$m+k-1$ gates in the kth row. Figure 7 illustrates the (3,3)-treelike game.

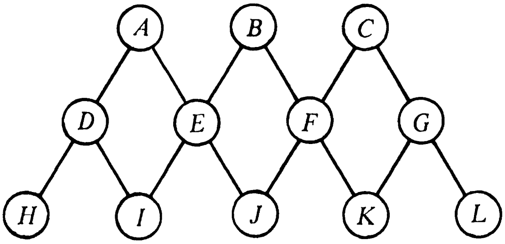


FIG. 7.

As we know, the patterns of the (3,3)-concave game fall into two classes, the odd patterns and the even patterns. The following questions are posed about the other THINK-A-DOT-like games:

1. The number of pattern classes in the (m,n)-concave game is $2^{[(n-1)/2]}$;
2. Prove or disprove that the number of pattern classes in the (3,3)-convex game is 4;
3. Prove or disprove that the number of pattern classes in the (m,n)-convex game is $4^{[(n-1)/2]}$;
4. What is the number of pattern classes in the (3,3)-treelike game? In the (m,n)-treelike game?
5. Effectively solve the minimum move problem for one of the generalized games.

References

1. B. L. Schwartz, Mathematical theory of THINK-A-DOT, this MAGAZINE, 40 (1967) 187–193.
2. A. C. Fleck, Isomorphism Groups of Automata, J. Assoc. Comput. Mach., 9 (1962) 469–476.
3. R. Bayer, Automorphism Groups and Quotients of Strongly Connected Automata and Monadic Algebras, Report No. 204, Department of Computer Science, University of Illinois, 1966.
4. Z. Bavel, On the Structure and Automorphism of Automata, Report 192, Department of Computer Science, University of Illinois, 1965.
5. THINK-A-DOT Instructions, E. S. R. Inc., Montclair, N. J.

FINITE GROUPS ACTING ON SETS WITH APPLICATIONS

LOUIS W. SHAPIRO, Howard University

1. The concept of a group acting on a set is a small generalization of the idea of a permutation group and provides a viewpoint that is useful in attacking a wide variety of problems. The basic concepts and some of the applications are presented here as a series of problems. None are exceptionally difficult although many are motivated by or follow from previous problems. For most an elementary knowledge of group theory will suffice. After the first two sections all sections can be read independently. With moderate supervision this might be useful as an independent study project for any student who has completed a first course in modern algebra.

DEFINITION. *A group, $(G,\circ)$ acts on a set S if each g in G is a function from S to S and*

(a) $(g \circ h)(s) = g(h(s))$ *for all g, h in G, s in S*

(b) $I(s) = s$ *for all s in S, where I is the identity of G.*

Exercise 1–1. If G acts on S each g in G is a permutation of S.

DEFINITION. *If S is a set,* $\mathrm{Sym}(S)$ *is the group of all permutations of S and* $\mathrm{Alt}(S)$ *is the set of all even permutations.* $\mathrm{Sym}(S)$ *is called the symmetric group on S and* $\mathrm{Alt}(S)$ *the alternating group on S.*

Except for informational items enclosed in parentheses, simple affirmative statements in the exercises are to be proved.

Exercise 1–2 *and definition.* If G acts on a set S then there is a homomorphism from G into $\mathrm{Sym}(S)$. This homomorphism will always be denoted θ and will be called the *homomorphism of G acting on S* or the action homomorphism.

Exercise 1–3 *and definition.* If $t \in S$ then $G_t = \{g \mid g \in G,\ g(t) = t\}$ is called the *stability subgroup* of t. Show that G_t is actually a subgroup of G.

DEFINITION. *If $t \in S$ where G acts on S, then the orbit of t under G is the set of all $g(t)$ where g ranges through the elements of G. This orbit is denoted $\mathcal{O}_G(t)$ or $\mathcal{O}(t)$.*

Exercise 1–4. If $S = \{1,2,3,4\}$ and G is $\mathrm{Sym}(S)$ (in such cases we will denote G as $\mathrm{Sym}(4)$) then find G_4 and $\mathcal{O}(4)$.

