Math. Z. 110, 213–217 (1969)

A Characterisation of Solvable Groups

ANDREAS DRESS

Introduction

Let G be a finite group. A G-set M is a finite set on which G operates from the left by permutations, i.e. a finite set together with a map $G \times M \to M$, $(g, m) \mapsto g\,m$ with $g(h\,m) = (g\,h)\,m$, $e\,m = m$ for $g, h, e \in G$, $m \in M$ and e the neutral element. With M and N a G-set the disjoint union $M \dot{+} N$ and the cartesian product $M \times N$ are in a natural way G-sets, too. This way the equivalence classes of isomorphic G-sets form a commutative halfring. Let $\Omega(G)$ be the associated ring. The following note is to prove that G is solvable if and only if the prime ideal spectrum $\mathrm{Spec}(\Omega(G))$ of $\Omega(G)$ is connected in the Zariski topology, i.e. if and only if 0 and 1 are the only idempotents in $\Omega(G)$.

The Additive Structure of $\Omega(G)$

Let T be a G-set. Then the following three statements are equivalent:

(i) G operates transitive on T, i.e. for $m, n \in T$ exists $g \in G$ with $g\,m = n$.

(ii) Any G-homomorphism of a G-set N into T is epimorphic[1].

(iii) There exists $U \leqq G$ with $G/U \cong T$.

We call such a G-set *transitive*.

Any G-set is in a unique way the disjoint union of transitive G-sets. This means

(1) $\Omega(G)$ is a free Z-module with basis the set $\mathfrak{T} \subseteq \Omega(G)$ of all elements in $\Omega(G)$ represented by transitive G-sets.

(2) Two G-sets are isomorphic if and only if they represent the same element in $\Omega(G)$.

We therefore identify a G-set M with the element in $\Omega(G)$ represented by M.

For $T \in \mathfrak{T}$ let $\tilde{T}$ be the uniquely defined class of conjugate subgroups $U \leqq G$ with $T \cong G/U$. For $S, T \in \mathfrak{T}$ we write $S \prec T$ if there exists a G-homomorphism $S \to T$ (or equivalently if any group in $\tilde{T}$ contains a group in $\tilde{S}$).

This relation is obviously transitive and because any G-homomorphism $M \to T$ for $T \in \mathfrak{T}$ is epimorphic, we also have: $S \prec T$ and $T \prec S$ if and only if $T = S$.

For $U \leqq G$ we write $\tilde{U}$ for the set of subgroups, conjugate to U and U for the element G/U in $\Omega(G)$. For $U, V \leqq G$ we write $U \sim V$ if U is conjugate to V

1. It is perhaps interesting to observe, that dually G operates primitive on a G-set M if and only if G acts non-trivial on M and any G-homomorphism $M \to N$ into any G-set N is either injective or sends M into just one (G-invariant) element.

and $U \lesssim V$ if U is conjugate to a subgroup of V. One has:

(3) $\quad U \in \mathfrak{T}; \quad (\tilde{U}) = \tilde{U}; \quad U \sim V \Leftrightarrow \tilde{U} = \tilde{V} \Leftrightarrow \boldsymbol{U} = \boldsymbol{V}; \quad U \lesssim V \Leftrightarrow \boldsymbol{U} \prec \boldsymbol{V}.$

Finally if we write for $S, T \in \mathfrak{T}$ the product $S \cdot T$ in the form $\sum_{R \in \mathfrak{T}} a_R R$, then $a_R \neq 0$ implies $R \prec S$, $R \prec T$ because for $a_R \neq 0$, i.e. $R \subseteq S \times T$ the projections $S \times T \to T$, $S \times T \to S$ imply the existence of maps of R into S and T. (More exactly for $S = \boldsymbol{U}$, $T = \boldsymbol{V}$ and $R = \boldsymbol{W}$ the number a_R equals the number of double cosets $U g V$ $(g \in G)$ with $W \sim U \cap V^g$.)

The Symbol $\langle U, M \rangle$

For a subgroup $U \leqq G$ and a G-set M we write $\langle U, M \rangle$ for the number of elements in M, invariant under U: $\langle U, M \rangle = \# M^U$.

