9

An Introduction to Crowns in Finite Groups

Gareth Tracey

Notation and Conventions

The following is a list of notation and conventions that will be used throughout the chapter. In what follows, G is a group.

- The notation $H \leq G$ means that H is a subgroup of G; while $H \trianglelefteq G$ means that H is a normal subgroup of G.
- For a subgroup H of G, $H\backslash G$ denotes the set of right cosets of H in G.
- $C_G(H)$ denotes the centraliser of the subgroup H in G.
- $Z(G)$ denotes the centre of G, while $\Phi(G)$ denotes the Frattini subgroup of G (see Definition 9.9).
- $\mathrm{Aut}(G)$ denotes the automorphism group of G.
- For elements x and g of G, we write $x^g = g^{-1}xg$.
- More generally, group actions will always be written on the right. So if the group G acts on the set Ω, we will write ω^g for the image of $\omega \in \Omega$ under the action of $g \in G$.
- For a positive integer k, we will write G^k for the direct product of k copies of G. That is, G^k is the group which, as a set, is the cartesian product of k copies of G, equipped with pointwise multiplication.
- $\mathrm{core}_G(H) := \bigcap_{g \in G} H^g$ denotes the *core* of the subgroup H in G (i.e. the largest normal subgroup of G contained in H).
- We will write Z_n for the cyclic group of order n, and $\mathbb{F}_p$ for the finite field of order p, for p prime.
- Alt_n and Sym_n will denote the alternating and symmetric groups of degree n, respectively.
- We will write $\mathrm{SL}_n(\mathbb{F})$ and $\mathrm{GL}_n(\mathbb{F})$ for the special and general linear groups of dimension n over the field $\mathbb{F}$.
- Abelian groups will always be written multiplicatively.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

- The term *minimal normal subgroup* will always refer to a non-trivial minimal normal subgroup.
- If $f\colon X \to Y$ is a map between sets X and Y, and $A \subseteq X$, we will write $f\downarrow_A$ for the restriction of f to A.

9.1 An Introduction to the Theory of Crowns

Roughly speaking, crowns are certain quotients of finite groups which have a "large" normal subgroup isomorphic to a direct product of simple groups. In order to define crowns rigorously, a number of basic notions from group and representation theory are required. In this section, we note the definitions and results necessary. We then conclude (see Subsection 9.1.3) by defining an equivalence relation on the set of chief factors of a finite group. This will set us up to define and study the notion of a crown (see Section 9.2).

9.1.1 Chief Factors in Finite Groups

Recall that for finite groups G and H, $H \leq G$ means that H is a subgroup of G, and $H \trianglelefteq G$ means that H is a normal subgroup of G. We begin by defining sections and normal sections in G.

Definition 9.1 Let G be a finite group. A *section* of G is a group X/Y, where $X, Y \leq G$ with $Y \trianglelefteq X$. If X and Y are both normal in G, then we say that X/Y is a *normal section* of G.

Thus, the composition factors in a finite group G are all sections of G, but are not necessarily normal sections. To study crowns in finite groups, we will be interested in the normal sections in G, and specifically the "minimal normal sections". These are called the chief factors of G, and their formal definition is as follows:

Definition 9.2 Let G be a finite group. A *chief factor* of G is a normal section X/Y of G with the property that if $Y \leq Z \leq X$ with $Z \trianglelefteq G$, then either $Z = X$ or $Z = Y$.

The most common (and some of the most important) examples of chief factors of a finite group G are the minimal normal subgroups of G. That is, those normal subgroups N of G with the property that if $Z \leq N$ with $Z \trianglelefteq G$, then $Z = 1$ or $Z = N$. These can be seen as chief factors of G by taking $Y := 1$ and $X := N$ in Definition 9.2. These groups are particularly important for inductive arguments in finite group theory, and they have a very particular structure:

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Lemma 9.3 *Let G be a finite group, and let N be a minimal normal subgroup of G. Then $N \cong S^t$ is isomorphic to a direct product of t copies of a finite simple group S.*

Proof We prove the lemma by induction on $|G|$. The socle $\mathrm{soc}(X)$ of a finite group X is the product of its minimal normal subgroups, and is clearly a non-trivial characteristic subgroup of X. Thus, $\mathrm{soc}(N)$, being characteristic in $N \trianglelefteq G$, is normal in G. Hence, $\mathrm{soc}(N) = N$, since N is a minimal normal subgroup of G.

Now, let N_1 be a minimal normal subgroup of N. Then $\prod_{g\in G} N_1^g$ is a normal subgroup of G contained in N, so must be equal to N, by the minimality of N (we caution the reader that the product $\prod_{g\in G} N_1^g$ here is not necessarily a direct product). Choose a set $\{N_1, \ldots, N_r\}$ of G-conjugates N_i of N_1 which is minimal with the property that $N = \prod_{i=1}^r N_i$. Then $N_i \not\leq \prod_{j\neq i} N_j$, for each i. Since N_i is a minimal normal subgroup of N, it follows that N_i intersects $\prod_{j\neq i} N_j$ trivially, for each i. Hence $N = N_1 \times \ldots \times N_r$. If $N = G$, then G is simple, and the result follows. So assume that $N < G$. Then the inductive hypothesis implies that each N_i is a direct product of isomorphic simple groups: $N_i \cong T_i^{k_i}$. But all N_i are G-conjugate, so $T_i \cong T_j$ for all i, j. This completes the proof. □

Since a chief factor X/Y of G is a minimal normal subgroup of G/Y, the following is immediate.

Corollary 9.4 *Let G be a finite group, and let X/Y be a chief factor of G. Then $X/Y \cong S^t$ is isomorphic to a direct product of t copies of a finite simple group S.*

We finish this section by noting that one can inductively define a series of subgroups of a finite group G as follows: Set $X_0 := 1$, and for $i \geqslant 1$, let X_i/X_{i-1} be a minimal normal subgroup of the group G/X_{i-1}. We then have a series:

$$1 = X_0 < X_1 < \ldots < X_t = G. \tag{9.1.1}$$

This is a so-called *normal series* (i.e. every group X_i in the series is normal in G, not just in X_{i+1}).

