Part (i) of Schur-Zassenhaus

The Schur-Zassenhaus Theorem is a fundamental result about coprime actions in finite group theory. Specifically, what it says is:

Let G be a finite group, and let N be a normal subgroup of G such that $\gcd\left(|N|, [G : N]\right) = 1$. Then:

(i) G has a subgroup H such that $H \cong G/N$.

(ii) Any two such subgroups of G are conjugate in G.

The purpose of this note is to give a proof of (i) (referred to as S-Z(i) for short) using affine geometry over fields of prime order. The two reductions that carry the reasoning into the case where N is an elementary abelian group of prime-power order are standard; after that, and after the structure of N is narrowed down, I don't know how different the reasoning employed here turns out to ultimately be from reasoning used elsewhere.

Recognizing complements to N in G

A *complement* to N in G, by definition, is a subgroup consisting of one element from each coset of N in G. Such a subgroup is easily seen to be isomorphic to G/N. Since there are $[G : N]$ cosets of N in G, this means any complement to N in G has order $[G : N]$. In the context of the Schur-Zassenhaus Theorem, however, a convenient converse is easy and useful to prove:

Claim. If H is a subgroup of G and $|H| = [G : N]$, then H is a complement to N in G.

Proof of Claim. If H does not consist of one element from each coset of N in G, then, since $|H| = [G : N]$, some coset of N will contain two different elements of H; call these elements x and y. Then, since x and y are in the same coset of N, $xy^{-1} \in N$. Also, since x and y are elements of H, $xy^{-1} \in H$. Since $x \neq y$ by assumption, $xy^{-1} \neq 1$. Then $H \cap N$ is nontrivial, since $xy^{-1} \in H \cap N$.

But $H \cap N$ must be trivial: $|H \cap N| \mid |H|$ and $|H \cap N| \mid |N|$, so $|H \cap N| \mid \gcd(|H|, |N|) = \gcd([G : N], |N|) = 1$. Therefore $|H \cap N| = 1$. This contradiction proves the Claim.

It's worth noting that S-Z(i) is trivially true when $|N| = 1$, since G itself is a complement to N in that case. Therefore, in what follows, we will assume $|N| > 1$.

The first reduction

In finite group theory, when we refer to a minimal normal subgroup of G, we don't want to refer to the trivial subgroup. We know the trivial subgroup is a normal subgroup of any group, so we exclude that from consideration (otherwise, we'd always be referring to it): a minimal normal subgroup of G is a normal subgroup which is minimal, with respect to inclusion, among normal subgroups other than the trivial subgroup. (This is analogous to the usage of "maximal" in "maximal subgroup".) This appears in the statement of Reduction 1:

Reduction 1. If G is a counterexample to S-Z(i) minimizing $|G|$, then N is a minimal normal subgroup of G.

Proof of Reduction 1. Suppose not; then there is a normal subgroup $K \triangleleft G$ which is a proper subgroup of N. Then $N/K \triangleleft G/K$. In fact, N/K is a normal subgroup satisfying the hypothesis of S-Z(i):

$$\gcd\left(|N/K|, [G/K : N/K]\right) = \gcd\left(|N/K|, [G : N]\right) \mid \gcd\left(|N|, [G : N]\right) = 1$$

from which it follows that $\gcd\left(|N/K|, [G/K : N/K]\right) = 1$.

Since K is nontrivial, $|G/K| < |G|$. Then the minimality of G, as a counterexample to S-Z(i), implies that S-Z(i) applies to G/K. So let L be a complement to N/K in G/K. Note that
$|L| = [G/K : N/K] = [G : N]$.

Now let's lift back to G. Let C be the lift of L from G/K to G. Then $|C| = |L||K| = [G : N]|K|$. But, as a lift, C contains K as a normal subgroup. In fact, the conditions of S-Z(i) apply to C, since

$$\gcd\left(|K|, [C : K]\right) = \gcd\left(|K|, [G : N]\right) \mid \gcd\left(|N|, [G : N]\right) = 1$$

and therefore $\gcd\left(|K|, [C : K]\right) = 1$. Also, we know that

$$|C| = |L||K| = [G : N]|K| < [G : N]|N| = |G|$$

so $|C| < |G|$. Then S-Z(i) applies to C and implies that C has a complement H to K, whose order is $|C/K| = [G : N]$. This implies, as explained earlier, that H is a complement to N in G. But then G isn't a counterexample to S-Z(i), so this contradiction establishes Reduction 1.

