *odd* according as α factors as a product of an even or an odd number of transpositions. We define the *sign* of α, *sg* α, by

$$sg\ \alpha = 1 \text{ if } \alpha \text{ is even}, \quad sg\ \alpha = -1 \text{ if } \alpha \text{ is odd}. \tag{14}$$

Then $sg\ 1 = 1$ and if $\alpha = (ab)\cdots(kl)$, $\beta = (pq)\cdots(uv)$, $\alpha\beta = (ab)\cdots(kl)(pq)\cdots(uv)$. Hencd $\alpha\beta$ is even if and only if both α and β are even or both are odd while $\alpha\beta$ is odd if one of the factors is even and the other is odd. It follows that

$$sg\ \alpha\beta = (sg\ \alpha)(sg\ \beta). \tag{15}$$

It is clear also that the subset A_n of even permutations is a subgroup of S_n. This is called the *alternating group* (of degree n). Suppose we lists its elements as

$$\alpha_1, \alpha_2, \ldots, \alpha_m.$$

Then if $n \geq 2$ we have m different odd permutations

$$\alpha_1(ab), \alpha_2(ab), \ldots, \alpha_m(ab)$$

and this catches them all, since if β is odd $\beta(ab)$ is even so $\beta(ab) = \alpha_i$ for some i and $\beta = \alpha_i(ab)$. Hence $|S_n| = 2m = 2\,|A_n|$ and so $A_n = n!/2$ if $n \geq 2$.

1.7 Orbits. Cosets of a Subgroup

Let G be a group of transformations of a set S. Then G defines an equivalence relation on S by the rule that $x \sim_G y$ if $y = \alpha(x)$ for some $\alpha \in G$. That relation is reflexive, symmetric, and transitive is immediate from the definition of a transformation group: $x = 1_S(x)$, also if $y = \alpha(x)$ then $x = \alpha^{-1}(y)$, and if $y = \alpha(x)$ and $z = \beta(y)$ then $z = (\beta\alpha)(x)$. Moreover, $1_S \in G$ and α^{-1} and $\beta\alpha \in G$, if α and $\beta \in G$. The G-equivalence calss determine by an element x is the set $Gx = \{\alpha(x) : \alpha \in G\}$ and this is called the *G-orbit* of $x \in S$. It may happen that there is just one orbit, that is, $S = Gx$ for some x (and hence for every x). In this case we say that G is a *transitive* group of transformations of the set S. It is clear that S_n is transitive on $\{1, 2, \ldots, n\}$. This is true also of the alternating group A_n if $n \geq 3$. On the other hand, if $\alpha \in S_n$ and $\alpha = (i_1 \cdots i_r)(j_1 \cdots j_s) \cdots (l_1 \cdots l_u)$ is the factorization of α into disjoint cycles, where we have included the 1-cycles, and every letter in $\{1, 2, \ldots, n\}$ appears once and only once among $i_1, \ldots, i_r, j_1, \ldots, j_s, \ldots, l_1, \ldots, l_u$, then the sets

$$\{i_1, \ldots, i_r\}, \{j_1, \ldots, j_s\}, \ldots, \{l_1, \ldots, l_u\}$$

are the orbits in $\{1, 2, \ldots, n\}$ determined by the cyclic group $\langle\alpha\rangle$ of S_n. Observe that this gives another interpretation of the number $N(\alpha)$ which we used in subsection 1.6, namely, $N(\alpha) = \sum(k-1)$ where k runs over the cardinal numbers of the orbits determined by $\langle\alpha\rangle$.

Now let G be any group and let H be a subgroup of G. We recall that we have the transformation groups G_L of the left translations g_L ($x \mapsto gx$) and G_R of right translations g_R both acting in G. Since $y = gx$ and $y = xg$ are solvable for g for any given y and

x it is clear that G_L and G_R are transitive groups. Now let $H_L(G)$ denote the subset of G_L of maps h_L (in G) for $h \in H$. Since H is a subgroup of G and $g \to g \mapsto g_L$ is an isomorphism, $H_L(G)$ is a subgroup of G_L and hence $H_L(G)$ is a transformation group of the set G. What are orbits in the set G determined by $H_L(G)$? If $x \in G$ then it is clear that its $H_L(G)$-orbit is

$$Hx := \{hx : h \in H\}. \tag{16}$$

In the group literature this is sometimes called the left coset of x relative to the subgroup H and sometimes the right coset of x relative to H. The majority opinion seems to favor the second terminology. Accordingly, we shall adopt it here and call Hx the *right coset* of x relative to H. We have the partition $G = \bigcup_{x \in G} Hx$. Moreover, any two right cosets Hx and Hy have the same cardinality since the map $(x^{-1}y)_R : z \mapsto z(x^{-1}y)$ is bijective from Hx to Hy. Since $H = H1$ is one of the right cosets we have $|Hx| = |H|$.

In particular, suppose G is a finite group and $|G| = n$ and $|H| = m$. We have the partition

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_r \tag{17}$$

where we have displayed the distinct cosets,m so $Hx_i \cap Hx_j = \varnothing$ if $i \neq j$. We call the number r of these cosets the *index* of H in G and denote this as $[G : H]$. Since $|Hx_i| = m$, we have by (17) that $n = mr$. This proves a fundamental theorem which is due to Lagrange:

Theorem 1.6. *The order of a subgroup of a finite group G is a factor of the order of G. More precisely, we have $|G| = |H|\,[G : H]$.*

We also have the following

Corollary. If G is a finite group of order n, then $x^n = 1$ for every $x \in G$.

Proof. Let m be the order of $\langle x \rangle$. Then $x^m = 1$ and $n = mr$, so $x^n = 1$. □

The results on the right cosets have their counterparts for left cosets. These are the orbits in G determined by the transformation group $H_R(G)$. The orbit of x in this case is $xH := \{xh : h \in H\}$ and this is called the *left coset* of x relative to H. If Hx is a right coset the set of inverses $(hx)^{-1} = x^{-1}h^{-1}$ of the elements of Hx is the left coset $x^{-1}H$. It is immediate that the map $Hx \mapsto x^{-1}H$ is a bijective map of the set of thwe right coset onto the set of left cosets. It follows that these two sets (of left and right coset) have the same cardinal number. As in the case of finite groups, we call this the *index of H in G* and denote it as $[G : H]$.

1.8 Congruences. Quotient Monoids and Groups

Definition 1.4. Let $(M, \cdot, 1)$ be a monoid. A congruence (or congruence relation) $\equiv$ in M is an equivalence relation in M such that for any a, a', b, b' such that $a \equiv a'$ and $b \equiv b'$

one has $ab \equiv a'b'$. (In other words, congruence are equivalence relations which can be multiplied.)

Let $\equiv$ be a congruence in the monoid M and consider the quotient set $\overline{M} = M/{\equiv}$ of relative to $\equiv$. We recall that $\overline{M}$ is the subset of the power set $\mathcal{P}(M)$ consisting of equivalence classes $\overline{a} = \{b \in M : b \equiv a\}$. Since congruences can be multiplied it is clear in the general case that, if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, then $\overline{ab} = \overline{a'b'}$. Hence

$$(\overline{a}, \overline{b}) \mapsto \overline{ab}$$

is a well-defined map of $\overline{M} \times \overline{M}$ into $\overline{M}$; that is, this is a binary composition on $\overline{M}$. We denote this again as $\cdot$, and we shall now show that $(\overline{M}, \cdot, \overline{1})$ is a monoid. We note first that $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$, since the left-hand side is $\overline{ab} \cdot \overline{c} = \overline{(ab)c}$ and the right-hand side is $\overline{a} \cdot \overline{bc} = \overline{a(bc)}$. Hence $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$ follows from the associative law in M. Also $\overline{a} \cdot \overline{1} = \overline{a1} = \overline{a}$ and $\overline{1} \cdot \overline{a} = \overline{1a} = \overline{a}$ so $\overline{1}$ is unit. The monoid $(\overline{M}, \cdot, \overline{1})$ is called the *quotient monoid of M relative to the congruence $\equiv$.*

We can say a good deal more if $M = G$ is a group and $\equiv$ is a congruence on G. In the first place, in this case the quotient monoid $(\overline{G}, \cdot, \overline{1})$ is agroup since $\overline{a} \cdot \overline{a^{-1}} = \overline{1} = \overline{a^{-1}} \cdot \overline{a}$. Hence, every $\overline{a}$ is invertible and its inverse is $\overline{a^{-1}}$. Next we can determine all congruences on a group—or, more precisely, we can reduce the problem of determining the congruences to that of determining certain kinds of subgroups of the given group which we specify in the following

Definition 1.5. A subgroup K of a group G is said to be normal (sometimes called invariant, and in the older literature, self-conjugate) if

$$g^{-1}kg \in K$$

for every $g \in G$ and $k \in K$.

We have the following fundamental connection between congruences on a group G and normal subgroups of G.

