There is Galois theory in algebraic topology. A *covering space* of a topological space X is an ordered pair $(\widetilde{X}, p)$, where $p : \widetilde{X} \to X$ is a certain type of continuous map. The elements of the group $\mathrm{Cov}(\widetilde{X}/X)$ defined as {homeomorphisms $h : \widetilde{X} \to \widetilde{X} : ph = p$} are dual to the elements of a Galois group in the following sense. If $i : F \to E$ is the inclusion, where E/F is a Galois extension, then an automorphism σ of E lies in the Galois group if and only if $\sigma i = i$. When $\widetilde{X}$ is simply connected, then $\mathrm{Cov}(\widetilde{X}/X) \cong \pi_1(X)$, the fundamental group of X; moreover, there is a bijection between the family of all covering spaces of X and the family of all subgroups of the fundamental group.

I am awed by the genius of Galois (1811–1832). He solved one of the outstanding mathematical problems of his time, and his solution is beautiful; in so doing, he created two powerful theories, group theory and Galois theory, and his work is still influential today. And he did all of this at the age of 19; he was killed a year later.

Appendices

FROM ROTMAN'S "GALOIS THEORY"

Appendix A
Group Theory Dictionary

Abelian group. A group in which multiplication is commutative.

Alternating group A_n. The subgroup of S_n consisting of all the even permutations. It has order $\frac{1}{2}n!$.

Associativity. For all x, y, z, one has $(xy)z = x(yz)$. It follows that one does not need parentheses for any product of three or more factors.

Automorphism. An isomorphism of a group with itself.

Commutativity. For all x, y, one has $xy = yx$.

Conjugate elements. Two elements x and y in a group G are called conjugate if there exists $g \in G$ with $y = gxg^{-1}$.

Conjugate subgroups. Two subgroups H and K of a group G are called conjugate if there exists $g \in G$ with

$$K = gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

Coset of H in G. A subset of G of the form $gH = \{gh : h \in H\}$, where H is a subgroup of G and $g \in G$. All the cosets of H partition G; moreover, $gH = g'H$ if and only if $g^{-1}g' \in H$.

Cyclic group. A group G which contains an element g (called a *generator*) such that every element of G is some power of g.

Dihedral group D_{2n}. A group of order $2n$ containing an element a of order n and an element b of order 2 such that $bab = a^{-1}$.

Even permutation. A permutation that is a product of an even number of transpositions. Every r-cycle, for r odd, is an even permutation.

Factor groups. Given a normal series $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$, its factor groups are the groups G_i/G_{i+1} for $i \geq 0$.

Four group V. The subgroup of S_4 consisting of

$$1, (12)(34), (13)(24), \text{ and } (14)(23);$$

it is a normal subgroup.

Generator of a cyclic group G. An element $g \in G$ whose powers give all the elements of G; a cyclic group may have several different generators.

Group. A set G equipped with an associative multiplication such that there is a unique $e \in G$ (called the *identity* of G) with $ex = x = xe$ for all $x \in G$, and, for each $x \in G$, there is a unique $y \in G$ (called the *inverse* of x) with $yx = e = xy$. One usually denotes e by 1 and y by x^{-1}. (Some of these axioms are redundant.)

Homomorphism. A function $f : G \to H$, where G and H are groups, such that $f(xy) = f(x)f(y)$ for all $x, y \in G$. One always has $f(1) = 1$ and $f(x^{-1}) = f(x)^{-1}$.

Image. Given a homomorphism $f : G \to H$, its image $\operatorname{im} f$ is the subgroup of H consisting of all $f(x)$ for $x \in G$.

Index $[G : H]$. The number of (left) cosets of a subgroup H in G; it is equal to $|G|/|H|$ when G is finite.

Isomorphism. A homomorphism that is a bijection.

Kernel. Given a homomorphism $f : G \to H$, its kernel $\ker f$ is the (necessarily) normal subgroup of G consisting of all $x \in G$ with $f(x) = 1$. One denotes this by $H \lhd G$.

Natural map. If H is a normal subgroup of G, then the natural map is the homomorphism $\pi : G \to G/H$ defined by $\pi(x) = xH$.

Normal series of G. A sequence of subgroups

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$$

with each G_{i+1} a normal subgroup of G_i. (A subgroup G_i may not be a normal subgroup of G.)

Normal subgroup. A subgroup H of a group G such that, for all $g \in G$,

$$gHg^{-1} = \{ghg^{-1} : h \in H\} = H.$$

Order of an element $x \in G$. The least positive integer m, if any, such that $x^m = 1$; otherwise infinity.

Order $|G|$ of a group G. The number of elements in G.

p-group. A group in which every element has order some power of the prime p. If G is finite, the $|G|$ is a power of p.

Permutation. A bijection of a set to itself; all the permutations of a set X form a group under composition, denoted by S_X.

Quotient group G/H. If H is a normal subgroup of G, then G/H is the family of all cosets gH of H with multiplication defined by

$$gHg'H = gg'H;$$

the order of G/H is $[G : H]$; the identity element is $1H = H$; the inverse of gH is $g^{-1}H$.

Simple group G. A group $G \neq \{1\}$ whose only normal subgroups are $\{1\}$ and G.

Solvable group. A group having a normal series with abelian factor groups.

Subgroup H of G. A subset of G containing 1 which is closed under multiplication and inverse.

Subgroup generated by a subset X. The smallest subgroup of G containing X, denoted by $\langle X \rangle$, consists of all the products $x_1{}^a x_2{}^b \ldots x_n{}^z$, where $x_i \in X$ and the exponents $a, b, \ldots, z = \pm 1$.

Sylow p-subgroup of a finite group G. A subgroup of G of order p^n, where p^n is the highest power of p dividing $|G|$. Such subgroups always exist, and any two such are conjugate, hence isomorphic.

Symmetric group S_n. The group of all permutations of $\{1, 2, \ldots, n\}$ under composition; it has order $n!$.

Appendix B
Group Theory Used in the Text

All groups in this appendix are assumed to be finite even though several of the theorems hold (perhaps with different proofs) in the infinite case as well. Definitions of terms not defined in this appendix can be found in the dictionary, Appendix A.