Exercise 1–5. If $S = \{1,2,3,4,5,6,7\}$ and G is the group of permutations I, $(1234)(56)$, $(13)(24)$, $(1432)(56)$ then find G_1, G_5, G_7, $\mathcal{O}_1, \mathcal{O}_5$, and $\mathcal{O}_7$.

Exercise 1–6. Let $f_1(z) = z, f_2(z) = -1/(1+z), f_3(z) = -(1+z)/z$. Show that $(G,\circ)$ is a group where $G = \{f_1, f_2, f_3\}$ and $\circ$ is compositions of functions. Then show that G acts on the complex plane with 0 and -1 deleted. Find G_1, G_i, and G_ω where $\omega = e^{(2\pi i/3)}$.

We still need an example of a group acting on a set which is not a permutation group. Such examples will be plentiful in Sections 2 and 5 but for now we provide the following:

Exercise 1–7. Let $G = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; ac \neq 0\right\}$ be the group of nonsingular upper triangular matrices with real coefficients. If $f = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ then let $f(x) = (ax + b)/c$. Show that this defines an action of G on the real line, $\mathbb{R}$. What is the kernel of the action homomorphism? What are G_0 and $\mathcal{O}(0)$?

Exercise 1–8. If G acts on S then $s \in \mathcal{O}(t)$ if and only if $\mathcal{O}(s) = \mathcal{O}(t)$.

Exercise 1–9. If G acts on S we say $s \sim t$ if $s = g(t)$ for some $g \in G$ where s and t

are in S. Show that $\sim$ is an equivalence relation and that the equivalence classes of $\sim$ are the orbits of G.

Perhaps the next exercise shows the origin of the term orbit.

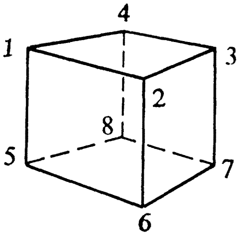
Exercise 1–10. Let G be the group of all 2×2 matrices of the form $\begin{pmatrix} \cos\theta \sin\theta \\ -\sin\theta \cos\theta \end{pmatrix}$. If $f = \begin{pmatrix} \cos\theta \sin\theta \\ -\sin\theta \cos\theta \end{pmatrix}$ then let $f(x, y) = (x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta)$. Thus f rotates the point (x, y) through an angle θ around the origin. Show that G is a group and that G acts on $\mathbb{R}^2$. What are $G_{(1,0)}$, $G_{(0.0)}$, $\mathcal{O}(1,0)$, $\mathcal{O}(0,0)$? Describe the orbits of G. These obviously partition $\mathbb{R}^2$ which we knew *a priori* by Exercise 1–8.

Exercise 1–11. If G acts on S and $g(s) = t$ then $G_s = g^{-1}G_tg$. In particular G_s and G_t are isomorphic.

We now assume G is finite and we can use the partition to do counting in S.

Exercise 1–12. The Basic ,Theorem. *If a finite group G acts on a set S then* $|G| = |G_t|\ |\mathcal{O}(t)|$ *for any t in S.* (*Here* $|A|$ *denotes the cardinality of the set A.*)

Exercise 1–13. Take a cube and label all its vertices, say, as follows.



Any rotation of the cube into itself can be represented by the permutation it affects on the vertices. $\alpha = (1234)\ (5678)$, $\beta = (1265)\ (4378)$, $\gamma = (12)\ (46)\ (35)\ (78)$ and $\delta = (254)\ (683)$ are all rotations of the cube. Show $\mathcal{O}(1) = \{1, 2, \cdots, 8\}$ and $R_1 = \{I, \alpha, \alpha^2\}$ and thus that $|R| = 24$ where R is the group of all rotations of the cube into itself.

2. If $G_t = G$ or equivalently $g(t) = t$ for all g in G then t is a *fixed point* of the action of G on S. An oft-occurring situation which guarantees fixed points is set up in the next few exercises.

Exercise 2–1 *and definition.* If P is a finite p-group acting on set S then every orbit has length $1, p, p^2, \cdots, |P|$. The *length* of the orbit $\mathcal{O}(t)$ is just $|\mathcal{O}(t)|$.

Exercise 2–2 (Basic p-group Theorem). *If P is a finite p-group acting on a set S with* $p \not| \ |S|$ *then P has at least one fixed point.*

Exercise 2–3. If G is a group of order 55 acting on a set, S, of order 18, show that G must have a fixed point (in fact at least 2).