The second reduction

The following is an instance of what is sometimes called 'the Frattini argument', although, as Isaacs [1] has observed, maybe it's more accurate to call it *a* Frattini argument, since reasoning like this has so many variations on it.

Reduction 2. If G is a counterexample minimizing $|G|$, then $|N|$ is a power of a prime.

Proof of Reduction 2. As already established, if G is a counterexample to S-Z(i), we must have $|N| > 1$. Then let p be a prime factor of $|N|$.

Since $p \mid |N|$, $p \nmid [G:N]$. This means any power of p dividing $|G|$ will divide $|N|$. Therefore, all Sylow p-subgroups of G are Sylow p-subgroups of N. Let P be a Sylow p-subgroup of G. Then the Sylow counting theorem tells us (again following Isaacs, using $n_p(X)$ to denote the number of Sylow p-subgroups of the finite group X) that

$$|N| = |\mathbf{N}_N(P)| n_p(N)$$

and

$$|G| = |\mathbf{N}_G(P)| n_p(G) = |\mathbf{N}_G(P)| n_p(N)$$

and therefore

$$\frac{|\mathbf{N}_G(P)|}{|\mathbf{N}_N(P)|} = \frac{|G|}{|N|} = [G:N]$$

Since $\mathbf{N}_N(P) = \mathbf{N}_G(P) \cap N$, this means the number of cosets of N in G containing elements normalizing P is $[G:N]$. Therefore every coset of N in G contains elements normalizing P.

If $|\mathbf{N}_G(P)| < |G|$ (that is, if P is not a normal subgroup of G), then S-Z(i) applies to $\mathbf{N}_G(P)$:

Since $|\mathbf{N}_G(P)| = |\mathbf{N}_N(P)|[G:N]$, we have

$$\gcd\left(|\mathbf{N}_N(P)|, [G:N]\right) \mid \gcd\left(|N|, [G:N]\right) = 1$$

and therefore S-Z(i) says there is a complement, H, to $\mathbf{N}_N(P)$ in $\mathbf{N}_G(P)$. Then, since
$|H| = [G:N]$, H is a complement to N in G and G is not a counterexample in this case.

Then we are forced to conclude that, in the minimal counterexample G, $|\mathbf{N}_G(P)| = |G|$ so $\mathbf{N}_G(P) = G$ and P is a normal subgroup of G. Since P is a subgroup of N and N is a minimal normal subgroup of G, this forces $N = P$ so that $|N|$ is a power of p. Reduction 2 is done.

Now write $|N| = p^k$, where k is a positive integer. In the rest of the proof, G is a counterexample to S-Z(i) of minimal order, so that Reductions 1 and 2 may be applied.

What does that tell us about N?

If X_1 is a characteristic subgroup of X_2 and X_2 is a normal subgroup of X_3, then X_1 is a normal subgroup of X_3. Then, the fact that N is a minimal normal subgroup of G implies that N has no proper characteristic subgroups.

Definition. Let q be a prime and let n be a positive integer. A group of order q^n is called *elementary abelian* if it's isomorphic to the Cartesian product of n cyclic groups of order q.

Theorem. If Y is a nontrivial finite group whose order is a power of a prime, and Y has no proper characteristic subgroups, then Y is elementary abelian.

Proof of Theorem. Suppose $|Y| = q^m$, where q is a prime and m is a positive integer. We establish the conclusion using two steps:
Step 1. Y is abelian.

Proof of Step 1. Since $|Y| = q^m$ where q is prime and m is a positive integer, the center $\mathbf{Z}(Y)$ is nontrivial. Since the center is always a characteristic subgroup, the condition on Y implies that $\mathbf{Z}(Y) = Y$. In other words, Y is abelian, and Step 1 is done.

Step 2. Y is elementary abelian.

Proof of Step 2. Since Y is abelian, the subset of Y consisting of the identity and all the elements of order q is a subgroup of Y. Its definition makes it clear that it's also a nontrivial characteristic subgroup of Y. Therefore it must be all of Y, from which it's easy to see that Y is elementary abelian. Step 2 is done, and the Theorem is proven.