This symbol has the following properties:

(4) $$\langle U, M \dotplus N \rangle = \langle U, M \rangle + \langle U, N \rangle,$$

(5) $$\langle U, M \times N \rangle = \langle U, M \rangle \langle U, N \rangle.$$

(6) For $T \in \mathfrak{T}$ we have

$$\langle U, T \rangle \neq 0 \Leftrightarrow \boldsymbol{U} \prec T \Leftrightarrow U \lesssim V \qquad \text{for } V \in \tilde{T}.$$

(7) $\langle U, \boldsymbol{U} \rangle = (N_G(U) \colon U)$.

Obviously (6) implies $\langle U, M \rangle = \langle V, M \rangle$ for all M if and only if $U \sim V$ (take $M = \boldsymbol{U}$ and $M = \boldsymbol{V}$).

But one has also:

Lemma 1. *Two G-sets M and N are isomorphic if and only if $\langle U, M \rangle = \langle U, N \rangle$ for all $U \leqq G$.*

Proof. Obviously $M \cong N$ implies $\langle U, N \rangle = \langle U, M \rangle$ for all $U \leqq G$.

On the other hand assume $M \neq N$. If $M = \sum_{T \in \mathfrak{T}} m_T T$, $N = \sum_{T \in \mathfrak{T}} n_T T$ there exists then a biggest $S \in \mathfrak{T}$ with $m_S \neq n_S$. We may assume $m_T = n_T = 0$ for all $T \succneqq S$. But then (4) and (6) implies for $U \in \tilde{S}$, i.e. $\boldsymbol{U} = S$:

$$\langle U, M \rangle = m_S \langle U, S \rangle \neq n_S \langle U, S \rangle = \langle U, N \rangle.$$

Furthermore we have the following formula:

(8) $$U \leqq G, M \ G\text{-set:} \ \boldsymbol{U} \cdot M = \langle U, M \rangle \boldsymbol{U} + \sum_{T \precneqq \boldsymbol{U}} m_T T.$$

Proof. Assume $\boldsymbol{U} \cdot M = \sum m_T T$. Obviously $m_T \neq 0$ implies again $T \prec \boldsymbol{U}$. So it remains to compute $m_{\boldsymbol{U}}$. But we have:

$$\langle U, \boldsymbol{U} M \rangle = \langle U, \boldsymbol{U} \rangle \cdot \langle U, M \rangle = \sum m_T \langle U, T \rangle$$
$$= m_{\boldsymbol{U}} \langle U, \boldsymbol{U} \rangle \Rightarrow \langle U, M \rangle = m_{\boldsymbol{U}}. \qquad \text{q.e.d.}$$

As another corollary of the properties (4)–(7) we have the following remark: Let $U, V \leqq G$, $W = U \cap V$. If $(N_G(W): W)$ does not divide $\langle W, U\rangle \langle W, V\rangle$, then there exists $g, h \in G$ with $W \subsetneqq U^g \cap V^h$.
Because otherwise with $U \cdot V = \sum m_T T$ we have $\langle W, U \cdot V\rangle = \langle W, U\rangle \langle W, V\rangle = \sum m_T \langle W, T\rangle = m_W \langle W, W\rangle$, which would imply:

$$(N_G(W):\ W) = \langle W, W\rangle \,|\, \langle W, U\rangle \langle W, V\rangle .$$

Prime Ideals in $\Omega(G)$

Because of (4) and (5) the map $M \mapsto \langle U, M\rangle$ extends to a ring homomorphism $\langle U, \cdot\rangle: \Omega(G) \to Z$. Define for p being 0 or a prime number $\mathfrak{p}_{U,p} = \{x \in \Omega(G) | \langle U, x\rangle \equiv 0 \bmod p\}$. Obviously $\mathfrak{p}_{U,p}$ is a prime ideal in $\Omega(G)$. We are going to prove, that any prime-ideal in $\Omega(G)$ is actually of this form. More exactly we have

Proposition 1. (a) *Let $\mathfrak{p}$ be a prime ideal in $\Omega(G)$. Then the set $\mathfrak{T} - (\mathfrak{T} \cap \mathfrak{p})$ contains exactly one minimal element $T_\mathfrak{p}$ and for $U \in \tilde{T}_\mathfrak{p}$ and $p = \operatorname{char} \Omega(G)/\mathfrak{p}$ one has $\mathfrak{p} = \mathfrak{p}_{U,p}$.*

(b) *One has $\mathfrak{p}_{U,p} \subseteq \mathfrak{p}_{V,q}$ if and only if $p = q$ and $\mathfrak{p}_{U,p} = \mathfrak{p}_{V,q}$ or $p = 0$, $q \neq 0$ and $\mathfrak{p}_{U,q} = \mathfrak{p}_{V,q}$. Especially $\mathfrak{p}_{U,p}$ is minimal, resp. maximal, if and only if $p = 0$, resp. $p \neq 0$.*