Theorem 1.7. *Let G be a group and $\equiv$ a congruence on G. Then the congruence class $K = \overline{1}$ of the unit is a normal subgroup of G and for any $g \in G$, $\overline{g} = Kg = gK$, the right or the left coset of g relative to K. Conversely, let K be any normal subgroup of G, then $\equiv$ defined by:*

$$a \equiv b \pmod{K}, \ \textit{if } a^{-1}b \in K$$

is a congruence relation in G whose associated congruence classes are the left (or right) cosets gK.

Proof. Suppose first that we have a congruence $\equiv$ on G and let $K = \overline{1}$. If $k_1, k_2 \in K$, then $k_1k_2 \in K$ since $\overline{k_1k_2} = \overline{k_1} \cdot \overline{k_2} = \overline{1} \cdot \overline{1} = \overline{1}$. Also $1 \in K$ and $k_1^{-1} \in K$ since, as we showed above, $\overline{k_1^{-1}} = \overline{k_1}^{-1} = \overline{1}^{-1} = \overline{1}$. Hence K is a subgroup of G. Next let g be any element of G and consider the congruence class $\overline{g}$. If $a \in \overline{g}$ then $g^{-1}a$ and $ag^{-1} \in K$ since $\overline{g^{-1}a} = \overline{g^{-1}} \cdot \overline{a} = \overline{g}^{-1}\overline{g} = \overline{1} = K$ and, similarly, $ag^{-1} \in K$. It follows that $a \in Kg$ and $a \in gK$. Conversely, let $a \in Kg$. Then $a = kg$, $k \in K$, and $\overline{a} = \overline{k} \cdot \overline{g} = \overline{1} \cdot \overline{g} = \overline{g}$ so $a \equiv g$. The same thing holds if $a \in gK$. Thus,

$$\overline{g} = gK = Kg, \quad g \in G. \tag{18}$$

It follows that K is normal in the sense of the foregoing definition. This can be seen directly, or better still, it can be seen by observing that $gK = Kg$ for all $g \in G$ and a subgroup K is equivalent to normality. If this holds, then for any $g \in G$ and any $k \in K$, $kg \in gK$, so kg has the form gk', $k' \in K$. Then, $g^{-1}kg \in K$, so K is normal. On the other hand, if K is normal, a reversal of the steps shows that $kg \in gK$ for $k \in K$, $g \in G$. Hence $Kg \subset gK$. Replacing g be g^{-1} in the definition of normality, we obtain $Kg^{-1} \subset g^{-1}K$, which implies that $gK \subset Kg$. Hence $Kg = gK$ for every g in G.

Conversely, let K be a normal subgroup of G and define $a \equiv b \pmod{K}$ to mean $a^{-1}b \in K$. This is equivalent to saying that $b \in aK$, or that b is in the orbit of a relative to the transformation group $K_R(G)$. We showed in the last section that the relation we are considering is an equivalence relation in G for any subgroup K of G. We now proceed to show that normality of K insures that equivalences can be multiplied and hence that $a \equiv b \pmod{K}$ is a congruence. Thus let $a \equiv g \pmod{K}$ and $b \equiv h \pmod{K}$. Then $a = gk_1$, $b = hk_2$, $k_i \in K$, and since $Kh = hK$, $k_1h = hk_3$, $k_3 \in K$. Then, $ab = gk_1hk_2 = ghk_3k_2$ so $ab \equiv gh \pmod{K}$. Thus $\equiv \pmod{K}$ is a congruence relation in G. For this congruence we have $\overline{1} = \{k : 1^{-1}k \in K\} = K$ and for any g,$\overline{g} = \{a : g^{-1}a \in K\} = gK$. This completes our verification. □

We shall now write G/K for $\overline{G} = G/{\equiv} \pmod{K}$ and call this the *factor group* (or *quotient group*) of G relative to the normal subgroup K. By definition, the product in G/K is

$$(gK)(hK) = ghK, \tag{19}$$

$K = 1K$ is the unit, and the inverse of gK is $g^{-1}K$.

Every group $\neq 1$ has two normal subgroups: G and 1. G is called *simple* if these are its only normal subgroups. Equivalently, G is simple if the only congruence on G are two trivial ones: $=$, and the one in which any two elements are equivalent. It is clear from the definition that any subgroup of an abelian group is normal. It follows easily that the only simple abelian groups are the cyclic groups of prime order. We remark also that if C is the center of G then every subgroup of C is normal in G.

There is another way of looking at factor group in terms of multiplication of subsets of a group. If A and B are subsets of a group (similarly of a monoid) one defines

$$AB = \{ab : a \in A, b \in B\}.$$

With this definition of product and $1 = \{1\}$, the set of non-vacuous subsets of G is a monoid, since $(AB)C$ is the set of elements $(ab)c$ and $A(BC)$ is the set of elements $a(bc)$, $a \in A$, $b \in B$, $c \in C$. Hence, associativity follows from the associative law in G. Also $1 \cdot A = A = A \cdot 1$. It is clear that a subset H of G is a subgroup if and only if: (1) $H^2 \subset H$, (2) $1 \in H$, (3) $H^{-1} \equiv \{h^{-1} : h \in H\} \subset H$, and (1) and (2) together imply that $H^2 = H$. It is clear also that the coset Hg is the product of H and $\{g\}$. A subgroup K is normal if and only if any of the following equivalent conditions hold:

1. $g^{-1}Kg \subset K$ for all $g \in G$.

2. $g^{-1}Kg = K$ for all $g \in G$.

3. $Kg = gK$ for all $g \in G$.

In this case, the product for sets as just defined gives $(gK)(hK) = g(Kh)K = g(hK)K = ghK^2 = ghK$. Thus the product in G/K as defined by (19) coincides with the set product of gK and hK.

1.9 Homomorphisms

Definition 1.6. If M and M' are monoids, then a map η of M into M' is called a homomorphism if

$$\eta(ab) = \eta(a)\eta(b), \quad \eta(1) = 1', \quad a, b \in M.$$

If M' is a group the second condition is superfluous. For, if the first holds, we have $\eta(1) = \eta(1^2) = \eta(1)^2$ and multiplying by $\eta(1)^{-1}$ we obtain $1' = \eta(1)$. We have already encountered several instances of homomorphisms which may not be isomorphisms. One of these is the map

$$\eta_a : n \mapsto a^n$$

of the additive group of integers into any group G, determined by a fixed element $a \in G$. Since $\eta_a(n + m) = a^{n+m} = a^n a^m = \eta_a(n)\eta_a(m)$, this is a homomorphism of $(\mathbb{Z}, +,))$ into group G.

We emphasize that a homomorphism η need not be surjective or injective. If, by chance, η is surjective then we call it an *epimorphism*, and if it is injective then we call it a *monomorphism*. Of course, if it is bijective, then η is an isomorphism.

If η is a homomorphism of the monoid M into the monoid M', then induction shows that for any $a \in M$ and $k \in \mathbb{N}$, $\eta(a^k) = \eta(a)^k$. If a is invertible, application of η to $a \cdot a^{-1} = 1 = a^{-1} \cdot a$ gives $\eta(a)\eta(a^{-1}) = 1' = \eta(a^{-1})\eta(a)$. Hence $a' = \eta(a)$ is invertible in M' and $\eta(a^{-1}) = \eta(a)^{-1}$. It then follows that $\eta(a^k) = \eta(a)^k$ for all $k \in \mathbb{Z}$. Another useful result which we have to refer to frequently enough to warrant stating as a theorem is

Theorem 1.8. *Let η and ζ be homomorphisms of a monoid M (or group G) into a monoid M' and let S be a set of generators for M (for the group G). Suppose $\eta(s) = \zeta(s)$ for all $s \in S$. Then $\eta = \zeta$.*

Proof. We consider first the case of monoids and let

$$M_1 = \{a \in M : \eta(a) = \zeta(a)\}.$$

Then $1 \in M_1$ since $\zeta(1) = 1' = \zeta(1)$ and $M_1 \supset S$. Also, if $a, b \in M_1$, then $ab \in M_1$ since $\eta(ab) = \eta(a)\eta(b) = \zeta(a)\zeta(b) = \zeta(ab)$. Thus M_1 is a submonoid, and since it contains a set of generators, $M_1 = M$. Hence $\eta(a) = \zeta(a)$ for all a, ans so $\eta = \zeta$. The proof is similar in the case of a group G. In this case the argument shows that the subset $G_1 = \{a \in G : \eta(a) = \zeta(a)\}$ is a submonoid. But if $a \in G_1$, then $\eta(a^{-1}) = \eta(a)^{-1} = \zeta(a)^{-1} = \zeta(a^{-1})$. Hence $a^{-1} \in G_1$ and G_1 is a subgroup. Then $G_1 = G$ since G_1 contains a set of generators of G (as a group). □

A homomorphism of M into itself is called an *endomorphism* and an isomorphism of M to M is called an *automorphism* of M. The identity map is an automorphism. Theorem 1.8 applied to any endomorphism η and to $\zeta = 1$ shows that if η is an endomorphism of a monoid or a group and η is the identical map on a set of generators then $\eta = 1$. We remark also that if η is an endomorphism, then the set of fixed elements under η ($\eta(a) = a$) is a submonoid if M is a monoid and a subgroup if $M = G$ is a group. This is clear from the proof of Theorem 1.8.

