Some defs: F is a <u>field</u> if:

$(F,+,\cdot)$, $(F,+)$ is an Abelian group (with identity 0)

$(F\setminus\{0\},\cdot)$ is an Abelian group

$\forall a,b,c$, $a(b+c)=a\cdot b+a\cdot c$.

Exs: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ p prime — usual $+,\cdot$

$\mathbb{F}_q$ – finite field order $q=p^k$, $k\in\mathbb{N}$, p prime.

More exs:

c) $G=\mathbb{Z}/p\mathbb{Z}\times\cdots\times\mathbb{Z}/p\mathbb{Z}$ (n-times)

$\mathrm{Aut}(G)\cong GL_n(\mathbb{Z}/p\mathbb{Z})=\{n\times n$ matrices A with entries in $\mathbb{Z}/p\mathbb{Z}$ and $\det(A)\neq 0\}$

(in $\mathbb{Z}_p$)

Note: $|GL_n(\mathbb{Z}/\mathbb{Z}_p)|=(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$.

# of vectors in a 0 dim v.s. over $\mathbb{Z}/p\mathbb{Z}$

in a 1-dim v.s. over $\mathbb{Z}/p\mathbb{Z}$

in an $(n-1)$-dim v.s. over $\mathbb{Z}/p\mathbb{Z}$.

2) $G = D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1} \rangle$

$Z(G) = \langle r^2 \rangle$: $r, s, r^{-1} \notin Z(G)$ ... $sr^i \notin Z(G)$

$r^2 \in Z(G)$

$|\mathrm{Inn}(G)| = |G/Z(G)| = 4$

(cyclic)

Note: $G/Z(G) \not\cong \mathbb{Z}/4\mathbb{Z}$, otherwise

G would be Abelian

so $\mathrm{Inn}(G) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3) Suppose $n = pq$, $p < q$ prime, and that $p \nmid q-1$. Then there are no non-Abelian groups of order n.

Pf: Suppose G is a non-Abelian group of order pq.

Then $Z(G) = \{1\}$, otherwise $G/Z(G)$ would be cyclic, so G would be Abelian.

Let H be a subgroup of G of order q.

Then $|G:H| = p \Rightarrow H \trianglelefteq G \Rightarrow N_G(H) = G$.

(smallest prime dividing $|G|$)

Also, H is Abelian $\Rightarrow H \leq C_G(H) \Rightarrow C_G(H) = H$ or G.

If $C_G(H) = G$ then $H \leq Z(G)$, which is a contr.

Therefore $C_G(H) = H$.

Finally by the cor. to our prop. from before,

$N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$.

Since $\left| N_G(H) / C_G(H) \right| = \left| G/H \right| = p$,

and $|\mathrm{Aut}(H)| = \varphi(q) = q-1$,

we must have $p \mid q-1$. $\blacksquare$

Semidirect products

(Motivation: Recall the recognition theorem for direct products: If $H, K \trianglelefteq G$, $H \cap K = \{1\}$, $HK = G$, then $G \cong H \times K$.)

Def: Suppose H and K are groups and that $\varphi: K \to \mathrm{Aut}(H)$ is a homom. The <u>semidirect product</u> $H \rtimes_\varphi K$ is $\{(h,k) : h \in H, k \in K\}$ with bin. op:

$$(h_1, k_1)(h_2, k_2) = (h_1 \varphi_{k_1}(h_2), k_1 k_2).$$

Prop: If H, K are groups and $\varphi: K \to \mathrm{Aut}(H)$ is a homom. then:

i) $H \rtimes K$ is a group

ii) $H \trianglelefteq H \rtimes K$ (this is the reason for the notation $\rtimes$)

iii) $\forall h \in H, k \in K$, $(1,k)(h,1)(1,k)^{-1} = (\varphi_k(h), 1)$.

Pf: i) Associativity:

$$(h_1,k_1)\big((h_2,k_2)(h_3,k_3)\big)$$
$$= (h_1,k_1)\big(h_2\varphi_{k_2}(h_3),\ k_2k_3\big)$$
$$= \big(h_1\underline{\varphi_{k_1}(h_2\varphi_{k_2}(h_3))},\ \underline{k_1k_2k_3}\big)$$

$$\big((h_1,k_1)(h_2,k_2)\big)(h_3,k_3)$$
$$= \big(h_1\varphi_{k_1}(h_2),\ k_1k_2\big)(h_3,k_3)$$
$$= \big(h_1\underline{\varphi_{k_1}(h_2)\varphi_{k_1k_2}(h_3)},\ \underline{k_1k_2k_3}\big) \checkmark$$

... (cont. next time)