(c) *In case $p = 0$ one has $\mathfrak{p}_{U,0} = \mathfrak{p}_{V,0}$ if and only if $U \sim V$. One has further: $\mathfrak{T} - (\mathfrak{T} \cap \mathfrak{p}_{U,0}) = \{T \in \mathfrak{T} | U \prec T\}$, especially $T_{\mathfrak{p}_{U,0}} = U$.*

(d) *In case $p \neq 0$ one has $\mathfrak{p}_{U,p} = \mathfrak{p}_{V,p}$ if and only if $U^p \sim V^p$, where for a group U the subgroup U^p is the (well defined!) smallest normal subgroup of U with U/U^p a p-group. In this case one has for $\mathfrak{p} = \mathfrak{p}_{U,p}$: $T_\mathfrak{p} = U_p$, where U_p is the preimage in $N_G(U^p)$ of any p-Sylow subgroup in $N_G(U^p)/U^p$.*

Proof. (a) If S and $T \in \mathfrak{T}$ are both minimal in $\mathfrak{T} - (\mathfrak{T} \cap \mathfrak{p})$, then

$$S \cdot T = \sum_{R \prec S, T} n_R R \notin \mathfrak{p},$$

therefore $R \notin \mathfrak{p}$ for at least one $R \prec S, T$ and then $R = S = T$. Furthermore for $T = U$ we have by an obvious extension of (8) to any element $x \in \Omega(G)$:

$$T \cdot x = \langle U, x\rangle T + \sum_{\substack{R \in \mathfrak{T} \\ R \lneqq T}} m_R R \equiv \langle U, x\rangle T \bmod \mathfrak{p}$$

which implies:

$$x \in \mathfrak{p} \Leftrightarrow \langle U, x\rangle \equiv 0 \bmod \operatorname{char} \Omega(G)/\mathfrak{p} \Leftrightarrow x \in \mathfrak{p}_{U,p} \qquad \text{for } p = \operatorname{char} \Omega(G)/\mathfrak{p}.$$

(b) Obviously any prime ideal containing $\mathfrak{p}_{U,0}$ is of the form $\mathfrak{p}_{U,p}$ and any prime ideal containing $\mathfrak{p}_{U,p}$ for $p \neq 0$ is equal to $\mathfrak{p}_{U,p}$, because $\mathfrak{p}_{U,p}$ is maximal.

(c) It is enough to prove $\mathfrak{T} - (\mathfrak{T} \cap \mathfrak{p}_{U,0}) = \{T \in \mathfrak{T} | U \prec T\}$, but this is just a restatement of (6).

(d) If $W \trianglelefteq U$ and U/W a p-group, then obviously $\langle U, M\rangle \equiv \langle W, M\rangle \bmod p$ for all M because $M^U \subseteq M^W$, M^W is U-invariant and $M^W - M^U$ is a disjoint union of nontrivial U/W-orbits. Therefore $U^p \sim V^p$ implies $\langle U, M\rangle \equiv \langle U^p, M\rangle = \langle V^p, M\rangle \equiv \langle V, M\rangle \bmod p$, i.e. $\mathfrak{p}_{U,p} = \mathfrak{p}_{V,p}$.

Now assume $\mathfrak{p}_{U,p} = \mathfrak{p}_{V,p} = \mathfrak{p}$ and $T = T_\mathfrak{p}$.

Obviously $T = W$ if and only if $\langle U, M\rangle \equiv \langle W, M\rangle \bmod p$ for all M and $\langle U, W\rangle \equiv \langle W, W\rangle = (N_G(W): W) \not\equiv 0 \bmod p$. But this is just the case for the preimage U_p of any p-Sylow subgroup of $N_G(U^p)/U^p$ because $U^p = (U_p)^p$ is characteristic in U_p, therefore $N_G(U_p) \subseteq N_G(U^p)$ and a fortiori $p \nmid (N_G(U_p): U_p)$ and on the other hand $\langle U, M\rangle \equiv \langle U^p, M\rangle \equiv \langle U_p, M\rangle \bmod p$. Therefore $\mathfrak{p}_{U,p} = \mathfrak{p}_{V,p}$ implies $U_p \sim V_p$ and then $(U_p)^p = U^p \sim (V_p)^p = V^p$. q.e.d.