Exercise 2–4. Returning to the rotation of a cube discussed in Exercise 1–13 we have a group, R, of order 24. Any element of order 3 generates a cyclic group of order 3. Conversely any subgroup of order 3 is cyclic and thus generated by an element. Show that any element of order 3 in R has 2 fixed points. Geometrically these points must be diametric. How many elements of order 3 are there in R?

We now set up another action. Let G be a group and also let $S = G$. We let G act on G by conjugation. That is, if g is in G then $f_g(x) = gxg^{-1}$ for all x in G. $f_g f_h(x) = f_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = ghx(gh)^{-1} = f_{gh}(x)$, and also $f_I(x) = IxI^{-1} = x$, so indeed this is an action. If g is an element of G, the function f_g is called an *inner automorphism.*

Exercise 2–5. Show that the kernel of the action of G acting on G by conjugation is $\mathbb{Z}(G)$, the center of G.

Exercise 2–6. If H is a subgroup of G let H act on the set G by conjugation. Show that g is a fixed point of H if and only if g is in $C_G(H)$, the centralizer of H in G.

This case of G acting on G by conjugation is of sufficient interest that a special terminology has developed. An orbit is called a *conjugate class* and the stabilizer of a is just the centralizer $C_G(a)$ of a in G. By Exercise 8 the conjugate classes partition G. This action of G on G by conjugation in general does not make G into a permutation group on itself.

Exercise 2–7 (The class equation). Let the conjugate classes of the finite group G be $Cl(a_1)$, $Cl(a_2), \cdots, Cl(a_m)$, $Cl(a_{m+1}), \cdots, Cl(a_k)$ with $|Cl(a_1)| = |Cl(a_2)| = \cdots = |Cl(a_m)| = 1$ and $|Cl(a_i)| > 1$ $\forall i > m$. Then

$$|G| = \sum_{i=1}^{k} |Cl(a_i)| = |\mathbb{Z}(G)| + \sum_{i=m+1}^{k} |Cl(a_i)|$$

$$= |\mathbb{Z}(G)| + \sum_{i=m+1}^{k} \frac{|G|}{|C_G(a_i)|} = \sum_{i=1}^{k} \frac{|G|}{|C_G(a_i)|}.$$

Exercise 2–8. Let the finite p-group P act on the set $P^{\#}$ of all nonidentity elements of P by conjugation. Since $p \nmid |P^{\#}|$ show that $|\mathbb{Z}(P)| > 1$.

Exercise 2–9. Every group of order p^2 (p a prime) is abelian.

Exercise 2–10. If N is a normal subgroup of a finite p-group then show that P acts on N by conjugation. Also show that $p \nmid |N^{\#}|$, that P has fixed points in $N^{\#}$, and that $|N \cap \mathbb{Z}(P)| > 1$. (Taking $N = P$ we obtain Exercise. 2.8 as a special case.)

Exercise 2–11. Find all finite groups G with exactly 1, 2 or 3 conjugate classes.

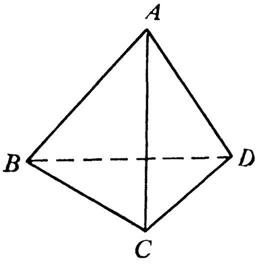
3. In this section we discuss the Pólya-Burnside Theorem and a few applications of it in some counting problems. The Pólya-Burnside Theorem appears in Burnside [**2**] page 189. Pólya realized its applicability and extended its uses in [**10**].

Exercise 3–1 (Pólya-Burnside). *If a finite group G acts on a finite set S and* $\chi(g)$

is the number of elements in S fixed by g then $(1/|G|)\sum_{g\in G}\chi(g)$ = *the number of orbits of G acting on S.* Hint: count the number of pairs (g, s) where $g(s) = s$ two different ways and compare.

Using this theorem we now can consider a counting problem. Let us assume we have wires set up as a regular tetrahedron and at each of the six edges we can attach our choice of a 100–ohm resistor, a 75 watt light bulb, or a capacitor. In our supplies are at least 6 of each of these components. We want to know how many essentially different contraptions we can make if we allow rotations of the tetrahedrons. First we take care of two preliminaries.