Theorem G.1. *Every subgroup S of a cyclic group $G = \langle a \rangle$ is itself cyclic.*

Proof. If $S = \{1\}$, then S is cyclic with generator 1. Otherwise, let m be the least positive integer for which $a^m \in S$; we claim $S = \langle a^m \rangle$. Clearly $\langle a^m \rangle \subset S$. For the reverse inclusion, take $s = a^k \in S$. By the division algorithm, there are integers q and r with $0 \leq r < m$ and

$$k = qm + r.$$

But $a^k = a^{qm+r} = (a^m)^q a^r$ gives $a^r \in S$. If $r > 0$, the minimality of m is contradicted; therefore $r = 0$ and $a^k = (a^m)^q \in \langle a^m \rangle$. •

Theorem G.2. (i) *If $a \in G$ is an element of order n, then $a^m = 1$ if and only if $n \mid m$.*

(ii) *If $G = \langle a \rangle$ is a cyclic group of order n, then a^k is a generator of G if and only if $(k, n) = 1$.*

(iii) *If $a \in G$ has order n, then the order of a is $|\langle a \rangle|$.*

Proof. (i) Assume that $a^m = 1$. The division algorithm provides integers q and r with $m = nq + r$, when $0 \leq r < n$. It follows that $a^r = a^{m-nq} = a^m a^{-nq} = 1$. If $r > 0$, then we contradict n being the smallest positive integer with $a^n = 1$. Hence $r = 0$ and $n \mid m$. Conversely, if $m = nk$, then $a^m = a^{nk} = (a^n)^k = 1^k = 1$.

(ii) Recall that two integers are *relatively prime* if and only if some integral linear combination of them is 1.

If a^k generates G, then $a \in \langle a^k \rangle$, so that $a = a^{kt}$ for some $t \in \mathbb{Z}$. Therefore $a^{kt-1} = 1$; by (i), $n \mid kt - 1$, so there is $v \in \mathbb{Z}$ with $nv = kt - 1$. Therefore, 1 is a linear combination of k and m, and so $(k, n) = 1$.

Conversely, if $(k, n) = 1$, then $nt + ku = 1$ for $t, u \in \mathbb{Z}$; hence

$$a = a^{nt+ku} = a^{nt} a^{ku} = a^{ku} \in \langle a^k \rangle.$$

Therefore every power of a also lies in $\langle a^k \rangle$ and $G = \langle a^k \rangle$.

(iii) The list $1, a, a^2, \ldots, a^{n-1}$ has no repetitions: if there are $i < j$ with $a^i = a^j$, then $a^{j-i} = 1$, contradicting n being the smallest exponent for which $a^n = 1$. Now $\{1, a, a^2, \ldots, a^{n-1}\} \subset \langle a \rangle$, and we let the reader prove the reverse inclusion. It follows that $|\langle a \rangle| = |\{1, a, a^2, \ldots, a^{n-1}\}| = n$. •

Theorem G.3 (Lagrange). *If H is a subgroup of a group G, then*

$$|G| = [G : H]|H|.$$

Proof. The relation on G, defined by $x \sim y$ if $y = xh$ for some $h \in H$, is an equivalence relation whose equivalence classes are the cosets of H. Therefore, the cosets of H in G partition G. Moreover $|H| = |xH|$ for every $x \in G$ (because $h \mapsto xh$ is a bijection), so that $|G|$ is the number of cosets times their common size. •

It follows that $[G : H] = |G|/|H|$. In particular, if H is a normal subgroup of a group G (so that the quotient group G/H is defined), then

$$|G/H| = [G : H] = |G|/|H|$$

when G is finite.

Another consequence of Lagrange's theorem is that the order of $a \in G$ is a divisor of $|G|$, for Theorem G.2 shows that the order of a is the order of the subgroup $\langle a \rangle$. Hence, $a^{|G|} = 1$ for all $a \in G$.

If $f : G \to H$ is a homomorphism, denote the image of f by $\operatorname{im} f$ and the kernel of f by $\ker f$.

Lemma G.4. *Let $f : G \to H$ be a homomorphism. Then f is an injection if and only if $\ker f = \{1\}$.*

Proof. If f is an injection, then $x \neq 1$ implies $f(x) \neq f(1) = 1$, and so $x \notin \ker f$. Conversely, assume $\ker f = \{1\}$ and that $f(x) = f(y)$ for $x, y \in G$. Then

$$1 = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

and $xy^{-1} \in \ker f = \{1\}$. Hence $x = y$ and f is an injection. •

Theorem G.5 (First Isomorphism Theorem). *If $f : G \to H$ is a homomorphism, then* ker f *is a normal subgroup of G and*

$$G/\ker f \cong \operatorname{im} f.$$

Proof. Let $K = \ker f$. Let us show K is a subgroup. It does contain 1 (because $f(1) = 1$); if $x, y \in K$ (so that $f(x) = 1 = f(y)$), then $f(xy) = f(x)f(y) = 1$ and $xy \in K$; if $x \in K$, then $f(x^{-1}) = f(x)^{-1} = 1$ and $x^{-1} \in K$. Furthermore, the subgroup K is normal: if $x \in K$ and $g \in G$, then $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1} = 1$ and so $gxg^{-1} \in K$.

Define $\varphi : G/K \to \operatorname{im} f$ by $\varphi(xK) = f(x)$. Now φ is well defined: if $x'K = xK$, then $x' = xk$ for some $k \in K$, and $f(x') = f(xk) = f(x)f(k) = f(x)$. It is routine to check that φ is a homomorphism (because f is) with $\operatorname{im}\varphi = \operatorname{im} f$. Finally, φ is an injection, by Lemma G.4, because $\varphi(xK) = 1$ implies $f(x) = 1$, hence $x \in K$ and $xK = K$. •

If K, H are subgroups of G, then $K \vee H$ is the smallest subgroup of G containing K and H; that is, $K \vee H$ is the subgroup of G generated by $K \cup H$.

Lemma G.6. *If K and H are subgroups of G with K normal in G, then $K \vee H = KH = \{kh : k \in K \text{ and } h \in H\} = HK$.*

Proof. Clearly $KH \subset K \vee H$. For the reverse inclusion, it suffices to prove that KH is a subgroup, for it does contain $K \cup H$.