Definition 9.5 Let G be a finite group. A series (9.1.1) in G is called a chief series for G.

Like a composition series for G, a chief series for G is unique in the following sense: if $1 = X_0 < X_1 < \ldots < X_t$ and $1 = Y_0 < Y_1 < \ldots < Y_s$ are two chief series for G, then $s = t$ and there is a bijection f from $\{X_i/X_{i-1} : 1 \leq i \leq t\}$ to $\{Y_i/Y_{i-1} : 1 \leq i \leq s\}$ such that $X_i/X_{i-1} \cong f(X_i/X_{i-1})$ for all i. Thus, we may

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

speak of t as the chief length of G, and the set $\{X_i/X_{i-1} : 1 \leq i \leq t\}$ as the set of chief factors of G.

9.1.2 Representations and the Action of a Finite Group on Its Chief Factors

Suppose that G and A are finite groups, and that G acts on A via $a \to a^g$, $a \in A$, $g \in G$. We say that G acts on A *via automorphisms* if $(ab)^g = a^g b^g$ for all $a, b \in A$, and all $g \in G$. In this case, the map $\theta_g : A \to A$, $a \to a^g$, is an automorphism of A. The associated map $g \to \theta_g$ is a homomorphism from G to $\mathrm{Aut}(A)$ with kernel denoted $C_G(A) = \{g \in G : a^g = a \text{ for all } a \in A\}$.

For example, a finite group G acts via automorphisms (by conjugation) on any normal section of G. In particular, if X/Y is a chief factor of G and $X/Y \cong S^t$, for a simple group S, we get a well-defined map $G \to \mathrm{Aut}(S^t)$ with kernel denoted $C_G(X/Y)$. The group $G/C_G(X/Y)$ is called the group *induced* by G on X/Y. Since $G/C_G(X/Y)$ is isomorphic to a subgroup of $\mathrm{Aut}(X/Y)$, we will abuse notation and write $G/C_G(X/Y) \leq \mathrm{Aut}(X/Y)$.

We would now like to garner more information on the groups induced by a finite group on its chief factors. Before doing so, we need the following definition:

Definition 9.6 Let A be a finite group, and let T be a subgroup of the symmetric group Sym_t of degree $t \geqslant 1$. Then the *(permutational) wreath product* of A by T is the group $A \wr T := A^t \rtimes T$, where the action of T on A^t is defined by

$$(a_1, a_2 \ldots, a_t)^x = (a_{1^{x^{-1}}}, a_{2^{x^{-1}}} \ldots, a_{t^{x^{-1}}})$$

for $x \in T$, $a_i \in A$. The subgroups A^t and T are called the *base group* and *top group* of $A \wr T$, respectively.

Definition 9.6 will be useful not only for our next lemma, but also for examples throughout the chapter.

Now let G be a finite group, and let X/Y be a chief factor of G. By Corollary 9.4, X/Y is isomorphic to a direct product S^t of t copies of a finite simple group S. Then S is either abelian (i.e. $S \cong Z_p$, for a prime p), or S is a non-abelian simple group. Since the induced group $G/C_G(X/Y)$ is a subgroup of $\mathrm{Aut}(X/Y) \cong \mathrm{Aut}(S^t)$, it will be useful to have information on the automorphism group of a direct product of isomorphic simple groups.

Lemma 9.7 *Let S be a finite simple group, $t \geqslant 1$.*

1 *If S is abelian (i.e. $S \cong Z_p$ for a prime p), then* $\mathrm{Aut}(S^t) \cong \mathrm{GL}_t(p)$.
2 *If S is non-abelian, then* $\mathrm{Aut}(S^t) \cong \mathrm{Aut}(S) \wr \mathrm{Sym}_t$.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Proof For part (i), note that an elementary abelian p-group is simply a vector space over $\mathbb{F}_p$, and that an automorphism is an invertible linear map. Part (ii) is straightforward, but requires a bit more effort. We refer the interested reader to [3, Theorem 3.1] for the details. □

Recall that a *representation* of a finite group G over a field $\mathbb{F}$ is a homomorphism from G into $\mathrm{GL}_n(\mathbb{F})$. We call n the degree of the representation, and the vector space $\mathbb{F}^n$ is called the *natural module* for G. We remark that we view matrices as acting on row vectors, so all modules considered here are right modules. Lemma 9.7(i) then states that each abelian chief factor $X/Y \cong Z_p^t$ of a finite group G yields a t-dimensional representation for G over the field $\mathbb{F}_p$ of p elements. Similarly, a permutation representation of a finite group G is a homomorphism from G into Sym_n, for some $n \geqslant 1$. The natural number n is called the *degree* of the permutation representation. Lemma 9.7(ii) states that each non-abelian chief factor of a finite group G yields a permutation representation for G of degree t.

The following lemma gives more information on the groups induced by a finite group on its chief factors.

Lemma 9.8 *Let G be a finite group, and let X/Y be a chief factor of G so that X/Y is isomorphic to a direct product, S^t, of t isomorphic copies of a non-abelian finite simple group S.*

(i) If S is abelian (i.e. $S \cong Z_p$ for a prime p), then $G/C_G(X/Y) \leq GL_t(\mathbb{F}_p)$ acts irreducibly on the natural module $\mathbb{F}_p^t$.

(ii) If S is non-abelian, then consider the projection $\pi\colon \mathrm{Aut}(S^t) \cong \mathrm{Aut}(S) \wr \mathrm{Sym}_t \to \mathrm{Sym}_t$. Then $\pi(G/C_G(X/Y))$ is a transitive subgroup of Sym_t.

Proof The proof follows immediately from the fact that if A is normal in G with $Y \leq A \leq X$, then $A = Y$ or $A = X$. □

9.1.3 An Equivalence Relation on a Special Set of Chief Factors of a Finite Group

Recall that our aim in the first section of these notes is to define an equivalence relation on the set of chief factors in a finite group G. We are almost ready to do so. But first, we require a standard definition.

Definition 9.9 Let G be a finite group.

