7. Minimal normal subgroups and the socle

Throughout this section G is a nontrivial group. A *minimal normal subgroup* of G is a normal subgroup $K \neq 1$ of G which does not contain any other nontrivial normal subgroup of G. The *socle*, $\mathrm{soc}(G)$ is the subgroup generated by the set of all minimal normal subgroups (if G has no minimal normal subgroups, then we set $\mathrm{soc}(G) = 1$).

> **(E7.1)** *Find the socle of D_{10}, A_4, S_4, $S_4 \times \mathbb{Z}$.*
>
> **(E7.2)** *Give an example of a group that has no minimal normal subgroup.*
>
> **(E7.3)** *If G is the direct product of a (possibly infinite) number of finite simple groups, then what is $\mathrm{soc}(G)$?*
>
> **(E7.4)** *Give a characterization of almost simple groups in terms of their socle.*

Clearly $\mathrm{soc}(G)$ is a characteristic subgroup of G. [26]

Theorem 7.1. *Let G be a nontrivial finite group.*

1. *If K is a minimal normal subgroup of G, and L is any normal subgroup of G, then either $K \leq L$ or $\langle K, L\rangle = K \times L$.*[27]
2. *There exist minimal normal subgroups $K_1, \dots, K_m$ of G such that $\mathrm{soc}(G) = K_1 \times \cdots K_m$.*
3. *Every minimal normal subgroup K of G is a direct product $K = T_1 \times \cdots T_k$ where the T_i are simple normal subgroups of K which are conjugate in G.*
4. *If the subgroups K_i in (2) are all nonabelian, then $K_1, \dots, K_m$ are the only minimal normal subgroups of G.*

Proof. (1) Since $K \cap L \trianglelefteq G$, the minimality of K implies that either $K \leq L$ or $K \cap L = \{1\}$. In the latter case, since K and L are both normal, we have that $\langle K, L\rangle = KL = K \times L$.

(2) Because G is finite we can find a set $S = \{K_1, \dots, K_m\}$ of minimal normal subgroups which is maximal with respect to the property that $H := \langle S\rangle = K_1 \times \cdots \times K_m$. We must show that H contains all minimal normal subgroups of G, and so is equal to $\mathrm{soc}(G)$. This follows immediately from (1).

(3) Let T be a minimal normal subgroup of K and observe that all conjugates T^g, for $g \in G$, are also minimal normal subgroups of K. Choose a set $S = \{T_1, \dots, T_m\}$ of these conjugates which is maximal with respect to the property that $L := \langle S\rangle = T_1 \times \cdots \times T_m$. Then, arguing *à la* (2), we see that L contains all of the conjugates of T under G and so $L \trianglelefteq G$. But, since $\{1\} < L \leq K$ and K is minimal normal, we conclude that $K = L = T_1 \times \cdots \times T_m$. Note, finally, that, for T_i to be minimal normal in $T_1 \times \cdots \times T_m$, we must have T_i simple.

(4) Let K be a minimal normal subgroup of G that is distinct from $K_1, \dots, K_m$, then, applying (1) with $L = K_i$, we find that $\langle K, L\rangle = K \times L$ and, in particular, K centralizes each of the K_i. Thus $K \leq Z(\mathrm{soc}(G))$. However if each K_i is nonabelian, then (3) implies that $Z(K_i) = \{1\}$ and we have a contradiction, as required.

□

Observe that if a minimal normal subgroup K is abelian, then K is an elementary-abelian p-group for some prime p.[28]

> **(E7.5)** *Suppose that G is elementary abelian. How many minimal (resp. maximal) normal subgroups does G have?*

---

[26] i.e. $\mathrm{soc}(G)$ is invariant under any automorphism of G. This is because any automorphism of G must permute the minimal normal subgroups of G.

[27] I am considering the *internal* direct product here, a special case of the internal semidirect product that we have already seen.

[28] Recall that an *elementary-abelian* p-group is defined to be a group that is isomorphic to $\underbrace{C_p \times \cdots \times C_p}_{n}$, where n is finite, p is a prime, and C_p is a cyclic group of order p.