Now $khk_1h_1 = k(hk_1h^{-1})hh_1 = (kk_2)(hh_1) \in KH$ for some $k_2 \in K$ (because K is normal). Also $(kh)^{-1} = h^{-1}k^{-1} = (h^{-1}k^{-1}h)h^{-1} = k'h^{-1} \in KH$ for some $k' \in K$ (again, because K is normal). Therefore, KH is a subgroup.

If $hk \in HK$, then $hk = (hkh^{-1})h = k'h \in KH$ for some $k' \in K$, and so $HK \subset KH$; the reverse inclusion is proved similarly. •

If K and H are subgroups of G with K normal, then the family of those cosets hK of K with $h \in H$ is easily seen to be a subgroup of G/K. Indeed, one may check, using Lemma G.6, that this subgroup is KH/K.

Theorem G.7 (Second Isomorphism Theorem). *If K and H are subgroups of G with K normal in G, then $K \cap H$ is a normal subgroup of H and*

$$H/(K \cap H) \cong KH/K.$$

Proof. Let $\pi : G \to G/K$ be the natural map, defined by $\pi(x) = xK$, and let $f : H \to G/K$ be the restriction $\pi \mid H$. Now $\ker f = K \cap H$ and $\operatorname{im} f$ is the family of all cosets xK in G/K with $x \in H$ (hence $\operatorname{im} f = KH/K$). The first isomorphism theorem now gives the result. •

Theorem G.8 (Third Isomorphism Theorem). *If $S \subset K$ are normal subgroups of G, then K/S is a normal subgroup of G/S and*

$$(G/S)/(K/S) \cong G/K.$$

Proof. The function $f : G/S \to G/K$ given by $xS \mapsto xK$ is well defined because $S \subset K$. One checks easily that f is a surjective homomorphism with kernel K/S, and so the theorem follows from the first isomorphism theorem. •

Theorem G.9 (Correspondence Theorem). *Let K be a normal subgroup of G, and let S^* be a subgroup of $G^* = G/K$.*

(i) *There is a unique intermediate subgroup S, i.e., $K \subset S \subset G$, with $S/K = S^*$;*

(ii) *If S^* is a normal subgroup of G^*, then S is normal in G;*

(iii) $[G^* : S^*] = [G : S]$;

(iv) *If T^* is normal in S^*, then T is normal in S and*

$$S^*/T^* \cong S/T.$$

Proof. (i) Define $S = \{x \in G : xK \in S^*\}$.

(ii) If $a \in G$, and $x \in S$, then $axa^{-1}K = aKxKa^{-1}K \in S^*$, because S^* is normal in G^*; therefore $axa^{-1} \in S$.

(iii)

$$\begin{aligned}[G^* : S^*] &= |G^*|/|S^*| = |G/K|/|S/K| \\ &= (|G|/|K|)/(|S|/|K|) = |G|/|S| = [G : S].\end{aligned}$$

(iv) T is normal in S, by (ii), and

$$S^*/T^* = (S/K)/(T/K) \cong S/T,$$

by the third isomorphism theorem. •

Definition. A group G ***acts*** on a set X if there is a function

$$G \times X \to X,$$

denoted by $(g, x) \mapsto g \cdot x$, such that:

(i) $1 \cdot x = x$ for all $x \in X$, where 1 is the identity in G;

(ii) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $x \in X$ and for all $g, h \in G$.

Definition. If G acts on X and $x \in X$, then the ***orbit*** of x is

$$\mathcal{O}(x) = \{g \cdot x : g \in G\} \subset X,$$

and the ***stabilizer*** of x is the subgroup

$$G_x = \{g \in G : g \cdot x = x\} \subset G.$$

A group G acts ***transitively*** on X if, for each x, $y \in X$, there exists $g \in G$ with $g \cdot x = y$. In this case, $\mathcal{O}(x) = X$.

Every group G acts on itself (here $X = G$) by conjugation: define

$$g \cdot x = gxg^{-1}.$$

The orbit $\mathcal{O}(x)$ of $x \in G$ is its ***conjugacy class***:

$$\{y \in G : y = gxg^{-1} \quad \text{for some } g \in G\};$$

the stabilizer of x is

$$\{g \in G : x = g \cdot x = gxg^{-1}\} = \{g \in G : gx = xg\}$$

(this last subgroup, called the ***centralizer*** of x in G, is denoted by $C_G(x)$).

The reader may check that the family of all orbits partitions X, for the relation $x \sim y$ on X, defined by $y = g \cdot x$ for some $g \in G$, is an equivalence relation on X whose equivalence classes are the orbits.

Theorem G.10. *If G acts on a set X and if $x \in X$, then*

$$|\mathcal{O}(x)| = [G : G_x] = |G|/|G_x|.$$

In particular, if G acts transitively on X, where $|X| = n$, then

$$|G| = n|G_x|.$$

Proof. Define $\varphi : \mathcal{O}(x) \to$ {the family of all cosets of G_x in G} by

$$\varphi(g \cdot x) = gG_x.$$

Now φ is well defined, for if $g \cdot x = h \cdot x$ (where $g, h \in G$), then $h^{-1}g \cdot x = x$, $h^{-1}g \in G_x$, and $gG_x = hG_x$. Reversing this argument shows that φ is an injection: if $\varphi(g \cdot x) = \varphi(h \cdot x)$, then $gG_x = hG_x$, $h^{-1}g \in G_x$, and $g \cdot x = h \cdot x$. Finally, φ is surjective, for a coset gG_x is $\varphi(g \cdot x)$. Hence, φ is a bijection.

If G acts transitively, then $\mathcal{O}(x) = X$ and $|\mathcal{O}(x)| = n = |X|$; hence $n = [G : G_x] = |G|/|G_x|$, and $|G| = n|G_x|$. •

Corollary G.11. *If $x \in G$, then*

$$\textit{the number of conjugates of } x = [G : C_G(x)].$$

Proof. This is the special case of G acting on itself by conjugation. •

Lemma G.12. *If p is a prime not dividing m ($p \nmid m$) and if $k \geq 1$, then*

$$p \nmid \binom{p^k m}{p^k}.$$

Proof. Write the binomial coefficient as follows:

$$\binom{p^k m}{p^k} = \frac{p^k m(p^k m - 1) \cdots (p^k m - i) \cdots (p^k m - p^k + 1)}{p^k(p^k - 1) \cdots (p^k - i) \cdots (p^k - p^k + 1)}.$$