(a) The *Frattini subgroup*, written $\Phi(G)$, of G is the intersection of all maximal subgroups of G. Thus, $\Phi(G) := \bigcap_{M <_{\max} G} M$.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

(b) A chief factor X/Y of G is called *non-Frattini* if X/Y is not a subgroup of $\Phi(G/Y)$.

Recall that a finite group G is *nilpotent* if all Sylow subgroups of G are normal in G. The following lemma states, in particular, that $\Phi(G)$ is nilpotent. Its proof can be found in any standard textbook in finite group theory (for example, see [6, Chapter 1]).

Lemma 9.10 *Let G be a finite group.*

(i) The subgroup $\Phi(G)$ is nilpotent.
(ii) G is nilpotent if and only if $G/\Phi(G)$ is abelian.
(iii) $\Phi(G)$ is the set of "non-generators" of G. More precisely,
$\Phi(G) = \{x \in G \colon A \subseteq G \text{ and } \langle x, A\rangle = G \text{ if and only if } \langle A\rangle = G\}$.

Notice that Lemma 9.10(i) implies that every non-abelian chief factor of G is non-Frattini. Suppose, then, that X/Y is an abelian chief factor of G. If X/Y is non-Frattini, then either $G = X$ or G/Y has the form $G/Y = X/Y \rtimes H/Y$, for some subgroup H of G containing Y. Indeed, X/Y being non-Frattini implies that there exists a maximal subgroup H/Y of G/Y not containing X/Y. Then $G/Y = (X/Y)(H/Y)$. Moreover, $(X/Y) \cap (H/Y)$ is a normal subgroup of G/Y (we leave the proof of this fact as an exercise). Thus, $(X/Y) \cap (H/Y)$ must be either trivial or equal to X/Y. Thus, either $G/Y = X/Y$ or $G/Y = X/Y \rtimes H/Y$, as claimed. For this reason, the non-Frattini chief factors in a finite group are often also called the *complemented* chief factors of G (a complement of a subgroup H in a finite group G is a subgroup K such that $HK = G$ and $H \cap K = 1$).

We would now like to define an equivalence relation on the set of non-Frattini chief factors in a finite group G. We begin with a definition.

Definition 9.11 A finite group L is called *monolithic* if L has a unique minimal normal subgroup N. If in addition N is not contained in $\Phi(L)$, then L is called a *monolithic primitive group*.

The reason for the terminology "primitive" in Definition 9.11 is that if $N \not\leq \Phi(L)$, then there exists a maximal subgroup M of L which does not contain N. It follows that M is core-free in L (i.e. $\text{core}_L(M) = 1$), and hence that L has a faithful primitive permutation action on the cosets of M (we will discuss this in more depth in Subsection 9.2.1).

Our next definition introduces the "crown" terminology:

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Definition 9.12 Let L be a monolithic primitive group and let N be its unique minimal normal subgroup. For each positive integer k, let L^k be the k-fold direct power of L. The *crown-based power of L of length k* is the subgroup L_k of L^k defined by

$$L_k = \{(l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \bmod N\}.$$

Equivalently, $L_k = N^k \operatorname{diag}(L^k)$, where $\operatorname{diag}(L^k) = \{(l_1, \ldots, l_k) \in L^k \mid l_i = l_j$ for all $i, j\}$.

Example 9.13 Let $A := Z_p$ be a cyclic group of order p, with p an odd prime. Let $H = \langle h \rangle$ be a cyclic group of order 2, and define an action of H on the k-fold direct power A^k by $a^h = a^{-1}$ for all $a \in A^k$. Let $L := A \rtimes H$. Then $A^k \rtimes H \cong L_k$ is the crown-based power of L of length k.

We are now almost ready to define the equivalence relation on chief factors in finite groups mentioned at the beginning of the section. First, recall that if a group G acts on a group A via automorphisms, then we say that A is a *G-group*. Some of the most widely studied G-groups are the groups of the form $A = \mathbb{F}^n$, for some field $\mathbb{F}^n$: these are the $\mathbb{F}[G]$-modules, and the associated maps $G \to \operatorname{Aut}(A) \cong \mathrm{GL}_n(\mathbb{F})$ are the $\mathbb{F}[G]$-representations. Our next definition generalises some basic notions in representation theory to arbitrary G-groups.

Definition 9.14 Let G be a finite group, and let A and B be G-groups.

(a) If G does not stabilise (set-wise) any non-trivial subgroup of A, then A is called an *irreducible* G-group.
(b) If there exists an isomorphism $f : A \to B$ such that $f(a)^g = f(a^g)$ for all $g \in G$, then A and B are said to be *G-isomorphic*.

We are now ready to define G-equivalent G-groups:

Definition 9.15 Let G be a finite group. We say that two G-groups A_1 and A_2 are *G-equivalent* and we put $A_1 \sim_G A_2$, if there are isomorphisms $\varphi : A_1 \to A_2$ and $\Phi : A_1 \rtimes G \to A_2 \rtimes G$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A_1 & \longrightarrow & A_1 \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & A_2 & \longrightarrow & A_2 \rtimes G & \longrightarrow & G & \longrightarrow & 1. \end{array} \tag{9.1.2}$$

Note that the two rows in the diagram (9.1.2) represent split short exact sequences. Moreover, the map $A_i \to A_i \rtimes G$ is the usual inclusion map, while $A_i \rtimes G \to G$ is the quotient map $(a_i, g) \mapsto g$ for $a_i \in A_i$, $g \in G$.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

The following lemma shows that being G-equivalent is weaker than being G-isomorphic.

Lemma 9.16 *Let G be a finite group, and let A_1 and A_2 be G-groups.*

(i) If A_1 and A_2 are G-isomorphic, then A_1 and A_2 are G-equivalent.
(ii) In the particular case where A_1 and A_2 are abelian the converse is true: if A_1 and A_2 are abelian and G-equivalent, then A_1 and A_2 are also G-isomorphic.