7.1. **Finite groups with elementary abelian socle.** In this section G is a finite group with an elementary-abelian socle. We write

$$V := \mathrm{soc}(G) = \underbrace{C_p \times \cdots \times C_p}_{d}.$$

Observe that V has a natural structure as a vector space over $\mathbb{F}_p$, the field of order p. This allows us to make the following assertion.

Lemma 7.2. *$G/C_G(V)$ is isomorphic to a subgroup of $\mathrm{GL}(V)$, and $G/C_G(V)$ acts on V via multiplication (on the right) by matrices.*

Proof. Consider the action of G on V by conjugation. Lemma 3.2 implies that this induces a homomorphism $\phi : G \to \mathrm{Aut}(V)$ where we view V is an object from **Group**. Furthermore $C_G(V)$ is the kernel of ϕ and, in particular, it is a normal subgroup of G.

Now, since $C_G(V)$ is the kernel of the conjugation action, the first isomorphism theorem of groups implies that G/V is isomorphic to a subgroup of $\mathrm{Aut}(V)$. Now the result follows from (E7.6) below. □

(E7.6) *Let V be an elementary-abelian p-group.*

1. *Let G be a group of automorphisms of V as an object from* **Group**. *Prove that G* acts linearly *on V, i.e. prove that G is a group of automorphisms of V as an object from* $\mathbf{Vect}_{\mathbb{F}_p}$.
2. *Let G be a group of automorphisms of V as an object from* $\mathbf{Vect}_{\mathbb{F}_p}$. *Prove that G is a group of automorphisms of V as an object from* **Group**.
3. *Conclude that $\mathrm{Aut}(V) = \mathrm{GL}(V)$, whether we consider it an object of* **Group** *or of* $\mathbf{Vect}_{\mathbb{F}_p}$.

Let us strengthen our supposition: let us suppose that G *splits over* V, i.e. that there exists a subgroup $H < G$, such that $G = V \rtimes H$. To state the structure result in this case, we need a definition.

Given a vector space V over a field K, define

$$\mathrm{AGL}(V) := \{(g, v) \mid v \in K^d, g \in \mathrm{GL}(V)\} = K^d \rtimes \mathrm{GL}(V).$$

Here we write K^d to mean the additive group whose elements are d-tuples with entries from K. Multiplication is defined in the usual way for a semidirect product:

$$(g_1, v_1)(g_2, v_2) := (g_1, g_2, v_1^{g_2} v_2)$$

where, for $v \in K^n$ and $g \in \mathrm{GL}_d(K)$, we define v^g to be the product of v (thought of as a row vector) with g, a matrix.

Note that, just as with $\mathrm{GL}(V)$, we will write $\mathrm{AGL}_d(K)$ as a pseudonym for $\mathrm{AGL}(V)$. Furthermore, if $K = \mathbb{F}_p$ is finite, then we will write $\mathrm{AGL}_d(p)$ as a synonym for $\mathrm{AGL}_d(\mathbb{F}_p)$.

Proposition 7.3. *Suppose that G is a finite group with socle V of order p^d for some prime p. If G splits over V, then G is isomorphic to a subgroup of $\mathrm{AGL}_d(p)$.*

Proof. Let H be a subgroup of G such that $G = V \rtimes H$. Consider the action of H on V by conjugation.

We claim that $C_H(V)$ is a normal subgroup of G; indeed it is enough to prove that it is a normal subgroup of H, since $G = VH$ and $C_H(V)$ is certainly normalized by V. To prove the claim, take $h \in C_H(V), h_1 \in H$ and $v \in V$. Now observe that

$$\begin{aligned} v^{(h^{h_1})} &= (h^{h_1})^{-1} v (h^{h_1}) \\ &= (h_1^{-1} h h_1)^{-1} v (h_1^{-1} h h_1) \\ &= h_1^{-1}(h^{-1}(h_1 v h_1^{-1})h)h_1 \\ &= h_1^{-1}(h_1 v h_1^{-1})h_1 = v. \end{aligned}$$

Thus $h^{h_1} \in C_H(V)$ and the claim is proved. But now, since $H \cap V = \{1\}$, we know that $C_H(V) \cap V = \{1\}$ and so, since V is the socle, we conclude that $C_H(V) = \{1\}$.