By Euclid's lemma, any factor p of the numerator (or of the denominator) arises from a factor of $p^k m - i$ (or of $p^k - i$). If $(m, p) = 1$ and $1 \leq i < p^k$, then $p^t \mid mp^k - i$ if and only if $p^t \mid i$. Therefore, the highest power of p dividing $p^k m - i$ is the same as the highest power of p dividing $p^k - i$ (because $p \nmid m$). Every factor of p upstairs is thus canceled by a factor of p downstairs, and hence the binomial coefficient has no factor p. •

Theorem G.13 (Sylow). *If G is a group of order $p^k m$, where p is a prime not dividing m, then G contains a subgroup of order p^k.*

Proof. (Wielandt) If X is the family of all subsets of G of cardinality p^k, then Lemma G.12 shows that $p \nmid |X|$. Let G act on X by left translation: if $B \subset G$ and $|B| = p^k$, then

$$g \cdot B = \{gb : b \in B\}.$$

There is some orbit $\mathcal{O}(B)$ with $p \nmid |\mathcal{O}(B)|$ (otherwise p divides the cardinality of every orbit, hence p divides $|X|$). Choose such a subset $B \in X$. Now $|G|/|G_B| = [G : G_B] = |\mathcal{O}(B)|$ is prime to p; it follows that $|G_B| = p^k m' \geq p^k$ for some $m' \mid m$. On the other hand, if $b_0 \in B$ and $g \in G_B$, then $gb_0 \in g \cdot B = B$ (definition of stabilizer); moreover, if g and h are distinct elements of G_B, then gb_0 and hb_0 are distinct elements of B. Therefore $|G_B| \leq |B| = p^k$, and so G_B is a subgroup of order p^k. •

Definition. If $|G| = p^k m$, where p is a prime not dividing m, then a subgroup of G of order p^k is called a ***Sylow p-subgroup*** of G.

One knows that any two Sylow p-subgroups of a group G are isomorphic (indeed, they are conjugate), and that there are exactly $1 + rp$ of them for some integer $r \geq 0$.

Corollary G.14 (Cauchy). *If p is a prime dividing $|G|$, then G contains an element of order p.*

Proof. Let H be a Sylow p-subgroup of G and choose $x \in H^\# = H - \{1\}$. By Lagrange's theorem, the order of x is p^t for some t. If $t = 1$, we are done; if $t > 1$, then it is easy to see that $x^{p^{t-1}}$ has order p. •

Lemma G.15. *Every finite abelian group $G \neq \{1\}$ contains a subgroup of prime index.*

Proof. We first prove that if G has composite order rs, then G has a proper subgroup. Choose $x \in G$ with $x \neq 1$. If x has order $< rs$, then $\langle x \rangle$ is a proper subgroup; otherwise, x has order rs and $\langle x^r \rangle$ is a proper subgroup.

The proof of the lemma is by induction on the number k of (not necessarily distinct) prime factors of $|G|$. If $k = 1$, then G has prime order and $\{1\}$ has prime index. If $k > 1$, the first paragraph gives a proper subgroup H, necessarily normal (because G is abelian), and so the quotient group G/H is defined. By induction, G/H has a subgroup S^* of prime index, and the correspondence theorem gives a subgroup S of G of prime index. •

Theorem G.16. *A group $G \neq \{1\}$ is solvable (it has a normal series with abelian factor groups) if and only if G has a normal series with factor groups of prime order.*

Proof. Sufficiency is obvious; we prove necessity by induction on $|G|$. Assume that

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

is a normal series with G_i/G_{i+1} abelian for all i; we may further assume that $G \neq G_1$. By Lemma G.15, the abelian group G/G_1 has a (necessarily normal) subgroup S^* of prime index; the correspondence theorem gives an intermediate subgroup S ($G \supset S \supset G_1$) with S normal in G and with $[G : S] = [G/G_1 : S^*]$ prime. Now S is a solvable group (consider the normal series

$$S \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\};$$

S/G_1 is abelian because it is a subgroup of the abelian group G/G_1), and induction provides a normal series of it with factor groups of prime order. •

Corollary G.17. *Every solvable group has a normal subgroup of prime index.*

Recall that the ***commutator*** of elements $x, y \in G$ is

$$[x, y] = xyx^{-1}y^{-1}.$$

The ***commutator subgroup*** G' of G is the subgroup generated by all the commutators (the product of two commutators may not be a commutator). Note that G' is a normal subgroup of G, for if $a \in G$, then

$$a[x, y]a^{-1} = [axa^{-1}, aya^{-1}];$$

moreover, G/G' is abelian.

Lemma G.18. *If H is a normal subgroup of G, then G/H is abelian if and only if $G' \subset H$.*

Proof. If G/H is abelian, then for all $x, y \in G$,

$$xyH = xHyH = yHxH = yxH,$$

and so $xyx^{-1}y^{-1} \in H$; it follows that $G' \subset H$ because every generator of G' lies in H. Conversely, if $G' \subset H$, then the third isomorphism theorem shows that G/H is a quotient group of the abelian group G/G', and hence it is abelian. •

Definition. The ***higher commutator subgroups*** are defined inductively:

$$G^{(0)} = G; \qquad G^{(i+1)} = G^{(i)\prime};$$

that is, $G^{(i+1)}$ is the commutator subgroup of $G^{(i)}$.

Lemma G.19. *A group G is solvable if and only if $G^{(n)} = \{1\}$ for some n.*

Proof. If G is solvable, then there is a normal series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

with each factor group G_i/G_{i+1} abelian. We prove, by induction on i, that $G_i \supset G^{(i)}$; this will give the result. If $i = 0$, then $G_i = G_0 = G$. Assume, by induction, that $G_i \supset G^{(i)}$; then $G_i' \supset G^{(i)\prime} = G^{(i+1)}$. But G_i/G_{i+1} abelian implies $G_{i+1} \supset G_i'$, by Lemma G.18, and so $G_{i+1} \supset G^{(i+1)}$.

Conversely, if $G^{(n)} = \{1\}$ (of course, $G^{(1)} = G'$), then

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} = \{1\}$$

is a normal series with abelian factor groups; hence G is solvable. •

Theorem G.20. *If G is a solvable group, then every subgroup and every quotient group of G is also solvable.*

Proof. If H is a subgroup of G, then it is easy to prove by induction that $H^{(i)} \subset G^{(i)}$ for all i. Hence, $G^{(n)} = \{1\}$ implies $H^{(n)} = \{1\}$ and H is solvable.