Preliminary 1. It is straightforward to count the different (ignoring rotations) contraptions available. We have 3 choices available at each of six locations so we have a set, S, of $3^6 = 729$ possible contraptions.



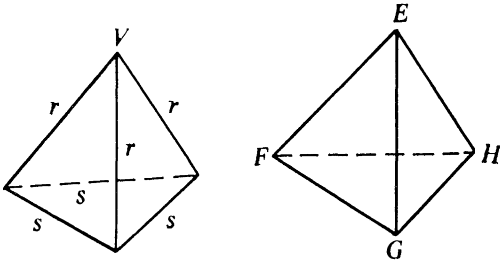
Preliminary 2. What does the group of rotations of a regular tetrahedron look like? If we label the vertices of a tetrahedron we find that the elements are I, (ABC), (ACB), (ABD), (ADB), (ACD), (ADC), (BCD), (BDC), (AB) (CD), (AC) (BD), and (AD) (BC). Thus there is one element of order 1, 8 elements of order 3 each fixing one vertex and 3 elements of order 2 each with no fixed vertices. Let us call this group G.

Returning now to our problem we find that we have a count from Preliminary 1 but it is too high. For instance, there are 6 different contraptions with 5 resistors and 1 light bulb but these are not essentially different if we allow rotations. In fact, these six elements of S form just one orbit under G. Upon further thought each orbit under G gives us just one "essentially different" contraption so the Pólya-Burnside Theorem is exactly what is needed here.

We now need only to compute the $\chi(g)$ for each g in G. $\chi(I) = 3^6$ since the identity fixes every contraption in S. If g is an element of order 3, (a 120° rotation about an axis through one vertex, V, and the center of the opposite triangle) then g fixes only elements of the form below where r and s are any of the 3 choices. Thus

$$\chi(g) = 3^2.$$

If h has order 2 and thus interchanges two pairs of vertices we can assume $h = (EF)$ (GH). Then we have an arbitrary choice of 3 for the edges EF and HG. Side EG is taken to FH (and conversely) so we have a free choice for EG but then FH must be the same choice. Similarly we have a free choice for EH but then no choice for FG. Thus



$\chi(h) = 3^4$ here. Putting this all together we obtain:

$$\text{Answer} = \text{number of orbits} = \frac{1}{|G|}\Sigma_{g\in G}\,\chi(g)$$

$$= \frac{1}{12}(\chi(I) + 8\chi(g) + 3\chi(h)) = \frac{1}{12}(3^6 + 8\cdot 3^2 + 3\cdot 3^4)$$

$$= 87.$$

Exercise 3–2. Redo this example with n choices available at each side instead of 3. This should incidentally give you a somewhat elaborate proof that $(1/12)\cdot(n^6 + 8n^2 + 3n^4)$ is an integer for all positive integers n.

Exercise 3–3. Analyze the dihedral group of order 12 (that is, the group of symmetries of a regular hexagon), as a permutation group on its 6 vertices. Analyze here means first find the number of elements of each order, then subdivide these either as to number of fixed points or geometrically.

Exercise 3–4. If at each carbon atom in a benzene molecule either a $-NH^3$, a $COOH$, or a $-OH$ radical can be attached, how many different compounds are possible?

Exercise 3–5. If each side of a regular hexagon can be painted red, yellow, black, or green, how many essentially different designs are possible allowing all symmetries of a regular hexagon?

Exercise 3–6. If each side and both ends of a regular triangular prism can be painted one of 6 colors, how many essentially different combinations are possible?

Exercise 3–7. If a tape contains 10 digits each either 0 or 1 but the tape can be read indiscriminately from either end, then how many essentially different messages can be recorded on this tape?

For further developments of this material see Pólya [**10**], Liu [**8**], or Harary [**6**]. This theorem can be extended to give a count of the number of graphs with n vertices. See Harary's book for this and for various other important counting problems in combinatorics. His book also contains an extensive list of unsolved counting problems.

There are some other results related to the Polya counting theorem.