Now consider $C_G(V)$. If $g \in G$, then $g = vh$ for a unique $v \in V$ and $h \in H$ and $g \in C_G(V)$ if and only if $h \in C_G(V)$. In particular,

$$C_G(V) = V.C_H(V) = V.$$

Now Lemma 7.2 implies that G/V is isomorphic to a subgroup of $\mathrm{GL}(V)$. Moreover the group $H \cong G/V$ acts on V by right multiplication by matrices; in other words $V \rtimes H$ is isomorphic to a subgroup of $\mathrm{AGL}_d(p)$ as required. □

(E7.7) *Suppose that K is finite.*
- *Prove that $\mathrm{soc}(\mathrm{AGL}_d(K)) \cong K^d$ and, moreover, that $\mathrm{soc}(\mathrm{AGL}_d(K))$ is a minimal normal subgroup of $\mathrm{AGL}_d(K)$.*
- *Suppose that $\mathrm{soc}(\mathrm{AGL}_d(K) \leq G \leq \mathrm{AGL}_d(K)$. Under what conditions is $\mathrm{soc}(\mathrm{AGL}_d(K))$ a minimal normal subgroup of G?*

(E7.8) *Describe the structure of $\mathrm{AGL}_1(p)$ for a prime p.*

7.2. **The socle of a primitive permutation group.**

Theorem 7.4. *If G is a finite primitive subgroup of $\mathrm{Sym}(n)$, and K is a minimal normal subgroup of G, then exactly one of the following holds:*

1. *for some prime p and some integer d, K is a regular elementary abelian group of order p^d, and $\mathrm{soc}(G) = K = C_G(K)$.*
2. *K is a regular non-abelian group, $C_G(K)$ is a minimal normal subgroup of G which is permutation isomorphic to K, and $\mathrm{soc}(G) = K \times C_G(K)$.*
3. *K is non-abelian and $\mathrm{soc}(G) = K$.*

Proof. Let $C = C_G(K)$. Since $C \trianglelefteq G$, either $C = 1$ or C is transitive. Since K is transitive, Lemma 3.7 implies that C is semiregular, and hence either $C = 1$ or C is regular.

Suppose that $C = 1$. Clearly K is non-abelian. Furthermore Theorem 7.1 (1) implies that K is the only minimal normal subgroup of G and so $\mathrm{soc}(G) = K$ and conclusion (3) of the result holds.

Suppose instead that C is regular. Then (E3.23) implies that $C_{\mathrm{Sym}(\Omega)}(C)$ is regular. Since $K \leq C_{\mathrm{Sym}(\Omega)}(C)$ and K is transitive, we conclude that $K = C_{\mathrm{Sym}(\Omega)}(C)$. Similarly, $C = C_{\mathrm{Sym}(\Omega)}(K)$ and, by (E3.24), C and K are permutation isomorphic.

Now, since C is regular, we conclude that C is a minimal normal subgroup of G (since any proper subgroup of C is intransitive). Now Theorem 7.1 (1) states that every minimal normal subgroup of G distinct from K is contained in C. Thus $\mathrm{soc}(G) = KC$ which equals K or $K \times C$ depending on whether $C \leq K$ or not.

If $C \leq K$, then $C = K$, K is abelian, $\mathrm{soc}(G) = K$ and conclusion (1) holds. If $C \not\leq K$, then conclusion (2) holds. □

(E7.9) *Suppose that G is a maximal primitive subgroup of $\mathrm{Sym}(n)$. Prove that G has a unique minimal normal subgroup (and so possibility (2) in Theorem 7.4 cannot occur).*[29]

(E7.10) *Suppose that K is a regular normal subgroup of G, a subgroup of $\mathrm{Sym}(n)$. Let H be the stabilizer of a point in the action on $\Omega := \{1, \dots, n\}$. Then $G = KH, K \cap H = \{1\}$ and, in particular, G splits over K, i.e. $G = K \rtimes H$.*

7.3. **Primitive permutation groups with abelian socle.** Our approach now is similar to that of §§5 and 6. In those sections we studied subgroups G of $\mathrm{Sym}(n)$ that preserved certain structures on the set $\{1, \dots, n\}$ (in §5, this was a G-congruence; in §6 it was a G-product structure). In this section the structure of interest is a *G-affine structure*.