If $\varphi : G \to K$ is a surjective homomorphism, then $\varphi(G') = K'$: if $uvu^{-1}v^{-1}$ is a commutator in K, choose $x, y \in G$ with $\varphi(x) = u$ and $\varphi(y) = v$; then $\varphi(xyx^{-1}y^{-1}) = uvu^{-1}v^{-1}$. One proves easily, by induction, that $\varphi(G^{(i)}) = K^{(i)}$ for all i. Hence, if G is solvable, then $G^{(n)} = \{1\}$ for some n and $K^{(n)} = \{1\}$; therefore K is solvable. Now take $K = G/N$, where N is any normal subgroup of G, and take φ to be the natural map $G \to G/N$. •

Theorem G.21. *Let G be a group with normal subgroup H. If H and G/H are solvable groups, then G is solvable.*

Proof. Let

$$G/H = G^* = G_0^* \supset G_1^* \supset \cdots \supset G_m^* = \{1\}$$

be a normal series with abelian factor groups. By the correspondence theorem, there is a series

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = H$$

with each G_i normal in G_{i-1} and with abelian factor groups. Since H is solvable, there is a normal series

$$H = H_0 \supset H_1 \supset \cdots \supset H_n = \{1\}$$

with abelian factor groups. Splicing these two series together gives a normal series for G with abelian factor groups. •

One can also prove this result using the criterion in Lemma G.19.

Definition. The ***center*** of a group G is

$$Z(G) = \{g \in G : gx = xg \quad \text{for all } x \in G\}.$$

It is easy to see that $Z(G)$ is an abelian normal subgroup of G.

It is also easy to prove that $g \in Z(G)$ if and only if the conjugacy class of g is $\{g\}$, so that $|Z(G)|$ is the number of conjugacy classes of cardinality 1.

There are groups G with $Z(G) = \{1\}$; for example, $Z(S_3) = \{1\}$.

Lemma G.22. *If p is a prime and $G \neq \{1\}$ is a p-group, then $Z(G) \neq \{1\}$.*

Proof. Partition G into its conjugacy classes: using our remark above about conjugacy classes of cardinality 1, there is a disjoint union

$$G = Z(G) \cup C_1 \cup \cdots \cup C_t,$$

where the C_i are the conjugacy classes of cardinality larger than 1. If we choose $x_i \in C_i$, then Corollary G.11 gives

$$|G| = |Z(G)| + \sum [G : C_G(x_i)].$$

By Lagrange's theorem, p divides $[G : C_G(x_i)]$ for all i (if $x_i \notin Z(G)$, then $C_G(x_i) \neq G$ and $[G : C_G(x_i)] \neq 1$), and so p divides $|Z(G)|$. •

Theorem G.23. *Every p-group G is solvable, and hence it has a normal subgroup of index p if $G \neq \{1\}$.*

Proof. We prove that G is solvable by induction on $|G|$. If $|G| \neq 1$, then $Z(G) \neq \{1\}$, by Lemma G.22. If $Z(G) = G$, then G is abelian, hence solvable. If $Z(G) \neq G$, then $G/Z(G)$ is a p-group of order $< |G|$, hence it is solvable, by induction. Since $Z(G)$ is solvable, being abelian, Theorem G.21 shows that G is solvable.

As G is solvable, the second statement follows from Corollary G.17. •

Let us pass from abstract groups to permutation groups; Cayley's theorem shows that this is no loss in generality.

Recall that S_X, the symmetric group on a set X, is the set of all permutations (bijections) of X under composition. If $X = \{x_1, \ldots, x_n\}$, then there is an isomorphism $S_X \to S_n$ (namely, $\alpha \mapsto \theta\alpha\theta^{-1}$, where $\theta(x_i) = i$) and one usually identifies these two groups.

Theorem G.24 (Cayley). *Every group G of order n is (isomorphic to) a subgroup of S_n.*

Proof. If $a \in G$, then the function $\lambda_a : G \to G$, defined by $x \mapsto ax$, is a bijection, for its inverse is $\lambda_{a^{-1}} : x \mapsto a^{-1}x$; hence $\lambda_a \in S_G$ (of course, $S_G \cong S_n$). Define $\lambda : G \to S_G$ by $a \mapsto \lambda_a$. It remains to prove that λ is an injective homomorphism.

If $a, b \in G$ are distinct, then $\lambda_a \neq \lambda_b$ (because these two functions have different values on $1 \in G$). Finally, λ is a homomorphism:

$$\lambda_a\lambda_b : x \mapsto bx \mapsto a(bx)$$

and

$$\lambda_{ab} : x \mapsto (ab)x,$$

so the associative law implies $\lambda_{ab} = \lambda_a\lambda_b$, as desired. •

Lemma G.25. *The alternating group A_n is generated by the 3-cycles.*

Proof. If $\alpha \in A_n$, then $\alpha = \tau_1 \cdots \tau_m$, where each τ_i is a transposition and m is even; hence

$$\alpha = (\tau_1\tau_2)(\tau_3\tau_4)\cdots(\tau_{m-1}\tau_m).$$

If τ_{2k-1} and τ_{2k} are not disjoint, then their product is a 3-cycle: $\tau_{2k-1}\tau_{2k} = (ab)(ac) = (acb)$;[18] if they are disjoint, then

$$\tau_{2k-1}\tau_{2k} = (ab)(cd) = (ab)(bc)(bc)(cd) = (bca)(cdb).$$

Therefore α is a product of 3-cycles. •

Lemma G.26. *The commutator subgroup of S_n is A_n.*

Proof. Since S_n/A_n is abelian (it has order 2), Lemma G.18 gives $S_n' \subset A_n$. Since A_n is generated by the 3-cycles, it suffices to prove every $\sigma = (ijk)$ is a commutator. Since σ has order 3, $\sigma = \sigma^4 = (\sigma^2)^2$. But

$$\sigma^2 = (ikj) = (ij)(ik),$$

[18] We multiply permutations from right to left:

$$(\sigma\tau)a = \sigma(\tau(a))$$

because we are composing functions: that is, $\sigma\tau : a \mapsto \tau a \mapsto \sigma(\tau a)$. In particular, $(ab)(ac) = (acb)$ because