The sets on which G acts, and the correspondence between them

The heavy lifting of this proof is accomplished by considering the action of G on a certain pair of sets, each consisting of $p^{[G:N]}$ elements.

To start defining these G-actions, we need to make some choices. Let $t_1, \ldots, t_{[G:N]}$ be a set of representatives for the cosets of N in G. Also, let V be chosen as a subgroup of N such that $[N : V] = p$.

Now we want to choose, for each i with $1 \leq i \leq [G : N]$, an $x_i \in N$ that cycles around the p right cosets of V contained in Nt_i. First of all, this means $Nt_ix_i = Nt_i$, which is equivalent to:

$$Nt_ix_i = Nt_i, \text{ or, equivalently,}$$

$$Nt_ix_it_i^{-1} = N, \text{ or, equivalently,}$$

$$t_ix_it_i^{-1} \in N, \text{ or, equivalently,}$$

$$x_i \in N$$

One right coset of V that is contained in Nt_i is Vt_i. Since $x_i \in N$, x_i cycles the right cosets of V in Nt_i as long as we don't have $Vt_ix_i = Vt_i$. In other words, what we want is:

$$Vt_ix_i \neq Vt_i, \text{ or, equivalently,}$$

$$Vt_ix_it_i^{-1} \neq V, \text{ or, equivalently,}$$

$$t_ix_it_i^{-1} \notin V, \text{ or, equivalently,}$$

$$x_i \notin t_i^{-1}Vt_i$$

So choosing $x_i \in N \setminus t_i^{-1} V t_i$ is both necessary and sufficient to enable x_i to act as desired. For each i with $1 \leq i \leq [G : N]$, now fix a choice of $x_i \in N \setminus t_i^{-1} V t_i$.

One of the sets on which G acts is the set of choices of a right coset of V within each coset of N. An element of this looks like $\{V t_i u_i \subset N t_i\}_{1 \leq i \leq [G:N]}$, where $u_i \in N$ for all i with $1 \leq i \leq [G : N]$. $g \in G$ acts on this set by right-multiplication; i.e., by sending $\{V t_i u_i \subset N t_i\}_{1 \leq i \leq [G:N]}$ to $\{V t_i u_i g \subset N t_i g\}_{1 \leq i \leq [G:N]} = \{V t_i g (g^{-1} u_i g) \subset N t_i g\}_{1 \leq i \leq [G:N]}$.

The other set on which G acts is the set of functions $f : G/N \to \mathbb{Z}/(p)$. This set can be naturally regarded as an affine space over $\mathbb{Z}/(p)$.

We define a bijection between these sets by identifying the function $f : G/N \to \mathbb{Z}/(p)$ with the set of right coset choices $\{V t_i x_i^{f(i)} \subset N t_i\}_{1 \leq i \leq [G:N]}$. This is how the action of G is carried over from the former set to the latter, and how the affine space structure is carried over from the latter to the former. This enables us to use these identifications to think of G as acting on a single set, which has the structure of a $\mathbb{Z}/(p)$-affine space on it. This set will be denoted Ψ, and called the *space of coset functions*, short for "functions from the cosets of N in G to $\mathbb{Z}/(p)$".

Since we have these G-actions set up, we wish to prove a few basic facts about them: G acts faithfully (on either set, since these actions are equivalent), G acts by affine transformations, and N acts by translations. Then it will be possible to assemble these into a proof of S-Z(i).

G acts faithfully

To say that g preserves the choice of $V t_i u_i$ within $N t_i$ is to say that $g \in u_i^{-1} t_i^{-1} V t_i u_i$. To say that is true over all i with $1 \leq i \leq [G : N]$ is to say that

$$g \in \bigcap_{1 \leq i \leq [G:N]} u_i^{-1} t_i^{-1} V t_i u_i$$

Since $t_i^{-1}Vt_i \subset N$, $u_i \in N$, and N is abelian, $u_i^{-1}t_i^{-1}Vt_iu_i = t_i^{-1}Vt_i$. Since the t_i form a set of coset representatives for N in G, and N normalizes $t_i^{-1}Vt_i$, $\bigcap_{1\leq i\leq [G:N]} t_i^{-1}Vt_i$ is the intersection of all G-conjugates of V. In other words, it's the core of V in G. Since N is a minimal normal subgroup of G and $[N:V] = p > 1$, the core of V in G must be trivial so G acts faithfully on Ψ.