Let $\eta : M \to M'$ and $\zeta : M' \to M''$ be homomorphisms of monoids. Then for $a, b \in M$, $\zeta\eta(ab) = \zeta(\eta(ab)) = \zeta(\eta(a)\eta(b)) = (\zeta\eta(a))(\zeta\eta(b))$. Also $\zeta\eta(1) = \zeta(1') = 1''$, the unit of M''. Hence $\zeta\eta : M \to M''$ is a homomorphism. If η is bijective then as we saw before η^{-1} is an isomorphism of M' into M. It is clear that the identity map is an automorphism. Hence the set, $\mathrm{Aut}M$, of automorphisms of a monoid is a group of transformations of the monoid. We call this the *group of automorphisms* of M. We remark also that the larger set, $\mathrm{End}M$, of endomorphism is a monoid of transformations, the *endomorphisms monoid* of M.

Let M be a monoid, $\equiv$ a congruence on M and $\overline{M}$ the quotient monoid determined by $\equiv$. Then the natural map $\nu : a \mapsto \overline{a}$ (the congruence class of a) is a homomorphism, since, $\nu(1) = \overline{1}$ is the unit of $\overline{M}$ and $\nu(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = \nu(a)\nu(b)$, by definition of the product in $\overline{M}$. We shall now derive the main result on homomorphisms of monoids and groups which we state as the

Theorem 1.9 (Fundamental Theorem of Homomorphisms of Monoids and Groups)**.** *Let η be a homomorphism of a monoid M into a monoid M'. Then the image $\eta(M)$ is a submonoid of M' and if M is a group, $\eta(M)$ is a subgroup of M'. The equivalence relation E_η determined by the map η ($aE_\eta b$ means $\eta(a) = \eta(b)$) is a congruence in M and we have* *a unique homomorphism $\overline{\eta}$ of the quotient monoid $\overline{M} = M/E_\eta$ into M' such that*

$$\eta = \overline{\eta} \circ \nu.$$

ν is an epimorphism and $\overline{\eta}$ is a monomorphism. In the case of groups, $\overline{1} = K = \eta^{-1}(1')$ is a normal subgroup of M, $\overline{M} = M/K$, ν is $a \mapsto aK$, and $\overline{\eta}$ is $aK \mapsto \eta(a)$.

Proof. Let $\eta : M \to M'$ be a homomorphism of monoids. Then $1' = \eta(1) \in \eta(M)$, and $\eta(a)\eta(b) = \eta(ab)$ shows that $\eta(M)$ is closed under the product in M'. Hence $\eta(M)$ is a submonoid. If M is a group, $\eta(a)$ is invertible with inverse $\eta(a^{-1})$, and so $\eta(M)$ is a subgroup of M'. Now consider the relation E_η in M. Suppose $a_1 E_\eta a_2$ and $b_1 \eta b_2$, which means $\eta(a_1) = \eta(a_2)$ and $\eta(b_1) = \eta(b_2)$. Then $\eta(a_1 b_1) = \eta(a_1)\eta(b_1) = \eta(a_2)\eta(b_2) = \eta(a_2 b_2)$ so $a_1 b_1 E_\eta a_2 b_2$. Thus E_η is a congruence. Our results on maps of sets (Section 0) show that we have a unique induced map $\overline{\eta}$ of $\overline{M} = M/E_\eta$ into M' such that $\eta = \overline{\eta} \circ \nu$. We have seen that ν is a homomorphism. All that remains (for the case of monoids) is to show that $\overline{\eta}$ is a homomorphism. We have $\overline{\eta}(\overline{a}) = \eta(a)$. Then $\overline{\eta}(\overline{a} \cdot \overline{b}) = \overline{\eta}(\overline{ab}) = \eta(ab) = \eta(a)\eta(b) = \overline{\eta}(\overline{a}) \cdot \overline{\eta}(\overline{b})$ and $\overline{\eta}(\overline{1}) = \eta(1) = 1'$, which is what we needed. We saw in Section 0 that ν is surjective and $\overline{\eta}$ is injective. Hence these are respectively an epimorphism and monomorphism of M and $\overline{M}$. Now suppose M and M' are groups. Since E_η is a congruence in the group M, we know that the congruence class K of 1 is a normal subgroup of M and the congruence class of any a is $Ka = aK$. By definition, the congruence class of 1 is

$$K = \{a \in M : \eta(a) = \eta(1) = 1'\},$$

that is, $K = \eta^{-1}(1')$. The rest is clear by Theorem 1.7. □

In the foregoing discussion we have derived the results on groups as consequences of results on monoids. For the latter the concepts of congruence and quotient monoid defined by a congruence are essential. On the other hand, the basic results on group homomorphisms can also be derived directly without recourse to congruences. We proceed to do this. This will help clarify the situation in the most important case of group homomorphisms.

We start from scratch and consider a homomorphism η of a group G into a group G'. Then it is immediate that the image ImG is a subgroup of G'. Next we consider $K = \eta^{-1}(1')$, which is analogous to the null space of a linear map of one vector space into the second one. Direct verification shows that K is a normal subgroup of G. We call this the *kernel* of η and denote it also as $\ker \eta$. We observe first that η is injective if and only if $\ker \eta = 1$; for, if $\ker \eta \neq 1$ then we have $b \neq 1$ in G such that $\eta(b) = 1' = \eta(1)$. On the other hand, if η is not injective then we have $a \neq b$ in G with $\eta(a) = \eta(b)0$. Then $a^{-1}b \neq 1$ and $\eta(a^{-1}b) = \eta(a)^{-1}\eta(b) = 1'$, so $\ker \eta \neq 1$.

Now let L be a normal subgroup of G contained in K. Then we can form the factor group $\overline{G} = G/L$ consisting of the cosets $aL = La$, $a \in G$, with multiplication

$(aL)(bL) = abL$ and unit $\overline{1} = L$. This definition shows that the map $\nu : a \mapsto aL$ is a homomorphism of G onto $\overline{G} = G/L$. Now suppose $aL = bL$. Then $b = al$, $l \in L$, and $\eta(b) = \eta(a)\eta(l) = \eta(a)1' = \eta(a)$ (since $L \subset \ker\eta$). Hence we have a well-defined map $\overline{\eta} : aL \mapsto \eta(a)$ of G/L into G'. Since $\overline{\eta}((aL)(bL)) = \overline{\eta}(abL) = \eta(ab) = \eta(a)\eta(b) = \overline{\eta}(aL)\overline{\eta}(bL)$, $\overline{\eta}$ is a homomorphism. We call $\overline{\eta}$ the homomorphism of $\overline{G} = G/L$ *induced* by η. If $a \in G$ then $\overline{\eta}\nu(a) = \overline{\eta}(aL) = \eta(a)$. Thus $\eta = \overline{\eta}\nu$, which means we have a commutative diagram as on the preceeding page.

Evidently $\text{Im}\overline{\eta} = \text{Im}\eta$. What is the kernel of $\overline{\eta}$? By definition, this is the set of cosets aL such that $\overline{\eta}(aL) = 1'$. Since $\overline{\eta}(aL) = \eta(a)$, the condition is $\eta(a) = 1'$. Hence $\ker\overline{\eta} = \{aL : a \in \ker\eta\} = \ker\eta/L$ (Clearly L is a normal subgroup of K.) Since a homomorphism is injective if and only if its kernel is 1, $\overline{\eta}$ is injective if and only if $L = \ker\eta$.

The facts we have listed go beyond those stated in the "Fundamental Theorem" in the replacement of $K = \ker\eta$ by any normal subgroup L of G contained in K. Now suppose $K = L$ and η is surjective. Then the homomorphism $\overline{\eta}$ of $\overline{G} = G/K$ into G' is surjective and injective, hence an isomorphism. We therefore have the

Corollary. If G is a group and η is an epimorphism of G onto the group G' with kernel K, then the induced map $\overline{\eta} : aK \mapsto \eta(a)$ is an isomorphism. Thus any homomorphic image of a group G is isomorphic to a factor group G/K by a normal subgroup K.