$$(ab)(ac) : a \mapsto c \mapsto c; \quad b \mapsto b \mapsto a; \quad c \mapsto a \mapsto b.$$

so that

$$\sigma = \sigma^4 = (ij)(ik)(ij)(ik);$$

this is a commutator because $(ij) = (ij)^{-1}$ and $(ik) = (ik)^{-1}$. •

Lemma G.27. *If $\gamma = (i_0, i_1, \ldots, i_{k-1})$ is a k-cycle in S_n and $\alpha \in S_n$, then $\alpha\gamma\alpha^{-1}$ is also a k-cycle; indeed,*

$$\alpha\gamma\alpha^{-1} = (\alpha i_0, \alpha i_1, \ldots, \alpha i_{k-1}).$$

Conversely, if $\gamma' = (i_0', i_1', \ldots, i_{k-1}')$ is another k-cycle, then there exists $\alpha \in S_n$ with $\gamma' = \alpha\gamma\alpha^{-1}$.

Proof. If $\ell \neq \alpha i_j, 0 \leq j \leq k-1$, then $\alpha^{-1}\ell \neq i_j$ and so $\gamma(\alpha^{-1}\ell) = \alpha^{-1}\ell$; therefore $\alpha\gamma\alpha^{-1}$: $\ell \mapsto \alpha^{-1}\ell \mapsto \alpha^{-1}\ell \mapsto \ell$; that is, $\alpha\gamma\alpha^{-1}$ fixes ℓ. If $\ell = \alpha i_j$, then $\alpha\gamma\alpha^{-1} : \ell = \alpha i_j \mapsto i_j \mapsto i_{j+1} \mapsto \alpha i_{j+1}$ (read subscripts mod k). Hence $\alpha\gamma\alpha^{-1}$ and $(\alpha i_0, \alpha i_1, \ldots, \alpha i_{k-1})$ are equal.

Conversely, given γ and γ', choose a permutation α with $\alpha i_j = i_j'$ for all j. Then the first part of the proof shows that $\gamma' = \alpha\gamma\alpha^{-1}$. •

Remark. The same technique proves the lemma with γ a cycle replaced by γ a product of disjoint cycles.

Lemma G.28. *If H is a subgroup of a group G of index 2, then H is a normal subgroup of G.*

Proof. If $a \in G$ and $a \notin H$, then $aH \cap H = \emptyset$ and, by hypothesis, $aH \cup H = G$; hence aH is the complement of H. Since $Ha \cap H = \emptyset$, it follows that $Ha \subset aH$; that is, after multiplying on the right by a^{-1},

$$H \subset aHa^{-1}.$$

This inclusion holds for every $a \in G$, so we may replace a by a^{-1} to obtain $H \subset a^{-1}Ha$; that is, $aHa^{-1} \subset H$. Therefore, H is a normal subgroup of G. •

Theorem G.29. *The alternating group A_n is the only subgroup of S_n having index 2.*

Proof. If $[S_n : H] = 2$, then H is normal in S_n, by Lemma G.28, and Lemma G.18 gives $A_n = S_n' \subset H$ (for S_n/H has order 2, hence is abelian). But $|A_n| = n!/2 = |H|$, and so $H = A_n$. •

We are going to prove that A_5 is a simple group.

Lemma G.30. (i) *There are* 20 3*-cycles in* S_5*, and they are all conjugate in* S_5.

(ii) *All* 3*-cycles are conjugate in* A_5.

Proof. (i) The number of 3-cycles (abc) is $5 \times 4 \times 3/3 = 20$ (one divides by 3 because $(abc) = (bca) = (cab)$). The conjugacy of any two 3-cycles follows at once from Lemma G.27.

(ii) Given 3-cycles γ, γ', one must find an *even* permutation α with $\gamma' = \alpha\gamma\alpha^{-1}$. This can be done directly, but it involves consideration of various cases; here is another proof.

If $\alpha = (123)$ and $C_S(\alpha)$ is the centralizer of α in S_5, then Corollary G.11 gives $20 = [S_5 : C_S(\alpha)]$; hence $|C_S(\alpha)| = 6$. But we can exhibit the six elements that commute with α:

$$1, \cdot \alpha, \quad \alpha^2, \quad (45), \quad (45)\alpha, \quad (45)\alpha^2.$$

Only the first three of these are even permutations, and so $|C_A(\alpha)| = 3$, where $C_A(\alpha)$ is the centralizer of α in A_5. By Corollary G.11, the number of conjugates of α in A_5 is $[A_5 : C_A(\alpha)] = |A_5|/|C_A(\alpha)| = 60/3 = 20$. Therefore, all 3-cycles are conjugate to $\alpha = (123)$ in A_5. •

Theorem G.31. A_5 *is a simple group.*

Proof. If $H \neq \{1\}$ is a normal subgroup of A_5 and if $\sigma \in H$, then every conjugate of σ in A_5 also lies in H. In particular, if H contains a 3-cycle, then it contains all 3-cycles, by Lemma G.30(ii); but then $H = A_5$, by Lemma G.25.

Let $\sigma \in H, \sigma \neq 1$. After a harmless relabeling, we may assume either $\sigma = (123)$, $\sigma = (12)(34)$, or $\sigma = (12345)$ (these are the only possible cycle structures of (even) permutations in A_5). If $\sigma = (123)$, then $H = A_5$, as we have noted above. If $\sigma = (12)(34)$, define $\tau = (12)(35)$; then

$$\tau\sigma\tau^{-1} = (\tau 1\, \tau 2)(\tau 3\, \tau 4) = (12)(45)$$

and

$$\tau\sigma\tau^{-1}\sigma^{-1} = (354) \in H.$$

Finally, if $\sigma = (12345)$, define $\tau = (132)$; then

$$\sigma\tau^{-1}\sigma^{-1} = (\sigma 1\, \sigma 2\, \sigma 3) = (234)$$

and

$$\tau\sigma\tau^{-1}\sigma^{-1} = (134).$$

In each case, H must contain a 3-cycle. Therefore, A_5 contains no proper normal subgroups $\neq \{1\}$ and hence it is simple. •

One can prove, by induction, that A_n is simple for all $n \geq 5$.

The next counting lemma is useful.