In fact, this argument shows also that any nonidentity element of N acts without fixed points on Ψ.

G acts affinely

The next step is to prove that G acts by affine transformations on Ψ. However, because of fundamental differences in how the underlying geometry works, it's helpful to divide this proof into cases depending on the value of p: p might be an odd prime, or p might be 2.

G acts affinely when p is an odd prime

First, assume that p is an odd prime. Unless $p = 3$ and $d = 1$, the affine group $\mathbf{AGL}_d(\mathbb{Z}/(p))$acts with transitivity degree 2 (i.e., doubly transitively, but not triply transitively) on the p^d points of a d-dimensional affine space over $\mathbb{Z}/(p)$. (If $p = 3$ and $d = 1$, then the fact that $\mathbf{AGL}_1(\mathbb{Z}/(3)) \cong S_3$ means all permutations are affine transformations, so the conclusion follows automatically. So, if $p = 3$, the reader is free to assume that $d \geq 2$, though it isn't strictly necessary.) This means we can use a ternary relation on coset functions to prove the affineness of the action of G:

Affineness Lemma, odd prime version. If d is a positive integer, a permutation of a d-dimensional affine space over $\mathbb{Z}/(p)$ is affine if and only if it sends 3-term arithmetic progressions to 3-term arithmetic progressions.

Proof of Affineness Lemma. Since $p \geq 3$, a permutation of affine space is affine if and only it preserves, for all $t \in \mathbb{Z}/(p)$, the binary operation combining u and v to

obtain $t \cdot u + (1-t)v$.

If a permutation sends 3-term arithmetic progressions to 3-term arithmetic progressions, then it preserves the binary operation combining u and v to obtain $2v - u$, since $2v - u$ is the third term of the arithmetic progression beginning with u and v. Then it must also preserve $3v - 2u = 2(2v - u) - v$, and $4v - 3u = 2(3v - 2u) - (2v - u)$. Continuing in this fashion, we see this permutation must preserve $k \cdot v - (k-1)u = k \cdot v + (1-k)u$ for all positive integers k. This allows k to be an arbitrary element of $\mathbb{Z}/(p)$, so the permutation must be affine.

If a permutation is affine, then, for any distinct points u and v in the space, it preserves the binary operation combining u and v to obtain $2v - u$, which completes the 3-term arithmetic progression whose first two terms are u and v. So then it sends 3-term arithmetic progressions to 3-term arithmetic progressions, and the Lemma is proven.

(a, b, c) is an ordered triple of functions from G/N to $\mathbb{Z}/(p)$ forming an arithmetic progression if and only if, for all i with $1 \leq i \leq [G : N]$, the ith coordinates $(a(i), b(i), c(i))$ form an arithmetic progression in $\mathbb{Z}/(p)$. To say that is to say we have right V-cosets chosen as

$$\begin{gathered} Vt_i x_i^{a(i)} \subset Nt_i, \\ Vt_i x_i^{b(i)} \subset Nt_i, \\ Vt_i x_i^{c(i)} \subset Nt_i \end{gathered}$$

such that $b(i) - a(i) = c(i) - b(i)$. Equivalently, since this arithmetic progression is obtained by right-multiplying by a fixed element of G, it is more pertinent to say that $(t_i x_i^{a(i)})^{-1} t_i x_i^{b(i)} = (x_i^{a(i)})^{-1} x_i^{b(i)} = (x_i^{b(i)})^{-1} x_i^{c(i)} = (t_i x_i^{b(i)})^{-1} t_i x_i^{c(i)}$. Right-multiplying by g takes these choices of right V-cosets within their respective N-cosets to

$$Vt_ix_i^{a(i)}g \subset Nt_ig,$$
$$Vt_ix_i^{b(i)}g \subset Nt_ig,$$
$$Vt_ix_i^{c(i)}g \subset Nt_ig$$