DEFINITION. *If a group G acts on a set S and the only orbit of this action is S itself then G is said to be transitive. If for every two pairs of points* $\{s_1, s_2\}$ *and* $\{t_1, t_2\}$ *in S there is a g in G such that* $g(s_1) = t_1$ *and* $g(s_2) = t_2$ *then G is doubly transitive.*

Exercise 3–8. *If G is transitive on S then* $|S| \,\big|\, |G|$.

Exercise 3–9. If *G is transitive on S then G is doubly transitive if and only if* G_t is transitive on $S - \{t\}$.

Exercise 3–10. If G is transitive on S then

$$\sum_{g \in G} (\chi(g))^2 = t|G|$$

where $\chi(g)$ is the number of fixed points of g and t is the number of orbits of G_s. In particular if G is doubly transitive

$$\sum_{g \in G} (\chi(g))^2 = 2|G|.$$

The following exercise is related.

Exercise 3–11*.

$$\sum_{g \in G} (\rho_2(g))^2 = \alpha|G|$$

where $\rho_2(g) = |\{x | x \in G, x^2 = g\}|$ and α is the number of conjugate classes, C, in G such that if x is in C so is x^{-1}.

Exercise 3–12** (unsolved). Generalize 3–11 for other numbers than 2. (See Research Problems, March 1971, AMERICAN MATHEMATICAL MONTHLY.)

4. In this section we consider the group $GL(2,F) = G$ of all 2×2 nonsingular matrices acting on various sets. Let the matrix $\binom{ab}{cd}$ take the point (x, y) to $(x, y)\binom{ab}{cd} = (ax + cy, bx + dy)$.

We can take S to be points in $F \times F$, lines in $F \times F$ through $(0,0)$, rays emanating from the origin, all subsets of $F \times F$, all finite subsets of $F \times F$, or a variety of other sets.

Exercise 4–1. Let $G = GL(2,F)$ act on the lines through $(0,0)$ in F^2 as above and let M be an element of G. Then a line, l, is fixed by M if and only if every point on l is an eigenvector of M.

Exercise 4–2. Find the subgroup of $GL(2,\mathbb{R})$ that takes all points on the hyperbola $xy = 1$ to other points on the same hyperbola. Prove that this is a maximal subgroup of $SL^*(2,\mathbb{R})$, the matrices of determinant ± 1.

Let $\mathbb{Z}_p$ denote the field of p elements where p is a prime. Let $S = \mathbb{Z}_p \times \mathbb{Z}_p$ and let $S' = \mathbb{Z}_p \times \mathbb{Z}_p - (0,0)$.

Exercise 4–3. If P is a p-subgroup of $GL(2, \mathbb{Z}_p)$ then P has a fixed point in S'. Therefore, there is a nonzero vector v in $\mathbb{Z}_p \times \mathbb{Z}_p$ such that v is an eigenvector with eigenvalue 1 for all the matrices in P. (Show this is also true if P is a p-subgroup of $GL(n, \mathbb{Z}_p)$.)

This last result can be generalized from $\mathbb{Z}_p$ to all fields of characteristic p. See Gorenstein [**5**] page 31.

Exercise 4–4. If $G = SL(n,F)$ denotes the group of all $n \times n$ matrices with determinant 1 and S is the set of all lines through the origin of $F_{(n)}$ then show that G acts on S. Show also that $\mathcal{O}(l) = S$ for any line l in S. Show that the kernel of the action homomorphism is $\mathbb{Z}(G)$. The group $G/\mathbb{Z}(G)$ is thus a permutation group on S and is called $PSL(n,F)$, the projective special linear group over F. (Except when F has order 2 or 3, $PSL(n,F)$ is a simple group.)

Exercise 4–5. Calculate the orders of $GL(2,\mathbb{Z}_p)$, $SL(2,\mathbb{Z}_p)$, $\mathbb{Z}(SL(2,\mathbb{Z}_p))$ and $PSL(2,\mathbb{Z}_p)$. Do the same for n instead of 2.

DEFINITION. *A finite group G is a Frobenius Group if N and H are proper subgroups of G such that $N \Delta G$, $NH = G$, and any $h \in H^*$ induces a fixed point free automorphism of n. That is $h^{-1}nh = n$ with $h \in H$, $n \in N$ implies $h = e$ or $n = e$.*

Frobenius groups are important in the theory of finite groups, division rings, projective geometry, and permutation groups. They have been classified quite thoroughly (see Passman [**9**]). It is known that N is always nilpotent and that H is solvable or involves $SL(2,\mathbb{Z}_5)$, N is called the kernel and H the complement. The following example is an interesting piece of folklore.