Proof For Part (i), let $f\colon A_1 \to A_2$ be a G-isomorphism. Then define the isomorphisms φ and Φ from Definition 9.15 by $\varphi := f$ and $\Phi\colon A_1 \rtimes G \to A_2 \rtimes G$, $a_1 g \to f(a_1)g$. It is straightforward to check that these maps are indeed isomorphisms. It is then trivial to see that the diagram (9.1.2) commutes.

For part (ii), assume that A_1 and A_2 are abelian, and that A_1 and A_2 are G-equivalent. Let φ and Φ be the maps from Definition 9.15. We claim that $\varphi\colon A_1 \to A_2$ is in fact a G-isomorphism. Indeed, fix $g \in G$, and let a_1 be an element of A_1. Then using the commuting diagram (9.1.2), we have

$$\varphi(a_1^g) = \Phi(a_1^g) = \Phi(a_1)^{\Phi(g)}, \tag{9.1.3}$$

where the last equality follows since Φ is a group homomorphism. The diagram (9.1.2), however, implies that $\Phi(g) = ug$, for some $u \in A_2$. Since A_2 is abelian, we deduce from equation (9.1.3) that $\varphi(a_1^g) = \Phi(a_1)^g$. Since $\Phi\downarrow_{A_1} = \varphi$, it follows that φ is a G-isomorphism, as claimed. □

Remark Note that if two G-groups A_1 and A_2 are G-isomorphic, then it follows from the definition of G-isomorphism that $C_G(A_1) = C_G(A_2)$. This is often a quick and easy way to show that two G-groups are not G-isomorphic.

The following is an example where two G-groups are G-equivalent, but not G-isomorphic:

Example 9.17 Let $G = \mathrm{Alt}_5 \times \mathrm{Alt}_5$, and let A_1 and A_2 be the normal subgroups $A_1 := \mathrm{Alt}_5 \times 1$, $A_2 := 1 \times \mathrm{Alt}_5$. Using the conjugation actions of G on A_1 and A_2, we can construct the (external) semidirect products $A_1 \rtimes G$ and $A_2 \rtimes G$.

Now, $C_G(A_1) = A_2$ and $C_G(A_2) = A_1$, so A_1 and A_2 are not G-isomorphic (see Remark 9.1.3).

On the other hand, define $\varphi\colon A_1 \to A_2$ by $\varphi((x,1)) = (1,x)$, and $\Phi\colon A_1 \rtimes G \to A_2 \rtimes G$ by $\Phi(((x,1),(g,h))) = ((1, xgh^{-1}),(g,h))$. Then it is a routine exercise to check that φ and Φ are isomorphisms, and the associated diagram as at (9.1.2) commutes.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

9.2 Equivalence Classes of Non-Frattini Chief Factors

In this section, our aim is to build on our work in Section 9.1 to define the *set of crowns* of a finite group G (see Definition 9.30). We begin with a necessary discussion on permutation group theory.

9.2.1 Primitive Permutation Groups

As Definition 9.11 suggests, primitive permutation groups play an important role in the theory of crowns in a finite group. In this subsection, we will briefly recall some important notions from permutation group theory and, in particular, from the theory of primitive groups.

First, recall from Subsection 9.1.2 that a *permutation group on a set* Ω is a subgroup G of the symmetric group $\mathrm{Sym}(\Omega)$. In this case, Ω is called a *G-set*. If Ω is finite of cardinality n, then we say that G is a *permutation group of degree n*. Recall also that if G is a finite group acting on a set Ω, then the associated homomorphism $G \to \mathrm{Sym}(\Omega)$ is called a *permutation representation* of G.

As with G-groups, we have a notion of isomorphism between G-sets.

Definition 9.18 Let G be a finite group. Two G-sets Ω_1 and Ω_2 are said to be *G-isomorphic* if there is a bijection $f\colon \Omega_1 \to \Omega_2$ such that $f(\omega_1^g) = f(\omega_1)^g$ for all $\omega_1 \in \Omega_1$, $g \in G$.

The following are special types of permutation representations.

Definition 9.19 Let G be a finite group acting on a finite set Ω.

(a) G is said to act *transitively* on Ω if, for all $\omega_1, \omega_2 \in \Omega$, there exists $g \in G$ such that $\omega_1^g = \omega_2$.
(b) G is said to act *primitively* on Ω if G acts transitively on Ω and a point stabiliser $G_\omega = \{g \in G\colon \omega^g = \omega\}$ is a maximal subgroup of G.

The following are basic, but important, remarks about transitive and primitive permutation representations of a finite group. See [6, Chapter 8] for a more detailed discussion.

Remark Suppose that G is a finite group acting transitively on a finite set Ω.

(1) All point stabilisers are G-conjugate, so if one point stabiliser is maximal in G, then they all are.
(2) Consider the G-set $G_\omega\backslash G$ (i.e. the set of right G-cosets of G_ω, acted upon by G by right multiplication). Then the G-sets Ω and $G_\omega\backslash G$ are G-isomorphic. Thus, each transitive permutation representation of a finite

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

group G may be viewed as an action on the set of right cosets of a subgroup. In particular, each primitive permutation representation of G can be viewed as an action on the set of right cosets of a maximal subgroup of G.

(3) The *kernel of the action of* G on Ω is the set $\{g \in G : \omega^g = \omega \text{ for all } \omega \in \Omega\}$. When H is a subgroup of G, the kernel of the action of G on $H\backslash G$ is precisely the core of H in G.

A famous result, due independently to O'Nan and Scott, characterises the primitive permutation groups into types, usually based on geometric considerations. In this chapter, we will only be concerned with two of these types, which we now define. Recall that an *almost simple* group is a finite group L such that $S \leq L \leq \mathrm{Aut}(S)$ for some finite simple group S.

Let L be an almost simple group, $S \leq L \leq \mathrm{Aut}(S)$, such that L/S is cyclic of prime order. Consider the crown-based power $G := L_2 = \{(l_1, l_2) \in L^2 : a_1 \equiv a_2 \bmod S\}$. Fix $\alpha \in \mathrm{Aut}(S)$ with the property that α centralises the group L/S (that is, $l^\alpha S = lS$ for all $l \in L$). Then $H := \{(l, l^\alpha) : l \in L\}$ is a subgroup of $G = L_2$.