To say that these chosen right V-cosets within the N-coset Nt_ig are in arithmetic progression is to say that

$$(x_i^{a(i)}g)^{-1}(x_i^{b(i)}g) = (x_i^{b(i)}g)^{-1}(x_i^{c(i)}g), \text{ or equivalently,}$$

$$g^{-1}(x_i^{a(i)})^{-1}x_i^{b(i)}g = g^{-1}(x_i^{b(i)})^{-1}x_i^{c(i)}g, \text{ or equivalently,}$$

$$(x_i^{a(i)})^{-1}x_i^{b(i)} = (x_i^{b(i)})^{-1}x_i^{c(i)}$$

which we were already assuming. As Nt_i varies over all cosets of N in G, so does Nt_ig. Therefore the arithmetic progression condition holds in each coordinate of (a^g, b^g, c^g). This means any $g \in G$ sends 3-term arithmetic progressions to 3-term arithmetic progressions and therefore G acts affinely, as claimed.

G acts affinely when $p = 2$

Now we assume that $p = 2$. Unless $d = 1$ or 2, the affine group $\mathbf{AGL}_d(\mathbb{Z}/(2))$ acts with transitivity degree 3 (i.e., triply transitively, but not quadruply transitively) on the 2^d points of a d-dimensional affine space over $\mathbb{Z}/(2)$. This means that there is no ternary relation involving coset functions we can use to prove the affineness of the action of G in this case. (If $d = 1$, then the fact that $\mathbf{AGL}_1(\mathbb{Z}/(2)) \cong S_2$ means the conclusion is automatic, as before. If $d = 2$, then the fact that $\mathbf{AGL}_2(\mathbb{Z}/(2)) \cong S_4$ means the conclusion is likewise automatic. So the reader is free to assume that $d \geq 3$, though only $d \geq 2$ is strictly necessary.) Instead, we can use the only quaternary relation preserved by the action of $\mathbf{AGL}_d(\mathbb{Z}/(2))$:

Affineness Lemma, $p = 2$ version. Let $d \geq 2$ be an integer. Then a permutation of a d-dimensional affine space over $\mathbb{Z}/(2)$ is affine if and only if it sends planes to planes.

Proof of Affineness Lemma. A permutation is affine if and only if it preserves all 1-sum linear combinations of points in the space. Since $\mathbb{Z}/(2) = \{0, 1\}$, a permutation of an affine space over $\mathbb{Z}/(2)$ is affine if and only if it preserves all sums of oddly many points in the space. Any such sum can be built from sums of 3 points: $v_1 + v_2 + v_3 + v_4 + v_5 = (v_1 + v_2 + v_3) + v_4 + v_5$, $v_1 + v_2 + v_3 + v_4 + v_5 + v_6 + v_7 = (v_1 + v_2 + v_3 + v_4 + v_5) + v_6 + v_7$, and so forth. So a permutation is affine if and only if it preserves all sums of 3 points in the space. That is, a permutation f of the space is affine if and only if, for all u, v, and w in the space, $(u + v + w)^f = u^f + v^f + w^f$.

If u, v, and w are distinct, then they cannot be collinear, since each line in the space consists of just 2 points. But there is a unique plane passing through them, and the sum of the points on this plane is the zero vector. (And, conversely, any set of 4 points in the space forms a plane when their sum is the zero vector.) That means the fourth point on this plane is $-(u + v + w) = u + v + w$.

But then the affineness condition says that f takes the plane $\{u, v, w, u + v + w\}$ to the set $\{u^f, v^f, w^f, u^f + v^f + w^f\}$. Since the points in this new set also have a sum equal to the zero vector and they are distinct, they, too, form a plane. Since u, v, and w are arbitrary distinct points in the space, this proves f preserves all planes in the space. Conversely, any permutation of the space sending planes to planes, for this reason, satisfies the affineness condition described above. We are done.

In any coordinate system (as long as the projection maps to individual coordinates are affine maps, as happens here because the coordinates define the affine structure) for an affine space over $\mathbb{Z}/(2)$, $u + v + w + x = \overrightarrow{0}$ if and only if, for all i indexing the set of coordinates, $u_i + v_i + w_i + x_i = 0$. $u_i + v_i + w_i + x_i = 0$, in turn, is equivalent to saying that the values, in $\mathbb{Z}/(2)$, assumed by u_i, v_i, w_i, and x_i are all equal, or equal in pairs (e.g., $u_i = w_i = 1$ while $v_i = x_i = 0$).