1.10 Subgroups of a Homomorphic Image. Two Basic Isomorphism Theorems

We shall establish a 1-1 correspondence between the set of subgroups of a homomorphic image $\overline{G}$ of a group and the set of subgroups of G containing the kernel of a given homomorphism. Since any homomorphic image is isomorphic to a factor group we may assume $\overline{G} = G/K$, K a normal subgroup of G. Then we have

Theorem 1.10 (The first Isomorphism Theorem)**.** *Let K be a normal subgroup of G, H a subgroup of G containing K. Then $\overline{H} = H/K$ is a subgroup of $\overline{G} = G/K$ and the map $H \mapsto \overline{H}$ is a bijective map of the set of subgroups of G containing K with the set of the subgroups of $\overline{G}$. $H(\supset K)$ is normal in G if and only if $\overline{H}$ is normal in $\overline{G}$. In this case,*

$$\frac{G}{H} \simeq \frac{\overline{G}}{\overline{H}} = \frac{G/K}{H/K}.$$

Proof. The fact that H/K is a subgroup of G/K is clear from the definition of G/K. Now let H_1 and H_2 be two subgroups of G containing K and suppose $H_1/K = H_2/K$. Then for any h_1 in H_1, $h_1K \in H_2/K$, so $h_1K = h_2K$ for some $h_2 \in H_2$. Then $h_2^{-1}h_1 \in K$, so $h_1 = h_2k$, $k \in K$. Since $K \subset H_2$ this shows that $h_1 \in H_2$. Thus $H_1 \subset H_2$ and, similarly, $H_2 \subset H_1$. Hence $H_1 = H_2$, and we have shown that $H \mapsto H/K$ is injective.

To see that it is surjective let $\overline{H}$ be a subgroup of $\overline{G}$, so that $\overline{H}$ is a collection of cosets. Let H be the union in G of these cosets. If $h_1, h_2 \in H$, $h_1K, h_2K \in \overline{H}$ and $h_1h_2K = (h_1K)(h_2)K \in \overline{H}$. Hence $h_1h_2 \in H$. Similarly $h_1^{-1}K = (h_1K)^{-1} \in \overline{H}$, so $h^{-1} \in H$. Hence H is a subgroup of G. Clearly $\overline{H} = H/K$. It is evident that if H is normal in G, then $\overline{H}$ is normal in $\overline{G}$. Conversely, if $\overline{H}$ is normal in $\overline{G}$, then for any $h \in H$, $g \in G$, $(g^{-1}hg)K = (gK)^{-1}(hK)(gK) = h'K$ for some $h' \in H$. It follows that $g^{-1}hg \in H$ and H is normal in G. If this condition is satisfied we can form the factor group $\overline{G}/\overline{H}$ and we have the natural homomorphism $\overline{\nu} : \overline{g} \mapsto \overline{g} \cdot \overline{H}$ of $\overline{G}$ with $\overline{G}/\overline{H}$. We also have the natural homomorphism $g \mapsto \overline{g}$ of G with $\overline{G}$. Hence we have the homomorphism $g \mapsto \overline{g} \cdot \overline{H}$ of G with $\overline{G}/\overline{H}$. The kernel is the set of $g \in G$ such that $\overline{g} \in \overline{H}$, that is, the set of g such that $gK = hK$ for some $h \in H$. This is just the subgroup H. Hence, by the fundamental theorem of homomorphisms, $gH \mapsto \overline{g} \cdot \overline{H}$ is an isomorphism of G/H with $\overline{G}/\overline{H}$. □

It is sometimes useful to state Theorem 1.10 in what appears to be a slighetly more general form, as follows:

Theorem 1.11 (The First Isomorphism Theorem $(*)$)**.** *Let η be an epimorphism of G onto G' and let Λ be the set of subgroups H of G containing $K = \ker\eta$. Then the map $H \mapsto \eta(H)$ of Λ gives a 1-1 correspondence between the set Λ and the complete set of subgroups of G'. H is normal in G if and only if $\eta(H)$ is normal in G'. In this case*

$$gH \mapsto \eta(g)\eta(H) \tag{20}$$

is an isomorphism of G/H with $G'/\eta(H)$.

This can be either be proved directly in a manner similar to the proof of Theorem 1.10, or, it can be deduced from Theorem 1.10 via the isomorphism $gK \mapsto \eta(g)$ of G/K with G'.

The isomorphism (20) is often called the *first isomorphism theorem* for groups. There is also a basic *second isomorphism theorem.* This is

Theorem 1.12 (The Second Isomorphism Theorem)**.** *Let H and K be subgroups of G, K normal in G. Then $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G containing K, $H \cap K$ is normal in H and the map*

$$hK \mapsto h(K \cap H), \quad h \in H \tag{21}$$

is an isomorphism of HK/K with $H/(K \cap H)$.

Proof. Since K is normal we have $hK = Kh$, $h \in H$. Since $HK = \bigcup_{h\in H} hK$ and $KH = \bigcup_{h\in H} Kh$, clearly $HK = KH$. Then $(HK)^2 = HKHK = H^2K^2 = HK$. Also $1 \in HK$ and if $hk \in HK$ ($h \in H$, $k \in K$) then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Hence HK is a subgroup of G. Clearly, $HK \supset 1K = K$ and K is normal in HK. We now consider the restriction $\nu' = \nu|_H$ where $\nu : g \mapsto gK$. The image of ν' is the set of cosets hK, $h \in H$. Since any coset of the form hkK, $h \in H$, $k \in K$, coincides with hK, it is clear that $\mathrm{Im}\nu'$ is HK/K. The kernel of this homomorphism is the set of $h \in H$ such that $hK = K$, the unit of HK/K. Since $hK = K$ if and only if $h \in K$, we see that $\ker \nu' = H \cap K$ and so this is a normal subgroup of H, and by the fundamental theorem of homomorphisms, $h(H \cap K) \mapsto hK$ is an isomorphism of $H/(H \cap K)$ with HK/K. The inverse is $hK \mapsto h(H \cap K)$ as given in (21). □

The proofs of the theorems in this subsection illustrate the power of the fundamental theorem. As another illustration of this and also of the use of the subgroup correspondence of Theorem 1.10, we shall now give a quick re-derivation of the results on cyclic groups. Everything will follow from the determination of the subgroups of $(\mathbb{Z}, +, 0)$ and their inclusion relations. Let K be a subgroup $\neq 0$ of $\mathbb{Z}$. Then if $n \in K$ so does $-n$; hence K contains positive integers and consequently K contains a least positive integer k. Now let n be any element of K. Then the division algorithm in $\mathbb{Z}$ permits us to write $n = qk + r$ where $0 \leq r < k$. Clearly $qk \in K$ and since $n \in K$, $r = n - qk \in K$. This forces $r = 0$, since k is the least positive integer in K. Thus we see that every element of K is a multiple of k and, of course, every multiple of k is in K. Hence $K = \mathbb{Z}k = \{mk : m \in \mathbb{Z}\}$. Conversely, it is clear that for any $k \geq 0$, $\mathbb{Z}k$ is a subgroup. This includes the subgroup 0 as $\mathbb{Z}0$. Thus the set of subgroups of $\mathbb{Z}$ are the various sets $\mathbb{Z}k$, $k \in \mathbb{N}$. Suppose $k, l \in \mathbb{N}$ and $\mathbb{Z}l \supset \mathbb{Z}k$. Then $k \in \mathbb{Z}l$ so $k = lm$ and $l \mid k$. The converse is clear. Hence

$$\mathbb{Z}l \supset \mathbb{Z}k \quad \iff \quad l \mid k. \tag{22}$$

Next we note that if $k = 0$ then $\mathbb{Z}/\mathbb{Z}k \simeq \mathbb{Z}$ and if $k > 0$ then $\mathbb{Z}/\mathbb{Z}k$ is just the set of congruence classes modulo the integer k, and these are

$$\overline{0} = \mathbb{Z}k, \quad \overline{1} = \{1 + mk : m \in \mathbb{Z}\}, \quad \ldots, \quad \overline{k-1} = \{(k-1) + mk : m \in \mathbb{Z}\}.$$

Thus the order of $\mathbb{Z}/\mathbb{Z}k$ is k. Clearly $\mathbb{Z}/\mathbb{Z}k$ is cyclic with $\overline{1}$ as generator.

Now let $G = \langle a \rangle$, so that G is cyclic group with generator a. Since $a^m a^n = a^{m+n}$ we have the epimorphism of $(\mathbb{Z}, +, 0)$ into G sending $n \mapsto a^n$. Hence $G \simeq \mathbb{Z}/\mathbb{Z}k$ for some $k \in \mathbb{N}$. If $k = 0$, $G \simeq \mathbb{Z}$ and if $k > 0$, G is finite of order k. Hence it is clear that any two cyclic groups of the same order are isomorphic.