Lemma G.32. *If* A *and* B *are subgroups of a finite group* G*, then*

$$|A \cap B||AB| = |A||B|,$$

where AB *is the subset* $\{ab : a \in A \text{ and } b \in B\}$.

Proof. We are going to use the following fact. If X and Y are finite sets and $\varphi : X \to Y$ is a surjection for which $|\varphi^{-1}(y)| = |\varphi^{-1}(y')|$ for all $y, y' \in Y$, then $|Y| = |X|/|\varphi^{-1}(y)|$.

Define $\varphi : A \times B \to AB$ by $(a, b) \mapsto ab$; of course, φ is a surjection. We claim that

$$\varphi^{-1}(ab) = \{(ac, c^{-1}b) : c \in A \cap B\}.$$

It is clear that $(ac, c^{-1}b) \in \varphi^{-1}(ab)$. Conversely, if $(\alpha, \beta) \in \varphi^{-1}(ab)$, then $ab = \alpha\beta$, where $\alpha \in A$ and $\beta \in B$. Hence, $\alpha^{-1}a = \beta b^{-1} \in A \cap B$; if c is their common value, then

$$(\alpha, \beta) = (ac, c^{-1}b).$$

Therefore, $|\varphi^{-1}(ab)| = |A \cap B|$ and $|AB| = |A \times B|/|A \cap B|$. •

Corollary G.33. *The only normal subgroups of* S_5 *are* $\{1\}$, A_5, *and* S_5.

Proof. Let $H \neq \{1\}$ be a normal subgroup of S_5. The second isomorphism theorem gives $H \cap A_5$ a normal subgroup of A_5; as A_5 is a simple group, either $H \cap A_5 = A_5$ or $H \cap A_5 = \{1\}$. In the first case, $A_5 \subset H$ and $H = A_5$ or $H = S_5$. In the second case, there is $h \in H$ with $h \notin A_5$, so that $HA_5 = S_5$. Since $H \cap A_5 = \{1\}$, Lemma G.32 gives $|H| = |S_5|/|A_5| = 2$. If $h \in H$, $h \neq 1$, then $h = (ab)$ (the only other elements of order 2 have the form $(ab)(cd)$, and they are even permutations). It is easy to find a conjugate distinct from h, and this contradicts the normality of H. •

Theorem G.34. S_n *is solvable for* $n \leq 4$*, but it is not solvable for* $n \geq 5$.

Proof. If $m < n$, then S_m is (isomorphic to) a subgroup of S_n. Since every subgroup of a solvable group is itself solvable (Theorem G.20), it suffices to show that S_4 is solvable and S_5 is not solvable.

Here is a normal series of S_4 that has abelian factor groups:

$$S_4 \supset A_4 \supset V \supset \{1\},$$

where V is the four group (the factor groups have orders 2, 3, 4, respectively, hence are abelian).

Were S_5 solvable, then its subgroup A_5 would also be solvable. Since A_5 is simple, its only normal series is $A_5 \supset \{1\}$, and the (only) factor group is the nonabelian group $A_5/\{1\} \cong A_5$. •

We now discuss Exercise 106, the group theoretic basis of the computation of the Galois groups of irreducible quartic polynomials over $\mathbb{Q}$.

First of all, we list the subgroups G of S_4 whose order is a multiple of 4. If $|G| = 4$, then the only abstract groups G are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, and both occur as subgroups of S_4 (in particular, $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$). There is a subgroup of order 8 isomorphic to the dihedral group D_8, namely, the symmetries of a square regarded as permutations of the 4 corners; since a subgroup of order 8 is a Sylow 2-subgroup of S_4, all subgroups of order 8 are isomorphic to D_8. Theorem G.29 shows that A_4 is the only subgroup of order 12 and, of course, S_4 itself is the only subgroup of order 24.

If $G \subset S_4$ and V is the four group (which is a normal subgroup of S_4), then the second isomorphism theorem gives $G \cap V \lhd G$ and

$$G/G \cap V \cong GV/V \subset S_4/V.$$

Define

$$m = |G/G \cap V|;$$

it follows that m is a divisor of $[S_4 : V] = 24/4 = 6$ ($S_4/V \cong S_3$, but we do not need this fact.)

Theorem G.35 (Exercise 106). *Let $G \subset S_4$ have order a multiple of 4 and let $m = |G/G \cap V|$.*

(i) *If $m = 6$, then $G = S_4$;*
(ii) *if $m = 3$, then $G = A_4$;*
(iii) *if $m = 1$, then $G = V$;*
(iv) *if $m = 2$, then $G \cong D_8$ or $\mathbb{Z}_4$ or V.*

Proof. If $m = 6$ or 3, then $|G| \geq 12$ ($|G|$ is divisible by 3 and, by hypothesis, 4). By Theorem G.29, A_4 is the only subgroup of S_4 of order 12, and so $A_4 \subset G$ in either case. But $V \subset A_4$. It follows easily that $m = 6$ forces $G = S_4$ and $m = 3$ forces $G = A_4$.

If $m = 1$, then $G = G \cap V$ and $G \subset V$; since $|G|$ is a multiple of 4, it follows that $G = V$.

If $m = 2$, then $|G| = 2|G \cap V|$; since $|V| = 4$, we have $|G \cap V| = 1$, 2, or 4. We cannot have $|G \cap V| = 1$ lest $|G| = 2$, which is not a multiple of 4. If $|G \cap V| = 4$, then $|G| = 8$ and $G \cong D_8$ (as we remarked above, D_8 is a Sylow 2-subgroup). If $|G \cap V| = 2$, then $|G| = 4$ and $G \cong \mathbb{Z}_4$ or V (these are the only abstract groups of order 4). •

The possibility $m = 2$ and $G \cong V$ can occur. Let G be the following isomorphic copy of V in S_4:

$$G = \{1, (12)(34), (12), (34)\}.$$

Note that $G \cap V = \{1, (12)(34)\}$ and $m = |G/G \cap V| = 4/2 = 2$. This group G does not act transitively on $\{1, 2, 3, 4\}$ because, for example, there is no $g \in G$ with $g(1) = 3$. Exercise 107 invokes the extra hypothesis of G acting transitively to eliminate the case $G \cong V$ from the list of candidates for G when $m = 2$.