Exercise 4–6. Show that $SL(2,\mathbb{Z}_5)$ acts on $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$ in a fixed point free manner, so that the semidirect product of $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$ with $SL(2,\mathbb{Z}_5)$ is the smallest Frobenius group whose complement is not solvable. You may assume $SL(2,5)$ is a subgroup of $SL(2,\mathbb{Z}_{11})$ which follows from some computations with generators and relations (see Huppert [**7**]). This result will follow if we can show every element of $SL(2,\mathbb{Z}_5)$ of order 2, 3, or 5 is fixed point free which follows from the basic p-group theorem applied to the vectors in $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$. Since $|(\mathbb{Z}_{11} \times \mathbb{Z}_{11})^*| = 120 = |SL(2,\mathbb{Z}_5)|$ this must be the smallest such example.

5. Many of the applications of groups acting on sets are in group theory itself. These come about by picking for the set S various sets of subsets of G. For instance back in Section 2 we let $S = G$ or $G - \{1\}$ and then let G act by conjugation.

Exercise 5–1. The Strong Cayley Theorem. *Let H be a subgroup of G and let $S = \{H, Hx, Hy, \cdots\}$ be the set of all right cosets of S. Let G act on S by right mul-*

tiplication so that $Hx \overset{g}{\to} Hxg$. Verify that this is an action and that the kernel of the action homomorphism is $\bar{H} = \bigcap_{x \in G} x^{-1}Hx$.

Exercise 5–2. If H is a subgroup of G show that $\bar{H} = \bigcap_{x \in G} x^{-1}Hx$ is the largest normal subgroup contained in H.

If H is of index n in G and θ is the action described above, we note that θ gives a homomorphism from G into Sym(n).

Exercise 5–3. If $H = \{I\}$, the identity subgroup, show that Cayley's Theorem results.

Using the Strong Cayley Theorem, we can obtain direct results saying that existence of a large subgroup guarantees the existence of a reasonably large normal subgroup. Conversely if normal subgroups are sparse so are large subgroups.

Exercise 5–4. If a group G has a subgroup H of finite index greater than 1, then G also has a normal subgroup of finite index greater than 1.

Exercise 5–5. If a group G has order 10,000, then G cannot be simple. [The 1st Sylow Theorem can be used here.]

Exercise 5–6. Using the fact that Alt(n) is simple for $n \geqq 5$ show that Alt(5) has no subgroups of order 15, 20 or 30. Show also that Alt(6) has no subgroups of prime index (it is the smallest group with this property).

Exercise 5–7. For $n \geqq 5$ show that Alt(n) has no subgroups of index $2, 3, \cdots, n-1$.

Exercise 5–8. If G has a subgroup of index 2, 3, or 4 show that G cannot be simple.

Exercise 5–9. For any positive integer, n, there are but a finite number of simple groups having a subgroup of index n.

It would be of great interest if this last result could be sharpened sufficiently to give a useful count. The next two problems are from recent issues of the AMERICAN MATHEMATICAL MONTHLY and are easy if set up with the proper group or subgroup acting on the correct set.

Exercise 5–10. If G is of order $p^n m$ where $m < 2p$ and p is prime, then G has a normal subgroup of order p^n or p^{n-1}.

Exercise 5–11. If G is a torsion group and H a subgroup of finite index m such that each nonidentity element of H has order $\geqq m$, then H is normal. [It is convenient to consider m prime and composite separately.]

Exercise 5–12. Show that the smallest symmetric group which contains a subgroup isomorphic to the quaternions is Sym (8).

Next we develop a short proof of the Sylow theorems using virtually no group theory. The standard proof due to Frobenius [4] can be found in many books such as Curtis and Reiner [**3**]. We start with some elementary results from ring theory. Our approach is due in part to Wielandt [**13**].

Exercise 5–13. Prove that the binomial theorem holds in any commutative ring.

Exercise 5–14. If p is a prime show

(a) $p \,\Big|\, \binom{p}{k}$ for $k = 1, 2, \cdots, p-1$.

