Proof. (i) The lemma shows that Hx is a block for every $x \in X$. Since X is primitive, either $Hx = \varnothing$ (plainly impossible), $Hx = \{x\}$, or $Hx = X$. If $Hx = \{x\}$ for some $x \in X$, then $H \leq G_x$. But if $g \in G$, then normality of H gives $H = gHg^{-1} \leq gG_xg^{-1} = G_{gx}$. Since X is transitive, $H \leq \bigcap_{y \in X} G_y = 1$, for X is faithful, and this is a contradiction. Therefore $Hx = X$ and X is a transitive H-set.

(ii) This follows from Theorem 9.2. ▩

Using this theorem, we see that the $\mathrm{GL}(V)$-set $V^{\#}$ in Example 9.4 is transitive but not primitive.

Corollary 9.18. *Let X be a faithful primitive G-set of degree n. If G is solvable, then $n = p^m$ for some prime divisor p of $|G|$; if G is nilpotent, then n is a prime divisor of $|G|$.*

Proof. If G is solvable, a minimal normal subgroup H of G is elementary abelian of order p^k, by Theorem 5.24. The theorem now gives n a divisor of p^k, and so n, too, is a power of p. If G is nilpotent, then G has a normal subgroup H of prime order p (e.g., take $H = \langle g \rangle$, where g is an element of order p in $Z(G)$). The theorem gives n a divisor of p; that is, $n = p$. ▩

EXERCISES

9.13. Let X be an imprimitive G-set and let B be a maximal nontrivial block of X; that is, B is not a proper subset of a nontrivial block. Show that the imprimitive system Y generated by B is a primitive G-set. Give an example with X faithful and Y not faithful.

9.14. (i) Let X be a transitive G-set, let $x \in X$, and let A be a nonempty subset of X. Show that the intersection of all gA containing x, where $g \in G$, is a block.
(ii) Let X be a primitive G-set and let A be a nonempty proper subset of X. If x and y are distinct elements of X, then there exists $g \in G$ with $x \in gA$ and $y \notin gA$. (*Hint.* The block in part (i) must be $\{x\}$.)

9.15. (i) Prove that if a group G has a faithful primitive G-set, then its Frattini subgroup $\Phi(G) = 1$.
(ii) Prove that a p-group G that is not elementary abelian has no faithful primitive G-set. (*Hint.* Theorem 5.47.)

Simplicity Criteria

We now prepare the way for new proofs showing that the alternating groups and the projective unimodular groups are almost always simple.

Definition. If X is a G-set and $H \lhd G$, then H is a ***regular normal subgroup*** if X is a regular H-set.

If H is a regular normal subgroup, then $|H| = |X|$. Thus, all regular normal subgroups have the same order.

Theorem 9.19. *Let X be a faithful primitive G-set with G_x a simple group. Then either G is simple or every nontrivial normal subgroup H of G is a regular normal subgroup.*

Proof. If $H \lhd G$ and $H \neq 1$, then Theorem 9.17(i) says that X is a transitive H-set. We have $H \cap G_x \lhd G_x$ for every $x \in X$, so that simplicity of G_x gives either $H \cap G_x = 1$ and X is regular or $H \cap G_x = G_x$; that is, $G_x \leq H$ for some $x \in X$. In the latter event, Theorem 9.15 gives G_x a maximal subgroup of G, so that either $G_x = H$ or $H = G$. The first case cannot occur because H acts transitively, so that $H = G$ and G is simple. ▩

It is proved in Burnside (1911), p. 202, Theorem XIII, that if a group G has a faithful doubly transitive G-set X whose degree is not a prime power, then either G is simple or G has a simple normal subgroup. (This result may be false when the degree is a prime power; S_4 is a counterexample.)

Here is the appropriate notion of homomorphism of G-sets.

Definition. If X and Y are G-sets, then a function $f: X \to Y$ is a ***G-map*** if $f(gx) = gf(x)$ for all $x \in X$ and $g \in G$; if f is also a bijection, then f is called a ***G-isomorphism.*** Two G-sets X and Y are ***isomorphic***, denoted by $X \cong Y$, if there is a G-isomorphism $f: X \to Y$.