It will be convenient to take a more categorical approach here, simply becaused the category associated to a G-affine structure is very standard. The category of interest is called $\mathbf{Aff}_K$; it is very similar to $\mathbf{Vect}_K$, but we are allowing more arrows.[30]

Objects: Objects are finite-dimensional vector spaces over the field K.

Arrows: An arrow $g : V_1 \to V_2$ is an *affine transformation*, i.e. a map that acts linearly on the difference between two vectors. In other words $g : V_1 \to V_2$ is an affine transformation if there exists a

[29] You may find it helpful to refer to the proof of (E3.23) and (E3.24).

[30] we have done this before – see Example 3 – but in a different direction.

linear transformation $h : V_1 \to V_2$ such that

$$v_2^g - v_1^g = (v_2 - v_1)^h.$$

Suppose that V is an object in $\mathbf{Aff}_K$. For $x \in V$ define the map

$$n_x : V \to V, v \mapsto v + x.$$

The map, n_x, is called the *translation* by the vector x and one can check that n_x is an arrow in $\mathbf{Aff}_K$.[31] The set of all translations

$$N := \{n_x \mid x \in V\}$$

is a subgroup of $\mathrm{Aut}(V)$. It is clear that any linear transformation of V is also an affine transformation, thus $\mathrm{GL}(V)$ is also a subgroup of $\mathrm{Aut}(V)$.

(E7.11) *Let V be a vector space. Prove that*
- $N \cap \mathrm{GL}(V) = \{1\}$, *where N is the set of translations of V;*
- $\mathrm{Aut}(V) = N \rtimes \mathrm{GL}(V) \cong \mathrm{AGL}_d(K)$ *where $d = \dim(V)$, the dimension of V as a vector space over K;*
- $\mathrm{AGL}(V)$ *acts faithfully and 2-transitively on V;*
- *The stabilizer of the zero vector is* $\mathrm{GL}(V)$.

Now let G be a subgroup of $\mathrm{Sym}(\Omega)$ where Ω is a finite set. An *affine structure* is a bijection $\theta : \Omega \to V$, where V is a finite-dimensional vector space over a finite field K. An affine structure is a *G-affine structure* if G acts on V as an object from $\mathbf{Aff}_K$.[32] By Lemma 3.2, if a G-affine structure exists, then the action of G on Ω yields a homomorphism $G \to \mathrm{Aut}(V)$. By (E7.11) $\mathrm{Aut}(V) \cong \mathrm{AGL}_d(p)$ for some positive integer d and some prime p.

Lemma 7.5. *Let Ω be a finite set of order n. Suppose that $\theta : \Omega \to V$ is an affine structure, where V is a d-dimensional vector space over a finite field $K = \mathbb{F}_p$.*

(1) *θ is a G-affine structure for a unique subgroup G of $\mathrm{Sym}(\Omega)$ that is isomorphic to $\mathrm{AGL}_d(p)$;*
(2) *if θ is a H-affine structure for some group $H \le \mathrm{Sym}(\Omega)$, then $H \le G$.*

Proof. We use θ to identify Ω with V throughout. We have seen that $\mathrm{Aut}(V) \cong \mathrm{AGL}_d(p)$ where we consider V an object from $\mathbf{Aff}_K$. By (E7.11), the action of $\mathrm{AGL}(V)$ on V, as a set, is faithful, thus $\mathrm{AGL}(V)$ is a subgroup of $\mathrm{Sym}(V)$.