Exercise 9.20 With notation as above, prove that H is a maximal subgroup of G.

Definition 9.21 We say that a primitive permutation group has *special simple diagonal type* if $G = L_2$ for some almost simple group $S \leq L \leq \mathrm{Aut}(S)$, and G_ω has the form $G_\omega = \{(l, l^\alpha) : l \in L\}$ for some $\alpha \in \mathrm{Aut}(S)$.

For our second type, we need to recall that the socle $\mathrm{soc}(X)$ of a finite group X is the product of the minimal normal subgroups of X.

Let $W = J \wr \mathrm{Sym}_t$, where $J \leq \mathrm{Sym}(\Delta)$ is a primitive permutation group on a finite set Δ, and $t > 1$. Fix $\delta \in \Delta$, set $I := J_\delta$, and consider the naturally embedded subgroup $I^t \leq J^t \leq W$. Set

$$H := I^t \rtimes \mathrm{Sym}_t \cong I \wr \mathrm{Sym}_t \leq W, \text{ and } \Omega := H\backslash W. \tag{9.2.1}$$

Exercise 9.22 Prove that H is a maximal subgroup of W (i.e. W acts primitively on Ω). (Hint: show that $I^t \leq H$ is maximal as a proper Sym_t-invariant subgroup of J^t.)

Definition 9.23 We will say that a primitive permutation group $G \leq \mathrm{Sym}(\Omega)$ has *special product action type* if $G \leq W := J \wr \mathrm{Sym}_t$, where:

(a) J is primitive of special simple diagonal type;
(b) G_ω has the form $G_\omega = G \cap H$, where H is as in (9.2.1) above;
(c) the projection $G \to \mathrm{Sym}_t$ has transitive image; and
(d) G contains the naturally embedded subgroup $\mathrm{soc}(J)^t \leq J^t \leq W$.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Note that a primitive permutation group of special simple diagonal type as in Definition 9.21 above has two minimal normal subgroups, each isomorphic to S. A primitive permutation group of special product action type, as in Definition 9.23, also has two minimal normal subgroups, each isomorphic to S^t (where S^2 is the socle of J). By the O'Nan–Scott theorem, these are the only examples of a primitive permutation group with more than one minimal normal subgroup. (See [9] for more details, and for proofs of the assertions made in this paragraph.)

Remark If G is a finite group, then a subgroup H of the direct product G^k of k copies of G is said to be a *diagonal subgroup* if H has the form

$$H = \{(g, g^{\alpha_2}, \ldots, g^{\alpha_k}) : g \in G\}$$

for some automorphisms $\alpha_i \in \mathrm{Aut}(G)$. Thus, in this language a primitive permutation group has simple diagonal type if there exists a finite simple group T such that $T \times T \leq G \leq \mathrm{Aut}(T) \times \mathrm{Aut}(T)$, and a point stabiliser in G intersects $T \times T$ in a diagonal subgroup.

9.2.2 Back to Equivalence Classes of Chief Factors

Now, we have already seen an example of a primitive permutation group of simple diagonal type. Namely, take $G = \mathrm{Alt}_5 \times \mathrm{Alt}_5$ to be as in Example 9.17 (so that $T = \mathrm{Alt}_5$), and take Ω to be the set of right cosets of the diagonal subgroup $\{(t,t) : t \in \mathrm{Alt}_5\}$.

For our purposes, the important thing about this group was that it gave us an example of a finite group G with G-equivalent chief factors which are not G-isomorphic. We have seen already that two abelian chief factors of G are G-isomorphic if and only if they are G-isomorphic. By a result of Jiménez-Seral and Lafuente [7, Proposition 4.1], the non-Frattini chief factors in a finite group which are G-equivalent but not G-isomorphic occur in a very similar way to Example 9.17.

Proposition 9.24 *Let G be a finite group, and let X_1/Y_1 and X_2/Y_2 be non-Frattini chief factors of G. Then X_1/Y_1 and X_2/Y_2 are G-equivalent if and only if one of the following holds:*

(i) X_1/Y_1 and X_2/Y_2 are abelian and G-isomorphic; or

(ii) G has a maximal subgroup containing $Y_1 \cap Y_2$ such that $\mathrm{core}_G(M) = Y_1 \cap Y_2$ and $G/\mathrm{core}_G(M)$ is a primitive permutation group of simple diagonal type, with minimal normal subgroups G-isomorphic to X_1/Y_1 and X_2/Y_2.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Proposition 9.24 gives us a useful way to determine the equivalence classes of chief factors in a finite group. Some important examples are as follows.

Example 9.25 Let G be a finite p-group, for p prime. Then the non-Frattini chief factors of G all occur in $G/\Phi(G)$ – an elementary abelian p-group. Thus, all non-Frattini chief factors of G are G-isomorphic to the trivial G-group $\mathbb{F}_p$.

Example 9.26 Let L be a primitive monolithic group with minimal normal subgroup N, and let $G = L_k$ be the crown-based power of L of length k (see Definition 9.11). Then $G = N^k \operatorname{diag}(L^k)$. In particular, each element of G can be written uniquely in the form $g = (l, n_2 l, \dots, n_k l)$, for $l \in L$ and $n_i \in N$.

For $1 \leq i \leq k$, let A_i be the ith coordinate subgroup of N^k. That is,

$$A_i := \{(1, \dots, 1, \underbrace{a_i}_{i\text{th position}}, 1 \dots, 1) \colon a_i \in N\}.$$

We claim that A_i is G-equivalent to A_j for all i, j. Indeed, for fixed $1 \leq i, j \leq k$, define $\varphi \colon A_i \to A_j$ by

$$\varphi(1, \dots, 1, \underbrace{a_i}_{i\text{th position}}, 1 \dots, 1) := (1, \dots, 1, \underbrace{a_i}_{j\text{th position}}, 1 \dots, 1).$$

Also, define $\Phi \colon A_i \rtimes G \to A_j \rtimes G$ as follows: for a generic element

$$x := ((1, \dots, 1, \underbrace{a_i}_{i\text{th position}}, 1 \dots, 1), (l, n_2 l, \dots, n_k l))$$

of the external semidirect product $A_i \rtimes G$, define

$$\Phi(x) := ((1, \dots, 1, \underbrace{a_i n_j^{-1}}_{j\text{th position}}, 1 \dots, 1), (l, n_2 l, \dots, n_k l)).$$

It is routine (though non-trivial) to prove that φ and Φ are homomorphisms, and that the associated diagram from (9.1.2) commutes. Thus, all A_i and A_j are G-equivalent.

