August 2013:

(8) – G group, $V = k^2$ $k = K$.

$$G \times V \longrightarrow V$$
$$(g, v) \longmapsto g \cdot v$$

(a) We want group homomorphism

$$\rho : G \longrightarrow GL_2(k)$$

Take a basis $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ for V. Now for $g \in G$ we have:

$$\begin{cases} g \cdot e_1 = g_{11} \cdot e_1 + g_{12} e_2 \\ g \cdot e_2 = g_{21} \cdot e_1 + g_{22} \cdot e_2 \end{cases}$$

g row, column

$$M_g = \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix},$$ M_g^T gives the group action!

Decompose $v \in V$ as $v = v_1 \cdot e_1 + v_2 \cdot e_2$

then: $g \cdot v = M_g^T v$.

$$\rho: G \longrightarrow M_2(k) \quad \text{is a map.}$$
$$g \longmapsto M_g^T$$

We can prove that: $\rho(g \cdot h) = \rho(g) \cdot \rho(h)$.

$$\begin{cases} h \cdot e_1 = h_{11} \cdot e_1 + h_{12} e_2 \\ h \cdot e_2 = h_{21} \cdot e_1 + h_{22} \cdot e_2 \end{cases}$$

$$\rho(g \cdot h) = M_{gh}^T$$

$$\rho(g) \cdot \rho(h) = M_g^T M_h^T =$$

$$= \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix}^T \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix}^T.$$

$$gh\cdot e_1 = g(h\cdot e_1) = \begin{aligned}&(g_{11}h_{11}+g_{12}h_{21})\cdot e_1\\ &+(g_{11}h_{12}+g_{12}h_{22})e_2\end{aligned}$$

$$gh\cdot e_2 = g(h\cdot e_2) = \begin{aligned}&(g_{21}h_{11}+g_{22}h_{21})e_1\\ &+(g_{21}h_{12}+g_{22}h_{22})e_2\end{aligned}$$

$$\left\{\begin{aligned}\mathbb{1} &= \rho(1) = \rho(gg^{-1}) = \rho(g)\rho(g^{-1})\\ \mathbb{1} &= \rho(1) = \rho(g^{-1}g) = \rho(g^{-1})\rho(g)\end{aligned}\right.$$

$\rho(g^{-1}) = \rho(g)^{-1}$. So $\rho(g)$ is invertible so $\rho: G \longrightarrow GL_2(k)$.

And $\rho(1) = \mathbb{1}$. because G acts on V.

(b) Suppose that $\rho(g) = \begin{bmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{bmatrix}$

$\beta: G \longrightarrow k$,

$\delta : G \longrightarrow k^\times$. Show V has a 1D invariant subspace.

Note: $\rho(g)\begin{bmatrix}\alpha \\ 0\end{bmatrix} = \begin{bmatrix}1 & \beta(g) \\ 0 & \delta(g)\end{bmatrix}\begin{bmatrix}\alpha \\ 0\end{bmatrix} = \begin{bmatrix}\alpha \\ 0\end{bmatrix}$

so $\rho(g)$ keeps $\underbrace{\{\alpha \cdot e_1 : \alpha \in k\}}_{\text{is a 1D invariant subspace } W \text{ of } V.}$ invariant.

for all $g \in G$; $\rho(g)(W) \subseteq W$

(c) Show that δ is a group homomorphism and that $\beta(gh) = \beta(h) + \beta(g)\delta(h)$.

Since: $\begin{bmatrix}1 & \beta(gh) \\ 0 & \delta(gh)\end{bmatrix} = \rho(gh) = \rho(g)\rho(h) =$

$$= \begin{bmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{bmatrix} \begin{bmatrix} 1 & \beta(h) \\ 0 & \delta(h) \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & \beta(h) + \beta(g)\cdot\delta(h) \\ 0 & \delta(g)\cdot\delta(h) \end{bmatrix}.$$

Compare entries.

(d) If $\beta(gh) = \beta(h) + \beta(g)\delta(h)$ and $v = \begin{bmatrix} a \\ b \end{bmatrix} \in V$ with $b \neq 0$. Take $U = k\cdot v$.

Suppose $\rho(g)(U) \subseteq U$ for all $g \in G$.

Show there is some $c \in k$ so that for all $g \in G$: $\beta(g) = \delta(g)c - c$.

Check that this β satisfies the condition in (c).