Now suppose that θ is a H-affine structure for some group $H \le \mathrm{Sym}(\Omega)$. By definition every element of h is an arrow in $\mathbf{Aff}_K$ and so lies in $\mathrm{AGL}(V)$. We are done. □

Lemma 7.5 can be combined with Proposition 6.5 to yield the following.

Proposition 7.6. *Let $H \le \mathrm{Sym}(\Omega)$ where $|\Omega| < \infty$. One of the following holds:*

(1) *H is intransitive and $H \le \mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$ for some $1 < k < n$;*
(2) *H is transitive and imprimitive and $H \le \mathrm{Sym}(k) \wr \mathrm{Sym}(\ell)$ for some $1 < k, l < n$ with $n = kl$;*
(3) *H is primitive, preserves a non-trivial product structure, and $H \le \mathrm{Sym}(k) \wr \mathrm{Sym}(\ell)$ for some $1 < l < n$, $2 < k < n$ with $n = k^l$;*
(4) *H is primitive, preserves an affine structure, and $H \le \mathrm{AGL}_d(p)$ for some $d > 1$ and prime p with $n = p^d$;*
(5) *H is primitive and preserves neither an affine structure nor a non-trivial product structure.*

We have seen examples of subgroups of $\mathrm{Sym}(\Omega)$ of every given type, except those that are primitive and preserve an affine structure. To see that the latter type of group really exisits, recall that $\mathrm{AGL}_d(p)$ acts 2-transitively on the associated vector space, thus, in particular, it is primitive; of course, by definition, it also preserves an affine structure.

[31] Indeed, a translation is precisely an affine map for which the associated linear map is the identity.

[32] As usual, I am identifying Ω with $\theta(\Omega)$ so that I can talk of 'G acting on V'. If I wanted to make this precise, I would define the action of G on V via

$$v^g := \theta((\theta^{-1}(v))^g).$$

(E7.12) *Let* $\mathrm{AGL}_d(p) = \mathrm{Aut}(\Omega)$ *for* Ω *an object from* $\mathbf{Aff}_K$. *Can you specify necessary and sufficient conditions for a subgroup* $G \leq \mathrm{Aut}(\Omega)$ *to act primitively on* Ω.

The following exercise implies that Proposition 7.6 can be strengthened by requiring that $4 < k$ for possibility (3).

(E7.13) *Let* G *be a subgroup of* $\mathrm{Sym}(k^\ell)$ *with* $k \in \{3,4\}$, *and suppose that* $G \cong \mathrm{Sym}(k) \wr \mathrm{Sym}(\ell)$ *in the product action. Prove that if* $k \leq 5$, *then* G *preserves an affine structure, and describe the group* $\mathrm{AGL}_d(p)$ *in* $\mathrm{Sym}(k^\ell)$ *that contains* G.

7.4. **The socle and affine structures.** Our job now is to connect our knowledge about the socle of a primitive permutation group with the work in the previous section on affine structures.

Lemma 7.7. *Suppose that* G *is a subgroup of* $\mathrm{Sym}(\Omega)$ *and that* G *contains a normal regular subgroup* K. *Let* H *be the stabilizer of any point of* ω. *The action of* G *on* Ω *is permutation isomorphic to the action of* G *on the set* K *given by*

$$\varphi : G \times K \to K, (g, k_1) \mapsto (k_1 k)^h$$

where $g = kh$ *for some* $k \in K$ *and* $h \in H$.

It is important to realise that the given action of G on K **is not** an action of G on K as an object from Group.[33] Note, too, that we are not assuming that Ω is finite here.