We can also determine the subgroups of $\mathbb{Z}/\mathbb{Z}k$. If $k = 0$ we are dealing with $\mathbb{Z}$ and we have the determination which we made: the subgroups are $\mathbb{Z}l$, $l \geq 0$, and $\mathbb{Z}l$ is cyclic with generator l. If $k > 0$ it follows from Theorem 1.10 that the subgroups of $\mathbb{Z}/\mathbb{Z}k$ have the form $\mathbb{Z}l/\mathbb{Z}k$ where $l \geq 0$ and $\mathbb{Z}l \supset \mathbb{Z}k$. Then $l \mid k$, say, $k = lm$. Now $(\mathbb{Z}/\mathbb{Z}k)/(\mathbb{Z}l/\mathbb{Z}k) \simeq \mathbb{Z}/\mathbb{Z}l$ so $|\mathbb{Z}l/\mathbb{Z}k| = |\mathbb{Z}/\mathbb{Z}k|/|\mathbb{Z}/\mathbb{Z}l| = k/l = m$. It follows that the cyclic group $\mathbb{Z}/\mathbb{Z}k$ of order k has one and only one subgroup of order m for each divisors m of k. Moreover, this subgroup, $\mathbb{Z}l/\mathbb{Z}k$, is cyclic with $l + \mathbb{Z}k$ as generator.

1.11 Free Objects. Generators and Relations

The method used in the last section of studying cyclic groups by considering these as a homomorphic images of the "universal" cyclic group $(\mathbb{Z}, +, 0)$ can be generalized to obtain the structure of finitely generated abelian groups. We shall carry out this program in Section 3. At this point we sahll define these universal finitely generated abelian groups, called free abelian groups, and consider also their analogues for commutative monoids, for arbitrary monoids, and for arbitrary groups.

We construct first for any positive integer r and abelian group $\mathbb{Z}^{(r)}$ with r generators $x_1, x_2, \ldots, x_r$ such that if G is any abelian group and $a_1, a_2, \ldots, a_r$ are elements of G then there exists a unique homomorphism of $\mathbb{Z}^{(r)}$ into G sending

$$x_i \mapsto a_i, \qquad 1 \leq i \leq r.$$

Let $\mathbb{Z}^{(r)}$ be the r-fold direct power of $\mathbb{Z}$: $\mathbb{Z}^{(r)}$ is the set of r-tuples $(n_1, n_2, \ldots, n_r)$ of integers n_i with addition by components, $(m_i) + (n_i) = (m_i + n_i)$ and $0 = (0, 0, \ldots, 0)$. This is an abelian group. Put

$$x_i = (0, \ldots, 0, 1, 0, \ldots, 0) \text{ (the } i\text{-th component)}, \qquad 1 \leq i \leq r. \tag{23}$$

Then $(n_1, n_2, \ldots, n_r) = \sum_1^r n_i x_i$, so the x_i generate $\mathsf{F}^{(r)}$. Now let $a_1, a_2, \ldots, a_r$ be a sequence of r elements of any abelian group G and consider the map

$$\eta : (n_1, n_2, \ldots, n_r) \mapsto a_1^{n_1} a_2^{n_2} \cdots a_r^{n_r}. \tag{24}$$

Since the a_i commutes, we have

$$(a_1^{m_1} a_2^{m_2} \cdots a_r^{m_r})(a_1^{n_1} a_2^{n_2} \cdots a_r^{n_r}) = (a_1^{m_1+n_1} a_2^{m_2+n_2} \cdots a_r^{m_r+n_r})$$

which implies that η is a homomorphism of $\mathbb{Z}^{(r)}$ into G. Moreover,

$$\eta(x_i) = \eta(0, \ldots, 0, 1, 0, \ldots, 0) = a_i$$

and, since the x_i generate $\mathbb{Z}^{(r)}$, there is only one homomorphism of $\mathbb{Z}^{(r)}$ sending $x_i \mapsto a_i$, $1 \leq i \leq r$ (see Theorem 1.8). We shall call $\mathbb{Z}^{(r)}$ the *free abelian group with r (free) generators x_i*.

Identical considerations apply to commutative monoids. Let $\mathbb{N}^{(r)}$ be the r-fold direct power of the monoid $(\mathbb{N}, +, 0)$. This is a commutative monoid generated by the r elements x_i, as in (23). Moreover, as in the group case, if $a_1, a_2, \ldots, a_r$ are elements of a commutative monoid M, there exists a unique homomorphism of $\mathbb{N}^{(r)}$ into M such that $x_i \mapsto a_i$, $1 \leq i \leq r$. We call $\mathbb{N}^{(r)}$ thr *free commutative monoid with r (free) generators x_i*.

We shall now drop the requirement of commutativity in these considerations. We seek to construct first a monoid, then a group, generated by r elements x_i such that if a_i

are any r elements of a monoid M (group G), then there exists a unique homomorphism of the constructed monoid (group) sending $x_i \mapsto a_i$, $1 \le i \le r$.

We consider first the monoid case. Put $X^1 = X = \{x_1, x_2, \dots, x_r\}$. $X^j = X \times X \times \cdots \times X$, j times, where $j = 2, 3, \dots$. Let $FS^{(r)}$ denote the disjoint union of the sets $X^1, X^2, \dots$. The elements of $FS^{(r)}$ are "words in the alphabet X," that is, they are sequence $(x_{i_1}, x_{i_2}, \dots, x_{i_m})$, $x_{i_j} \in X$, $m = 1, 2, 3, \dots$. We introduce a multiplication in $FS^{(r)}$ by juxtaposition, that is,

$$(x_{i_1}, x_{i_2}, \dots, x_{i_m})(x_{j_1}, x_{j_2}, \dots, x_{j_n}) = (x_{i_1}, x_{i_2}, \dots, x_{i_m}, x_{j_1}, x_{j_2}, \dots, x_{j_n}) \tag{25}$$

This is clearly an associative product, but we have no unit. However, we can adjoin one and call it 1 to obtain a monoid $FM^{(r)}$. It is clear from (25) that $(x_{i_1}, x_{i_2}, \dots, x_{i_m}) = x_{i_1} \cdots x_{i_m}$; hence $FM^{(r)}$ is generated by the x_i. Now let $a_1, a_2, \dots, a_r$ be any r elements of any monoid M. Then since we have a unique way writing an element $\neq 1$ of $FM^{(r)}$ as $(x_{i_1}, x_{i_2}, \dots, x_{i_m})$,

$$\eta : 1 \mapsto 1, \qquad (x_{i_1}, x_{i_2}, \dots, x_{i_m}) \mapsto a_{i_1} \cdots a_{i_m}$$

is a well defined map of $FM^{(r)}$. It is clear from (25) that this is a homomorphism of $FM^{(r)}$ sending $x_i \mapsto a_i$, $1 \le i \le r$. Since the x_i generate $FM^{(r)}$ this is the only homomorphism having this property. We call this the *free monoid (freely) generated by the r elements x_i* (*or the monoid of words in the x_i*).

To obtain a construction of a free group we observe first that the subgroup of a group generated by a subset X coincides with the submonoid generated by the union of X and the set of inverses of the elements of X. This suggests forming the set $X \cup X'$ where X is the given set $\{x_1, x_2, \dots, x_r\}$ and X' is another set $\{x'_1, x'_2, \dots, x'_r\}$ disjoint to X and in 1-1 correspondence $x_i \leftrightarrow x'_i$ with X. Form the free monoid $FM^{(2r)}$ generated by $X \cup X'$. Now suppose G is a group, and $a_1, a_2, \dots, a_r$ is a sequence of elements of G. Then we have a unique homomorphism η of $FM^{(2r)}$ into G sending $x_i \mapsto a_i$, $x'_i \mapsto a_i^{-1}$, $1 \le i \le r$. By the fundamental theorem of homomorphisms, we obtain a congruence E_η on $FM^{(2r)}$ by specifying that $aE_\eta b$ means that $\eta(a) = \eta(b)$. Then $x_i x'_i E_\eta 1$ and $x'_i x_i E_\eta 1$. This suggests that we consider the set Γ of all the congruences $\equiv_\alpha$ on $FM^{(2r)}$ in which $x_i x'_i \equiv_\alpha 1$ and $x'_i x_i \equiv_\alpha 1$ for $1 \le i \le r$, and form their intersection $\equiv$. By definition, $a \equiv b$ means $a \equiv_\alpha b$ for every $\equiv_\alpha$. This is again a congruence and so we can form the quotient monoid $FM^{(2r)}/{\equiv}$, which we shall denote as $FG^{(r)}$. We observe that $FG^{(r)}$ is a group generated by the congruence classes $\overline{x_i}$, $1 \le i \le r$. This is clear since the congruence class $\overline{x_i}$ has the inverse $\overline{x_i}'$ in $FG^{(r)}$ and $FG^{(r)}$ is generated as monoid by the elements $\overline{x_i}$ and $\overline{x_i}'$. Again, let G be a group, $a_1, a_2, \dots, a_r$ a sequence of elements of G. We have the unique homomorphism η of $FM^{(2r)}$ such that $x_i x'_i E_\eta 1$ and $x'_i x_i E_\eta 1$. Then $a \equiv b$ on $FM^{(2r)}$ implies $aE_\eta b$ and hence we obtain a well defined map of $FG^{(r)}$ sending the element $\overline{a}$ into $\eta(a)$. This is a homomorphism of $FG^{(r)}$ mapping $\overline{x_i} \mapsto a_i$, $1 \le i \le r$. Since the $\overline{x_i}$ generate $FG^{(r)}$ this is the only homomorphism which does this.