(b) $(a+b)^p = a^p + b^p$ in any commutative ring of characteristic p.

(c) The Frobenius map $a \xrightarrow{\theta} a^p$ is a ring homomorphism in any commutative ring of characteristic p.

(d) $a \xrightarrow{\theta^k} a^{p^k}$ is a ring homomorphism in any commutative ring of characteristic p. One application of Exercise 5–14 (c) is the following:

Exercise 5–15.

(I) $a^p = a$ for all $a \in \mathbb{Z}_p$, the integers modulo p.

(II) Equivalently $a^p \equiv a \pmod{p}$ for $a \in \mathbb{Z}$.

Exercise 5–16. Show that $\binom{p^a m}{p^a} = m\alpha$ where $\alpha \equiv 1 \pmod{p}$. If $p \nmid m$ this follows from Exercise 5–14(d). Otherwise it seems necessary to either expand the binomial coefficient or to check out what happens with a known group in the middle of Exercise 5–17.

Exercise 5–17 (The First Sylow Theorem). *Let G be a finite group of order $n = p^a m$ where $p \nmid m$ and let S be the set of all subsets of order p^b where $p^b \mid n$. Let G act on S by right multiplication and show that this actually is an action.*

Use the previous exercise to show that not every orbit has length divisible by p^{a-b+1}. Let $\mathcal{O}$ be one such nondivisible orbit and let T be one of the sets in $\mathcal{O}$. Show that G_T has order divisible by p^b. To finish let G_T act on the set T by right multiplication and use the left cancellation law to show $|G_T| \leqq p^b$ so that $St(T)$ is the desired subgroup.

Exercise 5–17.

(a) We now know that Alt(6) must have subgroups of order 1, 2, 4, 8, 3, 9, and 5. Write down explicitly one subgroup of each of these orders.

(b) Show that in any finite p-group the converse of Lagrange's Theorem is true.

Exercise 5–18. This proof of Sylow's Theorem is constructive in the sense that if the multiplication is known in a group the p-subgroups can be constructed. Try this for some group of very small order.

Exercise 5–19 (continued from Exercise 5–17). Show that p^{a-b+1} does not divide the orbit length of $\mathcal{O}$ if and only if $\mathcal{O}$ consists only of left cosets of subgroups of order p^b.

Exercise 5–20 (The 2nd Sylow Theorem). A group G of order $p^a m$ where $p \nmid m$ has $1 + kp$ subgroups of order p^a (which are called p-sylow subgroups). In fact the number of subgroups of order p^b is of the form $1 + kp$ for all $b \leqq a$.

Exercise 5–21 (The 3rd Sylow Theorem). The exercise is to fill in the details of the following argument. Let G be a finite group and let S be the set of all p-sylow subgroups of G. Assume that there are two distinct orbits $\mathcal{O}_1$ and $\mathcal{O}_2$ when G acts on S by conjugation. Let P_1 and P_2 be p-sylow subgroups, P_1 in $\mathcal{O}_1$, and P_2 in $\mathcal{O}_2$. If P_1 acts on $\mathcal{O}_2$ we see that $|\mathcal{O}|_2 = 0 \pmod p$ but P_2 acting on $\mathcal{O}_2$ yields $|\mathcal{O}|_2 = 1 \pmod p$. Thus G acting on S must have but one orbit and thus all the p-sylow subgroups of G are conjugate.

Exercise. 5–22 For each $p^n \,\Big|\, |P|$ where P is a finite p-group there are $1 + kp$ subgroups of order p^m.

Exercise 5–23. Show that the following 3 sets of matrices all with entries in Z_p are conjugate.

$$T_1 = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, \quad T_2 = \begin{bmatrix} 1 & e & 0 \\ 0 & 1 & 0 \\ f & g & 1 \end{bmatrix}, \quad T_3 = \begin{bmatrix} 1 & 0 & 0 \\ i & 1 & 0 \\ j & k & 1 \end{bmatrix}, \quad a,b,c,e,f,g,i,j,k \in \mathbb{Z}_p.$$

Exercise 5–24. If P is a p-sylow subgroup of a finite group G then the number of p-sylow subgroups in G is

$$\frac{|G|}{|N_G(P)|}.$$

Exercise 5–25. There are no simple groups of order 200.