By Theorem 9.1, every G-set X determines a homomorphism $\varphi: G \to S_X$. Usually there is no confusion in saying that X is a G-set and not displaying φ, but because we now wish to compare two G-sets, let us denote X more precisely by (X, φ). The action of $g \in G$ on $x \in X$ is now denoted by $\varphi_g x$ instead of by gx. The definition of G-map $f: (X, \varphi) \to (Y, \psi)$ now reads, for all $g \in G$ and $x \in X$, as

$$f(\varphi_g(x)) = \psi_g(f(x)).$$

EXAMPLE 9.5. Let G be a group, and let $\lambda, \rho: G \to S_G$ be the left and right regular representations of G (recall that $\lambda_g: x \mapsto gx$ and $\rho_g: x \mapsto xg^{-1}$ for all $x, g \in G$). We claim that (G, λ) and (G, ρ) are isomorphic G-sets. Define $f: G \to G$ by $f(x) = x^{-1}$; clearly f is a bijection. Let us see that f is a G-map.

$$f(\lambda_g(x)) = f(gx) = x^{-1}g^{-1} = f(x)g^{-1} = \rho_g(f(x)).$$

EXAMPLE 9.6. *Chinese Remainder Theorem.*

If $S \leq G$ is any (not necessarily normal) subgroup, we denote the family of all left cosets of S in G by G/S; it is a G-set with action $g(xS) = (gx)S$ (as in Theorem 3.12). If X and Y are G-sets, then their cartesian product $X \times Y$ may be regarded as a G-set with ***diagonal action***: $g(x, y) = (gx, gy)$.

If G is a (finite) group and $H, K \leq G$ are such that $HK = G$, then there is a G-isomorphism $f\colon G/(H \cap K) \tilde{\to} (G/H) \times (G/K)$, where the latter has diagonal action. Define f by $x(H \cap K) \mapsto (xH, xK)$. It is straightforward to show that f is a well defined injective G-map. Since $HK = G$, the product formula $|HK||H \cap K| = |H||K|$ gives $|G|/|H||K| = 1/|H \cap K|$; multiplying both sides by $|G|$ gives $[G:H][G:K] = [G:H \cap K]$, and so f must be surjective as well. Therefore, f is a G-isomorphism.

Theorem 9.20. *Every transitive G-set X is isomorphic to the G-set G/G_x of all left cosets of G_x on which G acts by left multiplication.*

Proof. Let $X = \{x_1, \ldots, x_n\}$, let $H = G_{x_1}$, and, for each i, choose $g_i \in G$ with $g_i x_1 = x_i$ (which is possible because X is transitive). The routine argument that $f\colon X \to G/H$, given by $f(x_i) = g_i H$, is a well defined bijection is left to the reader (recall that $n = |\mathcal{O}(x_1)| = [G:H]$). To check that f is a G-map, note that if $g \in G$, then for all i there is j with $gx_i = x_j$, and so

$$f(gx_i) = f(x_j) = g_j H.$$

On the other hand,

$$gf(x_i) = gg_i H.$$

But $gg_i x_1 = gx_i = x_j = g_j x_1$; hence $g_j^{-1} g g_i \in G_{x_1} = H$, and so $g_j H = g g_i H$, as desired. ▩

Theorem 9.21.

(i) *If $H, K \leq G$, then the G-sets G/H and G/K (with G acting by left multiplication) are isomorphic if and only if H and K are conjugate in G.*
(ii) *Two transitive G-sets (X, φ) and (Y, ψ) are isomorphic if and only if stabilizers of points in each are conjugate in G.*

Proof. (i) Assume that there is a G-isomorphism $f\colon G/H \to G/K$. In particular, there is $g \in G$ with $f(H) = gK$. If $h \in H$, then

$$gK = f(H) = f(hH) = hf(H) = hgK.$$

Therefore, $g^{-1}hg \in K$ and $g^{-1}Hg \leq K$. Now $f(g^{-1}H) = g^{-1}f(H) = g^{-1}gK = K$ gives $f^{-1}(K) = g^{-1}H$. The above argument, using f^{-1} instead of f, gives the reverse inclusion $gKg^{-1} \leq H$.

Conversely, if $g^{-1}Hg = K$, define $f\colon G/H \to G/K$ by $f(aH) = agK$. It is routine to check that f is a well defined G-isomorphism.

(ii) Let H and K be stabilizers of points in (X, φ) and (Y, ψ), respectively. By Theorem 9.20, $(X, \varphi) \cong G/H$ and $(Y, \psi) \cong G/K$. The result now follows from part (i). ▩

Corollary 9.22. *If G is solvable, then every maximal subgroup has index a prime power; if G is nilpotent, then every maximal subgroup has prime index.*

Remark. The second statement was proved in Theorem 5.40.