Lemma G.36. *If G is a group and H is a subgroup of index n, then there is a homomorphism $\varphi : G \to S_n$ with $\ker \varphi \subset H$.*

Proof. Let X be the family of all cosets of H in G; since $|X| = n$, it is easy to see that $S_X \cong S_n$ (where S_X is the group of all permutations of X). For $g \in G$, define $\varphi(g) : X \to X$ by $\varphi(g) : aH \mapsto gaH$ (where $a \in G$); note that $\varphi(g)$ is a bijection, for its inverse is $\varphi(g^{-1})$. To see that φ is a homomorphism, compute:

$$\begin{aligned} \varphi(gg') : aH &\mapsto (gg')aH; \\ \varphi(g)\varphi(g') : aH &\mapsto g'aH \mapsto g(g'aH). \end{aligned}$$

If $\varphi(g)$ is the identity on X, then $\varphi(g) : aH \mapsto aH$ for all $a \in G$; in particular, $\varphi(g) : H \mapsto H$, so that $gH = H$ and $g \in H$. •

Theorem G.37. *A_6 has no subgroups of prime index.*

Proof. Now A_6 is a simple group of order $360 = 2^3 \cdot 3^2 \cdot 5$ (in fact, A_n is a simple group of order $\frac{1}{2}n!$ for all $n \geq 5$). If H is a subgroup of prime index, then $[A_6 : H] = 2$, 3, or 5. By Lemma G.36, there is a homomorphism $\varphi : A_6 \to S_n$, where $n = 2$, 3, or 5, with $\ker \varphi \subset H$; in particular, $\ker \varphi$ is a normal subgroup of A_6 with $\ker \varphi \neq A_6$. Since A_6 is simple, $\ker \varphi = \{1\}$ and φ is an injection. But this is impossible because $|S_5| = 120 < 360$. •

Lemma G.38. *S_5 has no subgroups of order 30 or of order 40.*

Proof. If H is a subgroup of order 30, then H has index $[S_5 : H] = 120/30 = 4$. Lemma G.36 gives a homomorphism $\varphi : S_5 \to S_4$ with

$\ker \varphi \subset H$. But $\ker \varphi$ is a normal subgroup of S_5, and so its order must be 1, 60, or 120 (Corollary G.33). Since $|H| = 30$, it follows that $\ker \varphi = \{1\}$, and S_5 is isomorphic to a subgroup of S_4, a contradiction. A similar argument shows that S_5 has no subgroup of index 3. •

Theorem G.39. *If α is a 5-cycle in S_5 and τ is a transposition in S_5, then $\langle \alpha, \tau \rangle = S_5$.*

Proof. Let $H = \langle \alpha, \tau \rangle$ be the subgroup generated by α and τ. We may assume that $\alpha = (1\,2\,3\,4\,5)$ and $\tau = (1\,i)$. Now some power of α, say, α^k carries i into 1, so that Lemma G.27 gives $\alpha^k(1\,i)\alpha^{-k} = (j\ 1)$ for some j (actually, $j = \alpha^k 1$). Note that $i \neq j$ because α^k does not commute with $(1i)$. But $(1i)(1j) = (1\,j\,i)$, an element of order 3. The order of H is thus divisible by 2, 3, and 5, hence $|H| \geq 30$. By Lemma G.38, $|H| = 60$ or 120. If $|H| = 60$, then $H = A_5$, by Theorem G.29; but $H \neq A_5$ because $\tau \in H$ is an odd permutation. Therefore $H = S_5$. •

A more computational proof shows first that every transposition can be obtained from α and τ, and then that S_5 is generated by the transpositions.

Theorem G.40. *A subgroup H of S_5 is solvable if and only if $|H| \leq 24$.*

Proof. We leave to the reader the fact that every group of order ≤ 24 is solvable (whether or not it is a subgroup of S_5; indeed, every group of order < 60 is solvable).

Since $|S_5| = 120$, the only divisors of $|S_5|$ larger than 24 are 30, 40, 60, and 120. Now S_5 itself is not solvable, by Theorem G.34; also, A_5 is the only subgroup of order 60 (Theorem G.29), and it is not solvable because it is simple and not abelian (Theorem G.31). Lemma G.38 completes the proof. •

Theorem G.40 is used in Exercise 111. It is implicit in the second part of this exercise that S_5 does have a subgroup of order 20; the ***normalizer*** of a Sylow 5-subgroup is such a subgroup, where the normalizer $N_G(P)$ of a subgroup P of G is defined as:

$$N_G(P) = \{g \in G : gPg^{-1} = P\}.$$

Of course, S_5 does have a solvable subgroup of order 24, namely, S_4.

Appendix C
Ruler-Compass Constructions

We are going to show that the classical Greek problems: squaring the circle, duplicating the cube, and trisecting an angle, are impossible to solve. As we shall see, the discussion uses only elementary field theory; no Galois theory is required.

It is clear one that can trisect a 60° angle with a protractor (or any other device than can measure an angle); after all, one can divide any number by 3. Therefore, it is essential to state the problems carefully and to agree on certain ground rules. The Greek problems specify that only two tools are allowed, and each must be used in only one way. Let P and Q be points in the plane; we denote the line segment with endpoints P and Q by PQ, and we denote the length of this segment by $|PQ|$. A ***ruler*** (or ***straightedge***) is a tool that can draw the line $L(P, Q)$ determined by P and Q; a ***compass*** is a tool that draws the circle with radius $|PQ|$ and center either P or Q; denote these circles by $C(P; Q)$ or $C(Q; P)$, respectively. Since every construction has only a finite number of steps, we shall be able to define "constructible" points inductively.

Given the plane, we establish a coordinate system by first choosing two distinct points, A and $\overline{A}$; call the line they determine the ***x-axis***. Use a compass to draw the two circles $C(A; \overline{A})$ and $C(\overline{A}; A)$ of radius $|A\overline{A}|$ with centers A and $\overline{A}$, respectively. These two circles intersect in two points; the line they determine is called the ***y-axis***; it is the perpendicular bisector of $A\overline{A}$, and it intersects the x-axis in a point O, called the ***origin***. We define the distance $|OA|$ to be 1. We have introduced coordinates in the plane; in particular, $A = (1, 0)$ and $\overline{A} = (-1, 0)$.

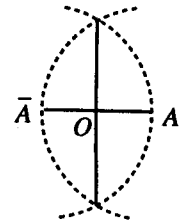

Figure 5