To summarize: given the set $X = \{x_1, \ldots, x_r\}$ we have obtained a map $x_i \mapsto \overline{x_i}$ of X into a group $FG^{(r)}$ such that if G is any group and $x_i \mapsto a_i$, $1 \leq i \leq r$ is any map of X into G then we have a unique homomorphism of $FG^{(r)}$ into G, making the following diagram commutative:

$$\begin{tikzcd}
X \arrow[rr, "x_i\mapsto\overline{x_i}"] \arrow[dr, "x_i\mapsto a_i"'] & & S \arrow[dl, "\overline{x_i}\mapsto a_i"] \\
& G &
\end{tikzcd}$$

We shall now show that the map $x_i \mapsto \overline{x_i}$ is injective. We do this by taking G in the forgoing diagram to be the free abelian group $\mathbb{Z}^{(r)}$ generated by the elements $(0, \ldots, 0, 1, 0, \ldots, 0)$ and choose the arrow from X to G to be the map sending x_i to $(0, \ldots, 0, 1, 0, \ldots, 0)$ (the i-th component). Since this is injective, and injectivity of the composite $\beta\alpha$ of two maps implies injectivity of α, it follows that $x_i \mapsto \overline{x_i}$ is injective. Our last step is to identify x_i with its image $\overline{x_i}$. We can then say that $FG^{(r)}$ is generated by the x_i. Moreover, if $a_i \in G$ then we ahve a unique homomorphism of $FG^{(r)}$ into G such that $x_i \mapsto a_i$, $1 \leq i \leq r$. We call $FG^{(r)}$ *free group (freely) generated by the* r *elements* x_i.

A group G is said to be *finitely generated* if it contains a finite set of generators $\{a_i : 1 \leq i \leq r\}$. Then we have the homomorphism η of $FG^{(r)}$ sending $x_i \mapsto a_i$. Since the a_i generate G, this is an epimorphism and $G \simeq FG^{(r)}/K$ where K is the kernel of η. The normal subgroup K is called the *set of relations connecting the generators* a_i. If S is a subset of a group, we can define the *normal subgroup generated by* S to be the intersection of all normal subgroups of the group containing S. If S is a subset of $FG^{(r)}$ we say that G is *defined by the relations* S if $G \simeq FG^{(r)}/K$ where K is the normal subgroup generated by S. If S is finite, then we say that G is a *finitely generated group.*

1.12 Groups Acting on Sets

Historically, the theory of groups dealt at first only with transformation groups. The concept of an abstract group was introduced later in order to focus attention on those properties of transformation groups that concern the resultant composition only and do not refer to the set on which the transformations act. However, in geometry one is interested primarily in transformation groups, and even in the abstract theory it often pays to switch back from the abstract point of view to the concrete one of transformation groups. For one thing, the use of transformation groups provides a counting technique that plays an important role in the theory of finite groups. We have already seen one instance of this in the proof of Lagrange's theorem. We shall see other striking examples of results obtained by counting arguments in this section and the next.

It is useful to have a vehicle for passing from the abstract point of view to the concrete one of transformations. This is provided by the concept of a group acting on a set which we proceed to define. The idea is a simple one. We begin with an abstract group G and we are interested in the various “realizations” of G by groups of transformations. At first one is tempted to consider only those realizations which are “faithful” in the sense that they are isomorphisms of G with groups of transformations. Experience soon shows that it is preferable to broaden the outlook to encompass also homomorphisms of G into transformation groups.

We now consider a group G and a homomorphism T of G into Sym$S$, the group of bijective transformations of a set S. Writing the transformation corresponding to $g \in G$ as $T(g)$, the conditions on T are:

1. $T(1) = 1 = 1_S \in \mathrm{Sym}S$.
2. $T(g_1g_2) = T(g_1)T(g_2)$, $g_1 \in G$.

The first of these can be omitted if we assume, as we are doing, that every $T(g)$ is bijective. On the other hand, if we retain condition 1, then the hypothesis that $T(g)$ is bijective is redundant. For, if T is a map if the group G into the monoid $M(S)$ of transformations of S satisfying both conditions, then T is a homomorphism of G into $M(S)$. Hence the image of G is a subgroup of $M(S)$ and so this is contained in Sym$S$. It is useful to regard the image $T(g)x$ of x under the transformation $T(g)$ corresponding to g as simply a product gx of the element $g \in G$ with the element $x \in S$. Thus we obtain a map

$$(g, x) \mapsto gx \equiv T(g)x$$

of $G \times S$ into S. What are its properties? Clearly, conditions 1 and 2 imply respectively:

$$1x = x, \qquad x \in S \tag{26}$$

$$(g_1g_2)x = g_1(g_2x). \tag{27}$$

We shall now reverse the order and put the following

Definition 1.7. A group G is said to act (or operate) on the set S if there exists a map $(g, x) \mapsto gx$ of $G \times S$ into S satisfying (26) and (27).

We have seen that a homomorphism T of G into $M(S)$ defines an action of G on S simply by putting

$$gx = T(g)x.$$

Conversely, suppose G acts on S. Then we define $T(g)$ to be the map $x \mapsto gx$, $x \in S$. Then (26) and (27) imply 1 and 2 so $T : g \mapsto T(g)$ is a homomorphism of G into Sym$S$.

We shall refer to T as *the homomorphism* associated with the action and to $T(G)$ as the *associated transformation group*. If T is a monomorphism then we shall say that G

acts effectively on the set S. Also the kernel of T will be called the *kernel of the action.* Thus G acts effectively if and only if the kernel of the action is 1.

There is a natural definition definition of equivalence of actions of a fixed group G: we sat that two actions of G on S and S' respectively are *equivalent* if there exists a bijective map $x \mapsto x'$ of S onto S' such that

$$(gx)' = gx', \quad g \in G,\ x \in S. \tag{28}$$

If we denote $x \mapsto x'$ by α and the transformations $x \mapsto gx$ and $x' \mapsto gx'$ by $T(g)$ and $T'(g)$ respectively, then (28) means the same thing as

$$\alpha T(g) = T'(g)\alpha, \qquad g \in G. \tag{29}$$

In other words, for every $g \in G$ we have the commutativity of the diagram

$$\begin{tikzcd}
S \arrow[r, "T(g)"] \arrow[d, "\alpha"'] & S \arrow[d, "\alpha"] \\
S' \arrow[r, "T'(g)"'] & S'
\end{tikzcd}$$

Since α is bijective (29) can be written also as

$$T'(g) = \alpha T(g)\alpha^{-1}, \qquad g \in G. \tag{30}$$

As an example of equivalence we consider the two actions of G on itself by left and by right translations. Here the map $x \mapsto x^{-1}$ is an equivalence since $(gx)^{-1} = x^{-1}g^{-1} = g \circ x^{-1}$. The equivalence relation on a set S defined by a transformation group of S carries over to actions. If G acts on S we define $x \sim_G y$ for $x, y \in S$ to mean that $y = gx$ for some $g \in G$. Evidently this means the same thing as equivalence relative to the transformation group $T(G)$, as we defined it before. As before we obtain a partition of S into orbits, where the G-*orbit* of X is $Gx = \{gx : g \in G\}$. WE denote the quotient set consisting of these orbits by S/G.

If H is a subgroup of G then the H-orbits of the action of H on G by left (right) translations are the right (left) cosets of H. Now let G acts on itself by conjugations. In this case the orbit of $x \in G$ is ${}^{G}x = \{gxg^{-1} : g \in G\}$. This is called the *conjugacy class* of the element x. Of course, we have a partition of G into the distinct conjugacy classes. It is worth noting that ${}^{G}x$ consists of a single element, ${}^{G}x = \{x\}$, if and only if x is in the center. Thus the center is the union of the set of conjugacy classes which consist of single elements of G.

As an example of a decomposition into conjugacy classes we consider the problem of determining this decomposition for S_n. We have noted before that if $\beta \in S_n$ then $\beta(i_1 i_2 \cdots i_r)\beta^{-1} = (\beta(i_1), \beta(i_2), \ldots, \beta(i_r))$. It follows that if α is a product of cycles $\gamma_1, \gamma_2, \ldots$ as in (10) then $\beta\alpha\beta^{-1} = (\beta\gamma_1\beta^{-1})(\beta\gamma_2\beta^{-1})\cdots$. Hence if

$$\alpha = (i_1 \cdots i_r) \cdots (l_1 \cdots l_u)$$

then

$$\beta\alpha^{-1}\beta = (\beta(i_1), \ldots, \beta(i_r)) \cdots (\beta(l_1), \ldots, \beta(l_u)). \tag{31}$$

It is convenient to assume that $r \geq s \geq \cdots \geq u$ and that the decomposition into disjoint cycles displays every number in $\{1, 2, \ldots, n\}$ once and only once. In this way we can only associate with α a set of positive integers $(r, s, \ldots, u)$ satisfying

$$r \geq s \geq \cdots \geq u, \qquad r + s + \cdots + u = n. \tag{32}$$

We call such a sequence $(r, s, \ldots, u)$ a *partition of* n. It is clear from (31) that two permutations are conjugate if and only if they determine the same partition. It follows that the conjugacy class are in 1-1 correspondence with the different partitions of n.