Proof. Fix $\omega \in \Omega$ and define a function $\beta : K \to \Omega, k \mapsto \omega^k$. Since K is regular this function is a bijection. Let $1 : G \to G$ be the identity map, and let ψ be the action of G on Ω given by the embedding of G in $\mathrm{Sym}(\Omega)$. Now the result is equivalent to proving that the following diagram commutes:

$$\begin{tikzcd} G \times K \arrow[r, "\varphi"] \arrow[d, "{(1,\beta_\omega)}"'] & K \arrow[d, "\beta_\omega"] \\ G \times \Omega \arrow[r, "\psi"] & \Omega \end{tikzcd} \qquad \begin{tikzcd} (g, k_1) \arrow[r, mapsto, "\varphi"] \arrow[d, mapsto, "{(1,\beta_\omega)}"'] & (k_1 k)^h \arrow[d, mapsto, "\beta_\omega"] \\ (g, \omega^{k_1}) \arrow[r, mapsto, "\psi"] & (*) \end{tikzcd}$$

Write $g = kh$ for some $k \in K$ and $h \in H$. If we follow the diagram from the top-left corner, down and across, then $(*) = \omega^{k_1 g} = \omega^{k_1 kh}$. On the other hand, if we go right and then down, we obtain

$$(*) = \omega^{(k_1 k)^h} = \omega^{h^{-1} k_1 kh} = (\omega^{h^{-1}})^{k_1 kh} = \omega^{k_1 kh}$$

and we are done. □

Proposition 7.8. *Suppose that* G *is a subgroup of* $\mathrm{Sym}(n)$ *and that* G *contains a normal regular elementary abelian subgroup* V. *Then there is a* G*-affine structure* $\theta : \Omega \to V$, *and there is a group* M *such that* $G \leq M \leq \mathrm{Sym}(n)$ *with* $M \cong \mathrm{AGL}(V)$.

Proof. By Lemma 7.7 we know that the action of G on Ω is permutation isomorphic to the action φ on V. Thus it is enough to show that φ is an action of G on V as an object from $\mathbf{Aff}_K$.

Let H be the stabilizer of 0, the identity element in V, and recall that, by (E7.11), $H = \mathrm{GL}(V)$. Let $g \in G$ and let $h \in H, v \in V$ be the unique elements such that $g = vh$. Let $v_1, v_2 \in V$ and observe that

$$v_1^g - v_2^g = (v_1 + v)^h - (v_2 + v)^h = v_1^h + v_h - v_2^h - v^h = v_1^h - v_2^h = (v_1 - v_2)^h$$

as required. □

[33] To see why you should think of the effect of this action on the identity of K.

7.5. **What is left.** Recall that we are trying to understand the subgroups of $\mathrm{Sym}(n)$, and that, by Proposition 5.8, this amounts to understanding the primitive subgroups. Now Theorem 7.4 gives three possibilities for a primitive subgroup, and Proposition 7.8 gives a full description for possibility (1).

If, moreover, we restrict our attention to *maximal* primitive subgroups of $\mathrm{Sym}(n)$, then (E7.9) implies that possibility (2) cannot occur.

Thus we can state the following corollary to Theorem 7.4:

Corollary 7.9. *If M is a finite maximal primitive subgroup of $\mathrm{Sym}(n)$, and K is a minimal normal subgroup of G, then exactly one of the following holds:*

(1) *$n = p^d$ for some prime p and some integer d, and $M = \mathrm{AGL}_d(p)$.*
(2) *K is non-abelian and $\mathrm{soc}(G) = K$.*

Thus, to understand the maximal subgroups of $\mathrm{Sym}(n)$, we need to understand those finite primitive groups that have a unique minimal normal subgroup K that is nonabelian. It is beyond the scope of this course to properly analyse this situation, although we will at least be able to state a theorem pertaining to this situation in the next section. Before we get there, though, let us observe that we have already seen two examples of primitive subgroups of this kind:

- In Exercise 16 we looked at actions of $\mathrm{Sym}(n)$ on the coset spaces of maximal subgroups other than $\mathrm{Alt}(n)$. This situation can be generalized to cover the action of any almost simple group G on the coset space of a maximal subgroup that does not contain $\mathrm{soc}(G)$.
- In §6 we considered the product action of the wreath product $W := \mathrm{Sym}(k) \wr \mathrm{Sym}(\ell)$, and the next exercise shows we have another example.

  (E7.14) *Let k and ℓ be integers with $k \geq 5$. Show that $W := \mathrm{Sym}(k) \wr \mathrm{Sym}(\ell)$ has a unique minimal normal subgroup, and give its isomorphism type.*