$\{a, b, c, d\}$ is a set of 4 (different) coset functions forming a plane if and only if, for all i with
$1 \leq i \leq [G : N]$, the ith coordinates $\{a(i), b(i), c(i), d(i)\}$ add up to 0 in $\mathbb{Z}/(2)$. To say that is to say we have right V-cosets chosen as

$$\begin{aligned} Vt_i x_i^{a(i)} &\subset Nt_i, \\ Vt_i x_i^{b(i)} &\subset Nt_i, \\ Vt_i x_i^{c(i)} &\subset Nt_i, \\ Vt_i x_i^{d(i)} &\subset Nt_i \end{aligned}$$

such that $\{a(i), b(i), c(i), d(i)\}$ are all equal, or equal in pairs. Right-multiplying by g preserves equality/distinctness of the right V-coset choices, so it preserves their being all equal, or being equal in pairs, within Nt_i, for all i. Therefore the coplanarity condition holds in each coordinate of $\{a^g, b^g, c^g, d^g\}$. This means any $g \in G$ sends planes to planes, and therefore G acts affinely, as claimed.

N acts by translations

It follows from the normality of N that N fixes each coset of N in G. When we break up each coset of N into p right cosets of V, then, since N is a p-group, N either cycles the right cosets of V around or it fixes all of them.

The choice of x_i, as an element of N, was made so that it does not fix Vt_i, so N must cycle around the p right V-cosets in each N-coset. That also means that every element of N cycles around these cosets exactly the way some power of x_i does. A power of x_i, say x_i^T, sends the right V-coset $Vt_i x_i^E$ to $Vt_i x_i^{E+T}$, for all $E \in \mathbb{Z}/(p)$. Therefore any element of N acts by translations on the right cosets of V in Nt_i, and, since i is arbitrary, N acts by translations on the whole space of coset functions.

Putting all the pieces together

G acts by affine transformations on Ψ, and, in this action, the normal subgroup N acts by translations. For $f_1, f_2 \in \Psi$, define $f_1 \sim f_2$ to mean that there is an element of N translating f_1 to f_2. Since every nonidentity element of N acts without fixed points on Ψ, every orbit of N on Ψ has size $|N|$.

Affine structure on $\Psi/\sim$: Let $\lambda, \mu \in \mathbb{Z}/(p)$. Suppose $u, v, w \in \Psi$. We need to verify that $u' \in \Psi$ and $u \sim u'$ imply that $\lambda u + \mu v + (1 - \lambda - \mu)w \sim \lambda u' + \mu v + (1 - \lambda - \mu)w$.

So let τ be the element of N such that $u^\tau = u'$. Then it's easy to compute that applying the translation $\lambda\tau$ carries $\lambda u + \mu v + (1 - \lambda - \mu)w$ to $\lambda u' + \mu v + (1 - \lambda - \mu)w$. This means the affine space structure present on Ψ is inherited by $\Psi/\sim$.

Groups acting on $\Psi/\sim$: G acts affinely on Ψ, and Ψ's affine structure is inherited by $\Psi/\sim$. So G acts affinely on $\Psi/\sim$. In the action on $\Psi/\sim$, N acts trivially. So the affine action of G on $\Psi/\sim$ gives us an affine action of G/N on $\Psi/\sim$.

Using the averaging trick: $\Psi/\sim$ is an affine space over $\mathbb{Z}/(p)$, and G/N is an affinely acting group whose order is a nonmultiple of p. This means that it's possible to average over the action of G/N to obtain a fixed point for it: specifically, consider

$$\overline{h} = \frac{1}{|G/N|} \sum_{g \in G/N} v^g,$$

for $v \in \Psi/\sim$.

Back to Ψ and G: Let $h \in \Psi$ be an element of the $\sim$-equivalence class $\overline{h}$. Then h has $|N|$ images under the action of G on coset functions: $\overline{h} = h/\sim$ is a fixed point for the action of G/N, but every nonidentity element of N has no fixed points in its action on Ψ. This means that, by the Orbit-Stabilizer Theorem, the stabilizer of h under the action of G is a subgroup of order $|G|/|N| = [G : N]$. As proven earlier, this subgroup is a complement to N in G. This proves S-Z(i), so we are done.

Reference

[1] I. Martin Isaacs. *Finite Group Theory*. Graduate Studies in Mathematics, vol. 92. American Mathematical Society, Providence, 2008.