Proof. If $H \leq G$, then the stabilizer of the point $\{H\}$ in the transitive G-set G/H is the subgroup H. If H is a maximal subgroup of G, then G/H is a primitive G-set, by Theorem 9.15, and so $|G/H| = [G:H]$ is a prime power, by Corollary 9.18. A similar argument gives the result when G is nilpotent. ▩

Lemma 9.23. *Let X be a transitive G-set and let H be a regular normal subgroup of G. Choose $x \in X$ and let G_x act on $H^\#$ by conjugation. Then the G_x-sets $H^\#$ and $X - \{x\}$ are isomorphic.*

Proof. Define $f\colon H^\# \to X - \{x\}$ by $f(h) = hx$ (notice that $hx \neq x$ because H is regular). If $f(h) = f(k)$, then $h^{-1}k \in H_x = 1$ (by regularity), and so f is injective. Now $|X| = |H|$ (regularity again), $|H^\#| = |X - \{x\}|$, and so f is surjective. It remains to show that f is a G_x-map. If $g \in G_x$ and $h \in H^\#$, denote the action of g on h by $g * h = ghg^{-1}$. Therefore,

$$f(g * h) = f(ghg^{-1}) = ghg^{-1}x = ghx,$$

because $g^{-1} \in G_x$; on the other hand, $g \cdot f(h) = g(hx)$, and so $f(g * h) = g \cdot f(h)$. ▩

Lemma 9.24. *Let $k \geq 2$ and let X be a k-transitive G-set of degree n. If G has a regular normal subgroup H, then $k \leq 4$. Moreover:*

(i) *if $k \geq 2$, then H is an elementary abelian p-group for some prime p and n is a power of p;*
(ii) *if $k \geq 3$, then either $H \cong \mathbb{Z}_3$ and $n = 3$ or H is an elementary abelian 2-group and n is a power of 2; and*
(iii) *if $k \geq 4$, then $H \cong \mathbf{V}$ and $n = 4$.*

Proof. By Lemma 9.5, the G_x-set $X - \{x\}$ is $(k-1)$-transitive for each fixed $x \in X$; by Lemma 9.23, $H^\#$ is a $(k-1)$-transitive G_x-set, where G_x acts by conjugation.

(i) Since $k \geq 2$, $H^\#$ is a transitive G_x-set. The stabilizer G_x acts by conjugation, which is an automorphism, so that all the elements of $H^\#$ have the same (necessarily prime) order p, and H is a group of exponent p. Now $Z(H) \lhd G$, because $Z(H)$ is a nontrivial characteristic subgroup, so that $|X| = |Z(H)| = |H|$, for $Z(H)$ and H are regular normal subgroups of G'. Therefore, $Z(H) = H$, H is elementary abelian, and $|X|$ is a power of p.

(ii) If $h \in H^\#$, then it is easy to see that $\{h, h^{-1}\}$ is a block. If $k \geq 3$, then $H^\#$ is a doubly transitive, hence primitive, G_x-set, so that either $\{h, h^{-1}\} = H^\#$ or $\{h, h^{-1}\} = \{h\}$. In the first case, $|H| = 3$, $H \cong \mathbb{Z}_3$, and $n = 3$. In the second case, h has order 2, and so the prime p in part (i) must be 2.

(iii) If $k \geq 4$, $k - 1 \geq 3$ and $|H^\#| \geq 3$; it follows that both $H \cong \mathbb{Z}_3$ and $H \cong \mathbb{Z}_2$ are excluded. Therefore, H contains a copy of $\mathbf{V}$; say, $\{1, h, k, hk\}$.

Now $(G_x)_h$ acts doubly transitively, hence primitively, on $H^\# - \{h\}$. It is easy to see, however, that $\{k, hk\}$ is now a block, and so $H^\# - \{h\} = \{k, hk\}$. We conclude that $H = \{1, h, k, hk\} \cong \mathrm{V}$ and $n = 4$.

Finally, we cannot have $k \geq 5$ because $n \leq 4$. ▩

Of course, the case $k = 4$ does occur ($G = S_4$ and $H = \mathrm{V}$). Compare the case $k = 2$ with Theorem 9.11.

Theorem 9.25. *Let X be a faithful k-transitive G-set, where $k \geq 2$, and assume that G_x is simple for some $x \in X$.*

(i) *If $k \geq 4$, then G is simple.*
(ii) *If $k \geq 3$ and $|X|$ is not a power of 2, then either $G \cong S_3$ or G is simple.*
(iii) *If $k \geq 2$ and $|X|$ is not a prime power, then G is simple.*

Proof. By Theorem 9.19, either G is simple or G has a regular normal subgroup H. In the latter case, Lemma 9.24 gives $k \leq 4$; moreover, if $k = 4$, then $H \cong \mathrm{V}$ and $|X| = 4$. Now the only 4-transitive subgroup of S_4 is S_4 itself, but the stabilizer of a point is the nonsimple group S_3. Therefore, no such H exists, and so G must be simple. The other two cases are also easy consequences of the lemma (note that the stabilizer of a point of an S_3-set is the simple group $S_2 \cong \mathbb{Z}_2$ so that S_3 is a genuine exception in part (ii)). ▩

Here is another proof of the simplicity of the large alternating groups.