We can now prove the final result. To put it a little bit more general, we define for a finite group U the subgroup U^s to be the (well defined!) minimal normal subgroup of U with U/U^s solvable. Then we have

Proposition 2. *Two prime ideals $\mathfrak{p}_{U,p}$ and $\mathfrak{p}_{V,q}$ are in the same connected component of* $\operatorname{Spec}(\Omega(G))$ *if and only if $U^s \sim V^s$. The connected components of* $\operatorname{Spec}(\Omega(G))$ *are therefore in a one-one correspondence with the classes of conjugate subgroups $U \leqq G$ with $U = [U, U]$. The number of minimal primes in the connected component of $\mathfrak{p}_{U,p}$ equals the number of classes of conjugate subgroups $V \leqq G$ with $V^s \sim U^s$.*

Proof. It is enough to prove the first statement. Let A be a noetherian ring. For any prime ideal $\mathfrak{p} \in \operatorname{Spec} A$ let $\bar{\mathfrak{p}} = \{\mathfrak{q} \mid \mathfrak{q} \in \operatorname{Spec} A, \mathfrak{p} \subseteq \mathfrak{q}\}$ be the closure of $\mathfrak{p}$ in $\operatorname{Spec} A$. Then two prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ are in the same connected component of $\operatorname{Spec} A$, if and only if there exists a series of minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ with $\mathfrak{p} \in \bar{\mathfrak{p}}_1$, $\mathfrak{q} \in \bar{\mathfrak{p}}_n$, $\bar{\mathfrak{p}}_i \cap \bar{\mathfrak{p}}_{i+1} \neq \emptyset$ $(i = 1, \dots, n-1)$. But for $A = \Omega(G)$ we have $\bar{\mathfrak{p}}_{U,0} \cap \bar{\mathfrak{p}}_{V,0} \neq \emptyset$ if and only if $U^p \sim V^p$ for some p, which implies $U^s = (U^p)^s \sim (V^p)^s = V^s$.

Therefore if $\mathfrak{p}_{U,p}$ and $\mathfrak{p}_{V,q}$ are in the same connected component of $\operatorname{Spec} \Omega(G)$, we have $U^s \sim V^s$.

On the other hand $\mathfrak{p}_{U,p}$ and $\mathfrak{p}_{U^s,0}$ always are in the same connected component, because we can find a series of normal subgroups of U: $U = {}_0U \rhd {}_1U \rhd {}_2U \rhd \cdots \rhd {}_nU = U^s$ with ${}_{i-1}U/{}_iU$ a p_i-group for some prime p_i $(i = 1, \dots, n)$, which implies:

$$\mathfrak{p}_{U,p} \in \bar{\mathfrak{p}}_{{}_0U,0}; \quad \bar{\mathfrak{p}}_{{}_{i-1}U,0} \cap \bar{\mathfrak{p}}_{{}_iU,0} \neq \emptyset \qquad \text{for } i = 1, \dots, n. \qquad \text{q.e.d.}$$

Proposition 2 yields obviously the wanted characterisation of solvable groups. As another corollary one gets: G is minimal simple if and only if $\Omega(G) \cong \mathbb{Z} \oplus \Omega'(G)$ for some $\Omega'(G)$ with spec $\Omega'(G)$ connected.

One also has the obvious generalisation:

Let π be a set of prime numbers. Define $Z_\pi \subseteq Q$ to be the subring of the rationals, containing all rational numbers with denominators prime to π: $\mathbb{Z}_\pi = \mathbb{Z}[p^{-1} \mid p \notin \pi]$ and define for a group U the subgroup U^π to be the smallest normal subgroup of U with U/U^{π} a solvable π-group. Then the connected components of Spec $\Omega_{\pi}(G)$ with $\Omega_{\pi}(G)=\Omega(G)\otimes_{\mathbb{Z}}\mathbb{Z}_{\pi}$ are in $1-1$ correspondence with the classes of conjugate subgroups $U \leqq G$ with $U=U^{\pi}$, i.e. $(U: [U, U])$ π-prime. Especially Spec $\Omega_{\pi}(G)$ is connected if and only if G is a solvable π-group and $\Omega_p(G)$ is a local ring if and only if G is a p-group. In general $\Omega_p(G)$ is a direct product of local rings, isomorphic to a ring of the form $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ if and only if p does not divide the order of G.

Dr. Andreas Dress
The Institute for Advanced Study
Princeton, New Jersey 08540, USA

(Received October 14, 1968)