If there is just one orbit in the action of a group G on a set S, that is, if $S = Gx$ for some $x \in S$ (and hence for every $x \in S$), then we say that G *acts transitively* on S. It is clear that the actions of G on itself by translations are transitive. More generally, if H is a subgroup, the action of G on the coset space G/H (set of left cosets) is transitive, since for any xH and yH we have $gxH = yH$ for $g = yx^{-1}$. We are now going to show that in essence these are the only transitive actions of a group G. To see this we need to introduce the *stabilizer*, Stab x, of an element $x \in S$, which we define to be the set of elements $g \in G$ such that $gx = x$. It is clear that this is a subgroup of G. For example, in the action of G on G by conjugation, Stab $x = C(x)$, the centralizer of x in G. If $y = ax$ then $gy = y$ is equivalent to $gax = ax$ and to $(a^{-1}ga)x = x$. Hence Stab $x = a^{-1}(\text{Stab } y)a$. It follows that if G acts transitively on S then all stabilizers of elements of S are conjugate: Stab $y = a(\text{Stab } x)a^{-1}$.

We shall now prove the following result, which gives an internal characterization of transitive actions.

Theorem 1.13. *Let G act transitively on S and let $H =$ Stab x for some $x \in S$. Then the action of G on S is equivalent to the action of G on the coset space G/H.*

Proof. Consider the map $\alpha : g \mapsto gx$ of G into S. This is surjective since G is transitive on S. Hence we have an induced bijective map $\overline{\alpha}$ of the quotient set $\overline{G}$ of G defined by α. We recall that $\overline{G}$ is the set of equivalence classes in G defined by $\overline{g} = \{a : \alpha(a) = \alpha(g)\} = \{a : ax = gx\}$. Now $ax = gx$ is equivalent to $g^{-1}ax = x$, that is , to $g^{-1}a \in$ Stab x. Hence $\overline{g}$ is the coset $g(\text{Stab } x)$ of Stab x and so we have the bijective map $\overline{\alpha} : g(\text{Stab } x) \mapsto gx$. It remains to see that this is an equivalence of actions. This requires verifying that if $g' \in G$ then $g'(g\text{Stab } x) \mapsto g'(gx)$ be $\overline{\alpha}$. This is clear since these are respectively $(g'g)\text{Stab } x$ and $(g'g)x$. □

From the point of view of finite groups one of the most important conclusions that can be drawn from the preceding theorem is that if G is a finite group acting transitively on a set S then $|S| = [G : \text{Stab } x]$ for any $x \in S$. This shows that $|S|$ is finite and this number is a divisor of $|G|$. More generally, we can apply this to any action of a finite group G on a finite set S. We have the partition

$$S = O_1 \cup O_2 \cup \cdots \cup O_r \tag{33}$$

where the O_i are the different orbits of elements of S under the action of G. Then G acts transitively in O_i, so if $x_i \in O_i$, then $|O_i| = [G : \text{Stab } x_i]$. Hence we have the following enumeration of the elements of S,

$$|S| = \sum [G : \text{Stab } x_i], \tag{34}$$

where the summation is taken over a set $\{x_1, x_2, \ldots, x_r\}$ of the representatives of the orbits. It is important to take note that all the terms $[G : \text{Stab } x_i]$ on the right-hand side are divisors of $|G|$. Another useful remark that is applicable to any group is

$$\text{Stab } (axa^{-1}) = a(\text{Stab } x)a^{-1} \tag{35}$$

The proof is clear.

An important special case of (34) is obtained by letting G acts on itself by conjugations. Then (34) specializes to

$$|G| = \sum [G : C(x_i)] \tag{36}$$

where $C(x_i)$ is the centralizer of x_i and $\{x_i\}$ is a set of representatives of the conjugacy classes of G. This formula is called the *class equation of the finite group* G. We can modify the formula slightly by collecting the classes consisting of the x_i such that $C(x_i) = G$. These are just the elements of the center C of G, and their classes contain a single element. Hence we have

$$|G| = |C| + \sum [G : C(y_i)] \tag{37}$$

where y_i run through a set of representative of the conjugacy classes which contain more than one element.

The type of counting of elements of a finite group given in (34) and (36) is an important tool in the study of finite groups. Some instances of this will be encountered in the text subsection when we consider the Sylow theorems. At this point we illustrate the method by using the class equation to prove

Theorem 1.14. *Any finite group G of prime power order has a center $C \neq 1$.*

Proof. The left hand side of (37) is divisible by the prime p and every term on the right hand side is a power of p. Moreover, since $C(y_i) \neq G$, $[G : C(y_i)] > 1$, so $[G : C(y_i)]$ is divisible by p. Then (37) shows that $|C|$ is divisible by p and so $C \neq 1$. □

There is a useful distinction we can make for transitive actions called primitivity and imprimitivity. This has to do with the induced action on the power set $\mathcal{S}$. We shall say that a partition $\pi(S)$ of S is *stabilized* by the action of G on S if $gA \in \pi(S)$ for every $g \in G$ and $A \in \pi(S)$. There are two partitions which trivially have this property: $\pi_1(S) = \{S\}$ and $\pi_0(S)$ consisting of the set of subsets $\{x\}$, $x \in S$. Now we shall call the action *primitive* if π_1 and π_0 are the only partitions of S stabilized by G. We have the partition of S into orbits relative to G and this partition is stabilized by G since $gA = A$ for every orbit A and every $g \in G$. If the orbits consist of single points, then G acts trivially in the sense that $gx = x$, $g \in G$, $x \in S$; if there is just one orbit then G is transitive. Hence if we have a non-trivial and intransitive action of G on S then this action is imprimitive. The interesting situation is that in which G acts transitively on a set with more than one element. In this case we have the following criterion.

Theorem 1.15. *If G acts transitively on a set S with $|S| > 1$, then G acts primitively if and only if the stabilizer,* Stab x, *of any $x \in S$ is a maximal subgroup of G, that is, there exists no subgroup H such that* Stab $x \subsetneqq H \subsetneqq G$.

Proof. We observe first that G acts imprimitively on a set S if and only if there exists a proper subset A of S with $|A| \geq 2$ such that for any $a \in G$ either $gA = A$ or $gA \cap A = \varnothing$. If this condition holds, then for any $g_1, g_2 \in G$ we have either $g_1A = g_2A$ or $g_1A \cap g_2A = \varnothing$. Let B be the complement in S of $\bigcup_{g \in G} gA$. Then $g_1B \cap g_2A = \varnothing$ for every $g_1, g_2 \in G$, which implies that $gB = B$ for every $g \in G$. It follows that the set of (distinct) subsets gA, $g \in G$, together with B constitute a non-trivial partition of S which is stabilized by G. Conversely, suppose G acts imprimitively on S so that we have a partition $\pi(S)$ that contains a proper subset A with $|A| \geq 2$ such that $\pi(S)$ is stabilized by G. Then if $g \in G$ either $gA = A$ or $gA \cap A = \varnothing$.

Now suppose Stab x for some $x \in S$ is not maximal, and let H be a subgroup such that Stab $x \subsetneqq H \subsetneqq G$. Since we are assuming that G acts transitively on S, this action is equivalent to the usual one on the coset space $G/\text{Stab } x$. Since equivalent actions are either both primitive or both imprimitive, it suffices to show that the action of G on $G/\text{Stab } x$ is primitive. Now consider the set A of cosets of the form $h \cdot \text{Stab } x$, $h \in H$. Since Stab $x \subsetneqq H \subsetneqq G$ we have $|A| \geq 2$ and A is proper subset of $G/\text{Stab } x$. If $h' \in H$ then $h'A$ is the set of cosets $h'h \cdot \text{Stab } x$, $h \in H$, and so $h'A = A$. On the other hand, if $g \notin H$, then $gh_1 \cdot \text{Stab } x \neq h_2\text{Stab } x$ for every $h_1, h_2 \in H$. Otherwise, we have $gh_1k_2 = h_2k_2$, where $h_1, h_2 \in H$, $k_1, k_2 \in \text{Stab } x$. This implies that $g = h_2k_2k_1^{-1}h_1^{-1} \in H$, contrary to our hypothesis. We now see that gA, which is the set of cosets of the form $gh \cdot \mathrm{Stab}\ x$, $h \in H$, has vacuous intersection with A if $g \notin H$. Thus $gA \cap A = \varnothing$ in this case. It follows as above that G acts imprimitively on $G/\mathrm{Stab}\ x$, hence on S.