The following is an illustration of how one finds representatives for the equivalence classes of non-Frattini chief factors of G in a specific example.

Example 9.27 Consider $G = \mathrm{Sym}_4$. Since G is soluble, two chief factors A_1 and A_2 are G-equivalent if and only if they are G-isomorphic. Now, a chief series for G is

$$1 < V_4 < \mathrm{Alt}_4 < G,$$

where $V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle$. Since G, $G/V_4 \cong \mathrm{Sym}_3$ and $G/\mathrm{Alt}_4 \cong Z_2$ all have trivial Frattini subgroups, each of the associated chief factors are

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

non-Frattini. Furthermore, finding a set of representatives for the G-equivalence classes of Frattini chief factors for G is easy in this case, since the chief factors V_4, Alt_4/V_4 and G/Alt_4 are pairwise non-isomorphic as groups, so are certainly pairwise non-isomorphic as G-groups. Thus, $\{V_4, \mathrm{Alt}_4/V_4, \mathrm{Sym}_4/\mathrm{Alt}_4\}$ is a complete set of representatives for the G-equivalence classes of chief factors in $G = \mathrm{Sym}_4$.

Exercise 9.28 Find a set of representatives for the non-Frattini chief factors in the cases $G = \mathrm{GL}_2(3)$ and $G = Z_p \rtimes Z_{p-1}$, where p is prime and Z_{p-1} acts on Z_p as $\mathrm{Aut}(Z_p)$.

9.2.3 The Set of Crowns in a Finite Group

In this subsection, we will define the set of crowns in a finite group G. As the terminology suggests, and as the next lemma shows, crown-based powers play an important role in this definition.

Lemma 9.29 *Let G be a finite group, and let A be a non-Frattini chief factor of G. With $C_G(A)$ as defined on page* 320*, define L_A, the* monolithic primitive group associated to *A, by*

$$L_A := \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian}, \\ G/C_G(A) & \text{otherwise}. \end{cases}$$

Then:

(i) There exists a normal subgroup N of G such that $G/N \cong L_A$.

(ii) Set $R_G(A) := \bigcap_N N$, where the intersection runs over all $N \trianglelefteq G$ such that $G/N \cong L_A$. Then $G/R_G(A) \cong (L_A)_k$, where k is the number of non-Frattini chief factors in any chief series for G which are G-equivalent to A.

Proof Since (i) is trivial in the case where A is non-abelian, we may assume that A is abelian.

Let G be a counterexample to (i) of minimal order, and let $Y \leq X$ be normal subgroups of G with $A = X/Y$. By minimality, we may assume that $Y = 1$, so that $A = X$ is a minimal normal subgroup of G.

Since A is non-Frattini, A has a complement H in G (see the discussion after the statement of Lemma 9.10). Thus, $G = A \rtimes H$. It is then clear that $N := C_H(A) \trianglelefteq G$, and $G/N \cong L_A$. This proves (i).

We will now prove (ii). To do so, we need a few standard group theoretic facts. In what follows, let G be a finite group and let N_1 and N_2 be distinct normal subgroups of G.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

(1) The factor group $G/N_1 \cap N_2$ is isomorphic to a subgroup of $G_1 \times G_2$, where $G_i := G/N_i$ via the embedding $\theta\colon G/N_1 \cap N_2 \hookrightarrow G_1 \times G_2$, $(N_1 \cap N_2)g \to (N_1 g, N_2 g)$ for $g \in G$.

(2) Let $\pi_i\colon G_1 \times G_2 \to G_i$ be the canonical projection. Then $\pi_i(\theta(G/N_1 \cap N_2)) = G_i$, for $i = 1,2$ (we say that $G/N_1 \cap N_2$ projects onto both G_1 and G_2). This is clear from the definition of ρ.

(3) If E and F are finite groups and X is a subgroup of $E \times F$ projecting onto both E and F, then $X_E := X \cap (E \times 1) \trianglelefteq E$, $X_F := X \cap (1 \times F) \trianglelefteq F$, $E/X_E \cong F/X_F$ and $X/X_E X_F$ is a diagonal subgroup of $(E/X_E) \times (F/X_F)$. We leave the proofs of these assertions as an exercise for the reader.

We now prove (ii), only in the case $k = 2$ (the proof for larger k follows the same line of argument, and is left as an exercise for the reader). So let N_1 and N_2 be distinct normal subgroups of G with $G/N_1 \cong G/N_2 \cong L_A$, and $R_G(A) = N_1 \cap N_2$. Note that $N_1, N_2 > 1$, since N_1 and N_2 are distinct and have the same order.

We need to show that $G/R_G(A) \cong (L_A)_2$. Thus, by factoring out $R_G(A)$, we may assume that $R_G(A) = 1$. Suppose first that A is non-abelian. Then by Proposition 9.24(ii), and since $R_G(A) = N_1 \cap N_2 = 1$, we see that G is isomorphic to a primitive permutation group of simple diagonal type, with two minimal normal subgroups, each G-isomorphic to A. By definition of primitive groups of simple diagonal type, we deduce that $G \cong (L_A)_2$.

Suppose next that A is abelian. Since $R_G(A) = 1$, Fact (1) above implies that G embeds as a subgroup of $L_1 \times L_2 \cong (L_A)^2$, where $L_i := G/N_i \cong L_A$. To avoid unnecessary additional notation, we will omit reference to the embedding given in Fact (1) and assume, for the remainder of the proof, that G is a subgroup of $L_1 \times L_2$. By Fact (3) and the definition of the embedding $G \hookrightarrow L_1 \times L_2$, we may then assume that $G \cap (L_1 \times 1) = N_1 \times 1$; $G \cap (1 \times L_2) = 1 \times N_2$; and $G/(N_1 \times N_2)$ is isomorphic to a diagonal subgroup of $L_1/N_1 \times L_2/N_2$.