Exercise 5–26. How many p-sylow subgroups are in $SL(2, \mathbb{Z}_p)$?

6. Exercises 6–1 and 6–2 are worth noting for anyone who has wanted to explain how modern algebra got its name (the algebra part) without explaining a substantial part of Galois Theory.

Exercise 6–1. If a and b are two elements of order 2 in a group G, then $\langle a, b\rangle$, the subgroup generated by a and b, is a dihedral group of order $2n$ where n is the order of the element ab.

We now want to examine the roots of polynomials over the rationals. If $f(x)$ is a polynomial of degree n it has at most n distinct roots in its splitting field, K. We are interested in Sym(n), the symmetric group on these n roots. In particular we are interested in two subsets of Sym(n), those elements that are in some way computable and the Galois group of K over $\mathbb{Q}$. Let us look at an example where there are a few computable elements of Sym(n) available.

Exercise 6–2. Is the polynomial $f(x) = x^8 + (x+1)^8 + 1$ irreducible? Hint: Note that $x \overset{a}{\to} 1/x$ and $x \overset{b}{\to} -1-x$ are elements permuting the 8 roots. (It can be shown that $f(x)$ has distinct roots by showing g.c.d. $(f(x), f'(x)) = 1$.)

[Use Exercise 6–1, some computations to find an element of order 3, Exercise 2–2, and the fact that complex roots of an equation with real coefficients come in complex pairs.]

Another interesting connection between computable elements and Galois groups is that if $x \xrightarrow{\alpha} \frac{ax+b}{cx+d}$ $(a,b,c,d \in \mathbb{Z})$ is a permutation of the roots of a polynomial, then α commutes with each element of the Galois group.

Exercise 6–3. Prove this assertion.

Exercise 6–4. Characterize those polynomials such that $x \xrightarrow{\alpha} 1/x$ permutes their roots.

Exercise 6–5. Show that $f(x) = \Sigma_{i=0}\, a_i x^i + \Sigma_{i=1}^{n}\, a_{n-i} x^{n+i}$ with $a_i \in \mathbb{Q}$ has a rational root. Hint: Use 2–2 and 6–4.

Exercise 6–6. Compute the centralizers of the following elements in Sym(n).
(a) $a = (123 \cdots n)$
(b) $b = (123)$
(c) $c = (12)(34) \cdots (n-1, n)$ where n is even.
Show that $C_{Sym(n)}(c)$ is solvable iff $n = 2, 4, 6$, or 8.

Exercise 6–7. Show that the polynomial

$$a_0(x^{2n} + 1) + a_1(x^{2n-1} + x) + a_2(x^{2n-2} + x^2) + \cdots + a_n x^n$$

is solvable by radicals if $n \leq 4$ where $a_i \in \mathbb{R}$.

References

1. E. Artin, Algebra I, Lecture notes in German from Universität Hamburg, 1961, pp. 9–14.

2. W. Burnside, Theory of Groups of Finite Order, 2nd ed., Dover, New York, 1955, pp. 189–191.

3. C. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience, New York, 1962, p. 17.

4. G. Frobenius, Gesammelte Abhandlungen II, Springer-Verlag, New York, 1968, p. 301.

5. D. Gorenstein, Finite Groups, Harper & Row, New York, 1968, p. 31.

6. F. Harary, Graph Theory, Addison-Wesley, Reading, 1969, pp. 178–197.

7. B. Huppert, Endliche Gruppen, Springer-Verlag, New York, 1969.

8. C. C. Liu, Introduction to Combinatorial Mathematics, McGraw-Hill, New York, 1968, pp. 126–166.

9. D. Passman, Permutation Groups, Benjamin, New York, 1968.

10. G. Polya, Kombinatorishe Anzahlbestimmungen für Gruppen, Graph und chemische Verbindungen, Acta Math., 68 (1937) 145–254.

11. C. H. Sah, Abstract Algebra, Academic Press, New York, 1967, pp. 54, 60, 79.

12. L. Sylow, Théorèmes sur les groupes de substitutions, Band V, (1872) 584–594.

13. H. Wielandt, Ein Beweis für den Existenz von Sylowgruppen, Arch. Math., 10 (1959) 401–402.