Blackbox for now:

Given a finite group G & a G-module A, $H < G$

we can define homomorphisms $H^n(G,A) \xrightarrow{\mathrm{res}^G_H} H^n(H,A)$

and $H^n(H,A) \xrightarrow{\mathrm{cor}^G_H} H^n(G,A)$

& these satisfy
$$\begin{tikzcd} H^n(G,A) \arrow[r, "\mathrm{res}"] \arrow[rr, bend right, "\cdot [G:H]"'] & H^n(H,A) \arrow[r, "\mathrm{cor}"] & H^n(G,A) \end{tikzcd}$$

From this it follows:

Lem: $H^n(G,A)$ is $|G|$-torsion.

i.e. $\forall \alpha \in H^n(G,A)$, $|G|\cdot\alpha = 0$

Pf:
$$\begin{tikzcd} H^n(G,A) \arrow[r, "\mathrm{res}"] \arrow[rr, bend right, "\cdot |G|"'] & H^n((e),A) \arrow[r, "\mathrm{cor}"] & H^n(G,A) \end{tikzcd}$$

$H = (e)$

but $H^n((e),A) = 0$ since

exercise: given any $\alpha \in Z^n(G,A)$ can find

$\alpha' \sim \alpha$ s.t. $\alpha'(e,\dots,e) = 0$ $\square$

But also, if A is finite,

$H^n(G,A)$ is $|A|$ torsion since $C^n(G,A)$ is $|A|$ torsion
$$C^n(G,A) = A^{|G|^n}$$

So useful corollary: if $(|G|,|A|) = 1$ then $H^n(G,A) = 0$

Def: If G is a finite group, we say $H < G$ is Hall if $(|H|, |G/H|) = 1$

If π is a set of prime numbers, we say that H is π-Hall if $|H|$ is divisible only by the primes in π and $[G:H]$ is divisible by none of the primes in π.

ex: $|G| = 50 = 2 \cdot 5^2$ then a subgp of order 25 is $\{5\}$-Hall & $\{3,5\}$ Hall

Def if $H \trianglelefteq G$ is Hall, $K < G$ is a complement for H is K is Hall & $|H||K| = |G|$

Theorem (Schur–Zassenhaus lemma)
If G is finite, $K \trianglelefteq G$ normall Hall subgroup then K has a complement

Proof: *Case 1*: K Abelian. Then $\bar{G} = G/K$ acts on K via $\varphi: \bar{G} \to \operatorname{Aut} K$. But all extensions & G is an extension of $\bar{G}$ by K. of $\bar{G}$ by K w/ action φ are classified by $H^2(\bar{G}, K)$ where the trivial element $0 \in H^2(\bar{G}, K)$ corresponds to $K \rtimes_\varphi \bar{G}$

but K Hall $\Rightarrow (|K|, \underset{|\bar{G}|}{|G/K|}) = 1 \Rightarrow H^2(\bar{G}, K) = 0$.

$\Rightarrow$ every extension is split $\Rightarrow G$ is a split extension $\Rightarrow$ get a complement.

Case 2: A is not Abelian.

Lemma: "The Frattini Argument"

if $K \trianglelefteq G$ finite, $P \in \mathrm{Syl}_p K$, then $G = K N_G(P)$

(slogan: as K shrinks, normalizers of its Sylows grow)

Pf: if $g \in G$, consider ${}^gP < {}^gK = K \Rightarrow {}^gP \in \mathrm{Syl}_p K$

$\Rightarrow \exists k \in K$ s.t. ${}^gP = {}^kP \Rightarrow {}^{k^{-1}g}P = P$ i.e.

$k^{-1}g \in N_G P \Rightarrow g \in k N_G P$

$\cap$

$K N_G P$ $\square$

$K \trianglelefteq G$ Hall subgp

WTS $\exists$ a complement

Induct on $|K|$

if $|K| = p$ or 1 then done. (assume not...)

Choose $P \in \mathrm{Syl}_p K$, and consider $N_G P$

Note: $G/K = K \cdot N_G P / K = N_G P / K \cap N_G P$

note: $K \cap N_G P < K$ so $(|K \cap N_G P|, |G/K|)$

$|G/K| = |N_G P / K \cap N_G P|$

So if $N_G P \neq G$ then

$|K \cap N_G P| < |K|$

$\Rightarrow$ by induction, have complement H of $K \cap N_G P$ in $N_G P$

order of $H = |N_G P / K \cap N_G P| = |G/K|$

$H < N_G P < G \Rightarrow H$ is a complement in G.

So WLOG, only need consider case that $N_G P = G$

i.e. $P \triangleleft G$ Sylow i.e. either K is a p-gp or
K has a subgp (P) normal in G.

in either case, K would then
have a subgp $N < K$ w/ $N \triangleleft G$.

if K is p-gp, $N = Z(K)$
if not a p-gp. $P < K$ Sylow, $P \triangleleft G$.

Reduced to: $\overset{m}{K} \triangleleft \overset{nm}{G}$, and $\exists\, N \lneq K$ w/ $N \triangleleft G$.

Consider $K/N \triangleleft G/N$ by induction, have a complement

$H/N < G/N$

$|K| = m$ $\quad K/N \leftarrow \frac{m}{\ell}$, $\quad G/N \leftarrow \frac{m}{\ell}\cdot n$, $\quad H/N \leftarrow n$

$|G| = nm$

$|N| = \ell$

$N \triangleleft H$ $\quad N \leftarrow \ell$, $\quad H \leftarrow n\ell$

$\ell < m \quad \ell | m$

$(\ell, n) = 1$

by induction, $\exists\, H' < H$ since $(m,n) = 1$
complement to N so order n.

$H' < G$ is a complement to K $\square$.

$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ } $\mathbb{R}$-algebra

$i^2 = -1 = j^2 = k^2 \quad ij = -ji = k$ division algebra

Q: other division algebras?

f.dim'l d.alg / $\mathbb{R}$? $\mathbb{R}, \mathbb{C}, \mathbb{H}$

(associativity)

$\rightsquigarrow$ 1900ish other division algebras!

$\mathbb{R} \rightsquigarrow \mathbb{Q}, \mathbb{Q}(i), \ldots$

by around 1920 full classification over # fields.

Albert - Brauer - Hasse - Noether

$F \rightsquigarrow (a,b)_{-1}$ $\quad i^2 = a \quad j^2 = b$ $\quad F(i) = \dfrac{F[x]}{x^2 - a}$

$a, b \in F$ $\quad ij = -ji$

$ji = -ij$

$j\alpha = \bar{\alpha} j \quad \alpha \in F(i)$

$\bar{\ } =$ Galois action.

$$\begin{array}{c} E \\ |G \\ F \end{array} \qquad A = \bigoplus_{\sigma \in G} E u_\sigma \qquad u_\sigma x = \sigma(x) u_\sigma$$

$$u_\sigma u_\tau = c(\sigma, \tau) u_{\sigma\tau}$$

__Thm:__ if $c: G \times G \longrightarrow E^\times$ is a 2-cocycle $\Rightarrow$ get an assoc. alg which is always simple and $Z(A) = F$.

$H^2(G, E^\times) \rightsquigarrow$ as G grows take limit.

$\rightsquigarrow H^2(F, \mathbb{G}_m)[\ell]$

$H^1 \cup H^1 \subset H^2(F)$