Theorem 9.26. *A_n is simple for all $n \geq 5$.*

Proof. The proof is by induction on $n \geq 5$. If $n = 5$, then the result is Lemma 3.8. By Theorem 9.9, A_n acts $(n-2)$-transitively on $X = \{1, 2, \ldots, n\}$; hence, if $n \geq 6$, then A_n acts k-transitively, where $k \geq 4$. The stabilizer $(A_n)_n$ of n is just A_{n-1} (for it consists of all the even permutations of $\{1, \ldots, n-1\}$), and so it is simple, by induction. Therefore, A_n is simple, by Theorem 9.25(i). ▩

Here is another simplicity criterion. It shall be used later to give another proof of the simplicity of the PSLs.

Theorem 9.27 (Iwasawa, 1941). *Let $G = G'$ (such a group is called **perfect**) and let X be a faithful primitive G-set. If there is $x \in X$ and an abelian normal subgroup $K \lhd G_x$ whose conjugates $\{gKg^{-1} : g \in G\}$ generate G, then G is simple.*

Proof. Let $H \neq 1$ be a normal subgroup of G. By Theorem 9.17, H acts transitively on X. By hypothesis, each $g \in G$ has the form $g = \prod g_i k_i g_i^{-1}$, where $g_i \in G$ and $k_i \in K$. Now $G = HG_x$, by Exercise 4.9(i), so that $g_i = h_i s_i$ for each i, where $h_i \in H$ and $s_i \in G_x$. Normality of K in G_x now gives

$$g = \prod h_i s_i k_i s_i^{-1} h_i^{-1} \in HKH \leq HK$$

(because H lies in the subgroup HK), and so $G = HK$. Since K is abelian, $G/H = HK/H \cong K/(H \cap K)$ is abelian, and $H \geq G' = G$. Therefore, G is simple. ▩

EXERCISES

9.16. If X is a G-set, let $\mathrm{Aut}(X)$ be the group of all G-isomorphisms of X with itself. Prove that if X is a transitive G-set and $x \in X$, then $\mathrm{Aut}(X) \cong N_G(G_x)/G_x$. (*Hint.* If $\varphi \in \mathrm{Aut}(X)$, there is $g \in G$ with $gx = \varphi(x)$; the desired isomorphism is $\varphi \mapsto g^{-1}G_x$.)

9.17. Let X be a transitive G-set, and let $x, y \in X$. Prove that $G_x = G_y$ if and only if there is $\varphi \in \mathrm{Aut}(X)$ with $\varphi(x) = y$.

Affine Geometry

All vector spaces in this section are assumed to be finite-dimensional.

Theorem 9.28. *If V is an n-dimensional vector space over a field K, then $V^\# = V - \{0\}$ is a transitive $\mathrm{GL}(V)$-set that is regular when $n = 1$. If $n \geq 2$, then $V^\#$ is doubly transitive if and only if $K = \mathbb{Z}_2$.*

Proof. $\mathrm{GL}(V)$ acts transitively on $V^\#$, for every nonzero vector is part of a basis and $\mathrm{GL}(V)$ acts transitively on the set of all ordered bases of V. If $n = 1$, only the identity can fix a nonzero vector, and so $V^\# = K^\times$ is regular.

Assume that $n \geq 2$, and that $\{y, z\}$ is a linearly independent subset. If $K \neq \mathbb{Z}_2$, there exists $\lambda \in K$ with $\lambda \neq 0, 1$; if $x \in V^\#$, then $\{x, \lambda x\}$ is a linearly dependent set, and there is no $g \in G$ with $gx = y$ and $g\lambda x = z$. Therefore, $\mathrm{GL}(V)$ does not act doubly transitively in this case. If $K = \mathbb{Z}_2$, then every pair of distinct nonzero vectors is linearly independent, hence is part of a basis, and double transitivity follows from $\mathrm{GL}(V)$ acting transitively on the set of all ordered bases of V. ▩

Definition. If V is a vector space and $y \in V$, then ***translation by y*** is the function $t_y : V \to V$ defined by

$$t_y(x) = x + y$$

for all $x \in V$. Let $\mathrm{Tr}(V)$ denote the group of all translations under composition (we may also write $\mathrm{Tr}(n, K)$ or $\mathrm{Tr}(n, q)$).

Definition. If V is a vector space over K, then the ***affine group***, denoted by $\mathrm{Aff}(V)$, is the group (under composition) of all functions $a : V \to V$ (called ***affinities***) for which there is $y \in V$ and $g \in \mathrm{GL}(V)$ such that

$$a(x) = gx + y$$