Write A_i for the unique minimal normal subgroup of L_i. We claim that $N_i = A_i$ for each i. To this end, note first that since $N_i \neq 1$, N_i contains A_i. Also, since A is abelian and A_1 and A_2 are G-equivalent, Proposition 9.24 and Remark 9.1.3 imply that $C_G(A_1) = C_G(A_2)$. On the other hand, since A_1 is the unique minimal normal subgroup of L_1 and A_1 is non-Frattini, we have $A_1 = C_{L_1}(A_1)$. Thus, the centraliser of A_1 in $G \leq L_1 \times L_2$ is precisely $(A_1 \times 1) \times (G \cap 1 \times L_2) = A_1 \times N_2$. Similarly, $C_G(A_2) = N_1 \times A_2$. Since $C_G(A_1) = C_G(A_2)$, it follows that $N_1 = A_1$ and $N_2 = A_2$, as claimed.

Thus, we have shown that G is isomorphic to a subgroup of $(L_A)^2$ containing A^2, and that, under this embedding, G/A^2 is isomorphic to a diagonal subgroup of $(L_A/A)^2$. We then see from the definition of $(L_A)_2$ that $G \cong (L_A)_2$. □

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Lemma 9.29 is the key lemma in the theory of crowns, and allows us to define the following:

Definition 9.30 Let G be a finite group, and let A be a non-Frattini chief factor of G.

(a) The normal subgroup $R_G(A)$ from Lemma 9.29 is called the *A-core* of G.
(b) The subgroup $I_G(A)$ is defined so that $I_G(A)/R_G(A) = \mathrm{soc}(G/R_G(A))$ is the socle of $G/R_G(A)$. We call $I_G(A)/R_G(A)$ the *A-crown* of G.
(c) As proved in Lemma 9.29, $I_G(A)/R_G(A) \cong A^k$. We define $\delta_G(A) := k$, so that $\delta_G(A)$ is the number of non-Frattini chief factors G-equivalent to A in any chief series for G.

We can now define the *set of crowns* in a finite group G.

Definition 9.31 Let G be a finite group. The set

$$\{I_G(A)/R_G(A) : A \text{ a non-Frattini chief factor of } G\}$$

is called the *set of crowns for G*.

9.3 An Application of Crowns: Minimal Generator Numbers

In this section, our aim is to demonstrate one of the most useful applications of the theory of crowns to problems in finite group theory. Namely, finding the minimal number of elements required to generate a finite group G.

For a finite group G, define $d(G) := \min\{|X| : X \subseteq G, \langle X\rangle = G\}$ to be the minimal size of a generating set for G. Thus, if G is cyclic, for example, then $d(G) = 1$. If V is an elementary abelian group of order p^n, then G may be viewed as a vector space of dimension n over the finite prime field $\mathbb{F}_p$, and then $d(G)$ is just the $\mathbb{F}_p$-dimension of G: that is, $d(G) = n$.

The last example shows that the function d is well behaved when G is a vector space: namely, $d(H) \leq d(G)$ when H is a subgroup (i.e. subspace) of G. But this is not true in general. For example, take G to be the wreath product $R \wr S$ (see Definition 9.6) where $R \cong S \cong Z_p$ (S is viewed as $S = \langle s\rangle$, with $s = (1,2,\ldots,p) \in \mathrm{Sym}_p$ in this case). The base group $H \cong R^p$ of G is elementary abelian of order p^p, and so $d(H) = \dim_{\mathbb{F}_p}(H) = p$. However, if we set $X := \{\underbrace{(r,1\ldots,1)}_{p}, s\} \subseteq G$, where r is a generator for R, then it is easy to see that $G = \langle X\rangle$. Thus, $d(G) = 2$, since G is not cyclic.

The above example shows that, in general, there can be no bound on $d(H)$ in terms of $d(G)$ for subgroups H of a finite group G, even for finite p-groups.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Finite p-groups are, however, quite straightforward to deal with when it comes to finding $d(G)$, as the next result shows.

Proposition 9.32 *Let G be a finite group. Then $d(G) = d(G/\Phi(G))$. In particular, if G is a finite p-group, for p prime, then $d(G)$ is the dimension of the $\mathbb{F}_p$-vector space $G/\Phi(G)$.*

Proof That $d(G) \leq d(G/\Phi(G))$ follows immediately from Lemma 9.10 (since $\Phi(G)$ is the set of "non-generators" for G). On the other hand, if X is a generating set for G, and N is any normal subgroup of G, then the set $\{xN : x \in X\}$ is a generating set for G. Hence $d(G/N) \leq d(G)$. In particular, $d(G/\Phi(G)) \leq d(G)$, so $d(G) = d(G/\Phi(G))$. □

Example 9.33 Recall from Example 9.25 that a finite p-group has a unique G-equivalence class of non-Frattini chief factors, represented by the trivial $\mathbb{F}_p[G]$-module $A := \mathbb{F}_p$. Since all non-Frattini chief factors of G occur as chief factors of $G/\Phi(G)$, and all chief factors of $G/\Phi(G)$ are non-Frattini, we deduce that G has precisely $d(G)$ non-Frattini chief factors of G (all G-equivalent to A). Since G acts trivially on A, we have $L_A = A$ (where L_A is as in Lemma 9.29), and so $G/R_G(A) \cong A^{d(G)} \cong (\mathbb{F}_p)^{d(G)}$. In particular, $R_G(A) = \Phi(G)$ and $\delta_G(A) = d(G)$ in this case.

Remark During the course of the proof of Proposition 9.32, we proved that if G is a finite group and N is a normal subgroup of G, we have $d(G/N) \leq d(G)$. An often-used inductive tool (for deriving upper bounds on $d(G)$) is the (almost trivial) upper bound $d(G) \leq d(G/N) + d(N)$.