Next assume that G is transitive but not primitive on S. Then we have a subset A of S, $A \neq S$, $|A| \geq 2$, such that for any $g \in G$, either $gA = A$ or $gA \cap A\varnothing$. Let $x \in A$ and let $H = \{h \in G : hA = A\}$. Then H is a subgroup of G and $H \supset \mathrm{Stab}\ x$ since $gx = x \implies gA \cap A \neq \varnothing \implies gA = A$. Since $A \neq S$ and G is transitive on S, there exists a $g \in G$ such that $gx \notin A$. Then $gA \neq A$ and $g \notin H$. Hence $G \neq H$. Now let $y \in A$, $y \neq x$ (existence clear since $|A| \geq 2$). Then we have a $g \in G$ such that $gx = y$. Then $(gA \cap A) \ni y$ and, consequently, $gA = A$ but $gx \neq x$. Thus $g \in H$, $g \notin \mathrm{Stab}\ x$, and so $H \neq \mathrm{Stab}\ x$. Hence $\mathrm{Stab}\ x$ is not a maximal subgroup of G. This completes the proof. □

1.13 Sylow's Theorems

We have seen that the order of a subgroup of a finite group G is a factor of $|G|$ and if G is cyclic, there is one and only one subgroup of order any giver divisor of $|G|$. A natural question is: If k divides G is there always a subgroup of G of order k? A little experimenting shows that this is not so. For example, the alternating group A_4, whose order is 12, contains no subgroup of order 6. Moreover, we shall show later (in Section 4) that A_n for $n \geq 5$ is simple, that is, contains no normal subgroup $\neq 1, A_n$. Since any subgroup of index two is normal, it follows that A_n, $n \geq 5$, contains no subgroup of order $n!/4$. The main positive result of the type we are discussing was discover by Sylow. This states that if a prime power p^k divides the order of a finite group G, then G contains a subgroup of order p^k. Sylow also proved a number of other important results on subgroups of order p^m where p^m is the highest power of p dividing $|G|$. We shall now consider these results.

We prove first

Theorem 1.16 (Sylow I)**.** *If p is a prime and p^k, $k \geq 0$, divides $|G|$ (assumed finite), then G contains a subgroup of order p^k.*

Proof. We shall prove the result by induction on $|G|$. It is clear if $|G| = 1$, and we may assume it holds for every group of order $< |G|$. We first prove a special case of the theorem (which goes back to Cauchy): if G is finite abelian and p is a prime divisor of $|G|$ then $|G|$ contains an element of order p. To prove this we take an element $a \neq 1$ in G. If the order r of a is divisible by p, say $r = pr'$ then $b = a^{r'}$ has order p. On the other hand, if the order r of a is prime to p, then the order $|G|/r$ of $G/\langle a\rangle$ is divisible by p and is less than $|G|$. Hence this factor group contains an element $b\langle a\rangle$ of order p. We claim that the order s of b is divisible by p, for we have $(b\langle a\rangle)^s = b^s\langle a\rangle = 1 = \langle a\rangle$. Hence the order p of $b\langle a\rangle$ is a divisor of s. Now since b has order divisible by p, we obtain an element of order

p as before. After this preliminary result we can quickly give the proof. We consider the class equation (37): $|G| = |C| + \sum[G : C(y_i)]$. If $p \nmid |C|$ then $p \nmid [G : C(y_i)]$ for some i. Then $p^k \mid |C(y_i)|$ and the subgroup $C(y_i)$ has order $< |G|$ since y_i is not in the center. Then, by the induction hypothesis, $C(y_i)$ contains an element of order p^k. Next suppose $p \mid |C|$. Then, by Cauchy's result, C contains an element c or order p. Now $\langle c\rangle$ is a normal subgroup of G of order p, and the order $|G|/p$ of $G/\langle c\rangle$ is divisible by p^{k-1}, Hence, by induction, $G/\langle c\rangle$ contains a subgroup of order p^{k-1}, This subgroup has the form $H/\langle c\rangle$ where H is a subgroup of G containing $\langle c\rangle$. Then

$$|H| = [H : \langle c\rangle] \cdot |\langle c\rangle| = p^{k-1} \cdot p = p^k.$$

This completes the proof. □

Let p^m be the largest power of p dividing $|G|$. Then Theorem 1.16 proves the existence of subgroups of order p^m of G. Such subgroups are called *Sylow p-subgroups* of G. The next Theorem concerns these.

Theorem 1.17 (Sylow II)**.**

1. *Any two Sylow p-subgroups of G are conjugate in G; that is, if P_1 and P_2 are Sylow p-subgroups, then there exists an $a \in G$ such that $P_2 = a \cdot P_1 \cdot a^{-1}$.*
2. *The number of Sylow p-subgroups is a divisor of the index of any Sylow p-subgroups and is $\equiv 1 \pmod{p}$.*
3. *Any subgroup of order p^k is contained in a Sylow p-subgroup.*

We shall obtain the proof by considering the action of G on the set Π of Sylow p-subgroups by conjugation. More generally, we note that if H is a subgroup of a group G and $g \in G$ then gHg^{-1} is a subgroup. It follows that we have an action of G on the set Γ of subgroups of G by conjugation: ${}^gH = gHg^{-1}$. The stabilizer of H under this action is the subgroup $N(H)$ (or $N_G(H)$) $= \{g \in G : gHg^{-1} = H\}$. This is called the *normalizer of H in G*. Evidently $H \subset N(H)$ and hence H is a normal subgroup of $N(H)$. The orbit of H under the conjugation action of G is $\{gHg^{-1} : g \in G\}$. The counting formula (34) shows that $\left|\{gHg^{-1} : g \in G\}\right| = [G : N(H)]$. If G is finite then $[G : N(H)] \mid [G : H]$ since $G \supset N(H) \supset H$ and hence $[G : H] = [G : N(H)] \cdot [N(H) : H]$.

Now let G be finite and let Π denote the set of Sylow p-subgroups of G. If $P \in \Pi$ then $gPg^{-1} \in \Pi$, so we have an action of G on Π induced by the conjugation action on Γ. We shall require the following

Lemma 3. Let P be a Sylow p-subgroup of G, H a subgroup of order p^j contained in $N(P)$. Then $H \subset P$.

Proof. Since H is a subgroup of $N(P)$ and P is a normal subgroup of $N(P)$, HP is a subgroup and $HP/P \simeq H/(H \cap P)$ (by the second isomorphism theorem). Thus HP/P is isomorphic to a factor group of H and so it has order p^k. Then $|HP| = p^k \cdot |P|$. Since P is a Sylow p-subgroup, $k = 0$, $HP = P$ and so $H \subset P$. □

Evidently P is a Sylow p-subgroup of $N(P)$. Moreover, it is clear from the foregoing lemma that P is the only Sylow p-subgroup of $N(P)$.

We are now ready to give the

Proof of Theorem 1.17. Let Π be the set of Sylow p-subgroups and let G act on Π by conjugation. Let Σ be one of the orbits under this action. Now let $P \in \Sigma$ and restrict the action of G on Σ to an action of P on Σ. Then we have a decomposition of Σ into P-orbits, one of which is $\{P\}$. Moreover, $\{P\}$ is the only P-orbit in Σ of cardinality one. For, if $\{P'\}$ is such a P-orbit then $P \subset N(P')$, so $P = P'$ since P' is the only Sylow p-subgroup of $N(P')$. Now every P-orbit has cardinality a power of p since this cardinality is a divisor of $|P|$. Hence $|\Sigma| \equiv 1 \pmod{p}$. We show next that $\Sigma = \Pi$. Otherwise, we have a $P \in \Pi$, $P \notin \Sigma$. Applying the foregoing argument to this P we see that there are no P-orbits in Σ of cardinality one. This gives $|\Sigma| \equiv 0 \pmod{p}$ contrary to $|\Sigma| \equiv 1 \pmod{p}$. Hence $\Sigma = \Pi$, which means G acts transitively on Π. Hence 1 is proved. We also have $|\Pi| \equiv 1 \pmod{p}$, which is the second assertion in 2. The first is clear also, since $|\Pi| = [G : N(P)]$. Now let H be a subgroup of G of order p^k and restrict the action of G on Π to H. Since the H-orbits have cardinality a power of p and since $|\Pi| \equiv 1 \pmod{p}$, there exists an orbit $\{P\}$ containing one element. Then $H \subset N(P)$ and so $H \subset P$, by the lemma. This proves 3. □

A lot of the time when you do math, you're stuck, but at the same time there are all these moments where you feel privileged that you get to work with it. You have this sensation of transcendence, you feel like you've been part of something really meaningful.

2018 Fields medalist Akshay Venkatesh.

許多時候，當你研究數學時會卡住，但在同一時間你會對能夠處理這個問題感到榮幸。你會有一種卓越的感覺，而且覺得正在參與一些眞正有意義的事情。

2018 年費爾茲獎得主 Akshay Venkatesh.