As mentioned in Example 9.33, we have $d(G) = d(G/R_G(A))$ for a finite p-group G, where A is the (up to G-equivalence) unique non-Frattini chief factor of G (here, $R_G(A) = \Phi(G)$). The next result shows that this (perhaps surprisingly) can be made more general.

Theorem 9.1 *[4, Theorems 1.4 and 2.7] Let G be a finite group with $d(G) \geqslant 3$. Then G has a non-Frattini chief factor A such that $d(G) = d(G/R_G(A))$. Moreover:*

(1) if G is abelian, then $d(G) = d(G/R_G(A)) \leq \delta_G(A) + 1$;
(2) if G is non-abelian, then $d(G) = d(G/R_G(A)) \leqslant \lceil \log_{|A|}\left(\frac{90}{54}\delta_G(A)\right) + 5/4 \rceil$.

The proof of Theorem 9.1 is beyond the scope of this course, but we refer the interested reader to [4, Theorems 1.4 and 2.7] for details.

Theorem 9.1 is an extremely useful tool for determining the minimal generator numbers in various classes of finite groups. We close the section by illustrating this with some examples.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Example 9.34 Let $G = T^k$ be the direct product of k copies of a non-abelian finite simple group T. As mentioned in Remark 9.3, we have $d(G) \leq d(G/N) + d(N)$ for any normal subgroup N of G. Hence, since every finite simple group can be generated by two elements, we have $d(G) \leq 2k$.

Let us see if we can do any better using the theory of crowns. We will assume that $d(T^k) \geqslant 3$. Then $k \geqslant 2$, since $d(T) = 2$ (as mentioned above). Now, note that G is isomorphic to the crown-based power T_k (this is, in some sense, the "trivial crown-based power associated to T"). It follows that G has a unique equivalence class of non-Frattini chief factors, isomorphic to T, by Example 9.26. Clearly, $\delta_G(T) = k$. Hence, Theorem 9.1 yields $d(G) \leq \log_{|T|}(k) + 1$ – a far tighter bound than $d(G) \leq 2k$.

Example 9.35 Let G be the wreath product $R \wr S$, where $R = Z_p$ is cyclic of prime order p, and $S = \mathrm{Alt}_s$ is the alternating group of degree $s \geqslant 5$. Consider the following subgroups of the base group R^s of G:

$$A_1 := \{(x,x,\ldots,x) \colon x \in R\} \text{ and } A_2 := \{(x_1,x_2,\ldots,x_s) \colon x_i \in R, \prod_{i=1}^{s} x_i = 1\}.$$

The subgroups A_1 and A_2 are clearly normal in G. Since $|A_1| = p$, A_1 is a minimal normal subgroup of G. Note that $A_1 \leq A_2$ if $p \mid s$, and $A_1 \not\leq A_2$ otherwise. Since A_2 has order p^{s-1}, we deduce that $A_1A_2 = A_2$ has index p in R^s if $p \mid s$, and $A_1A_2 = R^s$ otherwise. It is not difficult to prove (see [8, Proposition 5.4.1]) that Alt_s acts irreducibly on the $\mathbb{F}_p[\mathrm{Alt}_s]$-module A_1A_2/A_1, and hence that A_1A_2/A_1 is a chief factor of G. Thus, since $G/R^s \cong \mathrm{Alt}_s$ is simple, we deduce that

$$1 < A_1 < A_1A_2 \leq R^s < G$$

is a chief series for G. Since $|A_1A_2/A_1| = p^{s-2}$ if $p \mid s$, and $|A_1A_2/A_1| = p^{s-1}$ otherwise, we have that G has two chief factors G-isomorphic to the trivial $\mathbb{F}_p[G]$-module $\mathbb{F}_p$ if $p \mid s$, and one chief factor G-isomorphic to $\mathbb{F}_p$ otherwise. Hence, $\delta_G(\mathbb{F}_p) \leq 2$. Furthermore, we clearly have $\delta_G(A_1A_2/A_1) = 1$, and $\delta_G(\mathrm{Alt}_s) = 1$. In fact, it is not difficult to prove that if $p \mid s$, then $A_1 \leq \Phi(G)$, so $\delta_G(A) = 1$ for all non-Frattini chief factors A of G. Hence, Theorem 9.1 yields $d(G) \leq 2$. Thus, $d(G) = 2$, since G is not cyclic.

Recommended Further Reading

A more detailed account of crowns in finite groups in given in [2, Chapter 1], which we can certainly recommend for further reading.

The theory of crowns also naturally arises in the study of the first cohomology group of a finite group: see [1] for more details.

https://doi.org/10.1017/9781009093750.011 Published online by Cambridge University Press

Bibliography

[1] Aschbacher M., and Guralnick, R. M. 1984. Some applications of the first cohomology group, *J. Algebra*, **90**(2), 446–460.
[2] Ballester-Bolinches, A. and Ezquerro, L. M., Classes of finite groups, Mathematics and Its Applications (Springer), vol. 584, Springer, Dordrecht, 2006.
[3] Bidwell, J. N. S., Automorphisms of direct products of finite groups II, Arch. Mat. 91 (2008), 111–121.
[4] Dalla Volta, F. and Lucchini, A., Finite groups that need more generators than any proper quotient, J. Austral. Math. Soc., Series A, 64 (1998) 82–91.
[5] Doerk, K. and Hawkes, T., Finite soluble groups, de Gruyter, Berlin, 1992.
[6] Isaacs, I. M., Finite Group Theory, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, 2008.
[7] Jiménez-Seral, P. and Lafuente, J. On complemented nonabelian chief factors of a finite group, Israel J. Math. 106 (1998), 177–188.
[8] Kleidman, P. and Liebeck, M. W., The subgroup structure of the finite classical groups, CUP, Cambridge, 1990.
[9] Liebeck, M. W., Praeger, C. E. and Saxl, J., On the O'Nan-Scott Theorem for finite primitive permutation groups, J. Austral. Maths. Soc (Series A) 44 (1988), 389–396.