$\rho(g)\cdot v = \alpha\cdot v$ (*)

Further assume that $\rho(g) = \begin{bmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{bmatrix}$.

$$\gamma(g) \quad \begin{bmatrix} 0 & \delta(g) \end{bmatrix}$$

Rmk: If we work over some general action $\begin{bmatrix} \alpha(g) & \beta(g) \\ \gamma(g) & \delta(g) \end{bmatrix}$ the conclusion is not true; take $\alpha(g) = 2 = \delta(g)$,

$$\beta(g) = 0 = \gamma(g),$$

now $0 = \beta(g) = \delta(g) \cdot c - c = 2 \cdot c - c =$

$$= c.$$

(*) $$\begin{bmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a + \beta(g) \cdot b \\ \delta(g) \cdot b \end{bmatrix} = \begin{bmatrix} \alpha \cdot a \\ \alpha \cdot b \end{bmatrix}$$

$$\Rightarrow \delta(g) b = \alpha \cdot b \Rightarrow \delta(g) = \alpha.$$

$$a + \beta(g) b = \alpha a \Rightarrow \beta(g) b = (\alpha - 1) a$$

$$\Rightarrow \beta(g) = (\alpha - 1) \frac{a}{b} \text{ since } b \neq 0.$$

$$= (\delta(g) - 1) \frac{a}{b}.$$

So set $c := \frac{a}{b}$, β decomposes as desired.

To check that $\beta(gh) = \beta(h) + \beta(g)\delta(h)$:

$$\beta(gh) = \delta(gh)c - c = \delta(g)\delta(h)c - c$$

$$\beta(h) + \beta(g)\delta(h) = \delta(h)c - c + (\delta(g)c - c)\delta(h) =$$

$$= \cancel{\delta(h)c} - c + \delta(g)\delta(h)c - \cancel{\delta(h)c} =$$

$$= \delta(g)\delta(h)c - c$$

January 2014:

① - A characteristic group is normal.

φ given by conjugation is an automorphism

so: $g^{-1}Hg = \varphi(H) = H$, any H that

is characteristic must be normal.

Suppose $G = HK$ with H, K characteristic,

$H \cap K = \{e\}$. Show $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

H, K are both characteristic, so both are normal.

<u>Recognition Thm:</u> $\tilde{H}, \tilde{K} \trianglelefteq \tilde{G}$, $\tilde{H} \cap \tilde{K} = \{e\}$ and $\langle \tilde{H}\tilde{K} \rangle = \tilde{G}$, then $\tilde{G} \cong \tilde{H} \times \tilde{K}$.

We want to apply this to
$\tilde{H} = \mathrm{Aut}(H)$, $\tilde{K} = \mathrm{Aut}(K)$,
$\tilde{G} = \mathrm{Aut}(G)$.

Hungerford p. 61 Corollary 8.7.

$A :=$ automorphisms of G leaving K fix.
$A \leq \mathrm{Aut}(G)$.

<u>Claim:</u> $A \cong \mathrm{Aut}(H)$.

$$\sigma \longmapsto \left(\begin{array}{l} \varphi : H \longrightarrow H \\ \quad\; h \longmapsto \sigma(h) \end{array} \right)$$

this is well defined.

Surjective: every $\phi \in \mathrm{Aut}(H)$ can be seen as $\Phi \in A$ by just

using $G \cong H \times K$.

leaving $\Phi|_K := id_K$.

Injective: if $\sigma, \tau \in A$ with $\sigma(H) = \tau(H)$

then $\sigma|_H = \tau|_H$ and

$\sigma|_K = \tau|_K$ so $\sigma|_G = \tau|_G$.

$B :=$ automorphisms of G leaving H fix.

$B \leq Aut(G)$.

<u>Claim:</u> $B \cong Aut(K)$, as before.

Now, we prove $A, B \leq Aut(G)$ satisfy hypothesis of the Recognition Theorem.

$A \cap B = \{e\}$ is clear.

$A \trianglelefteq Aut(G)$ because for $\varphi \in Aut(G)$ and $\psi \in A$, then: $\varphi \psi \varphi^{-1}(hk) =$

$$= \varphi\psi(\varphi^{-1}(h)\varphi^{-1}(k)) =$$

$$= \varphi(\psi\varphi^{-1}(h)\underbrace{\psi\underbrace{\varphi^{-1}(k)}_{\in K}}_{\varphi^{-1}(k)}) =$$

$$= \varphi(\psi\varphi^{-1}(h)\varphi^{-1}(k)) = \varphi\psi\varphi^{-1}(h)k$$

$$\varphi\varphi^{-1}(k) = k$$

If $h = e$ then $\varphi\psi\varphi^{-1}$ fixes K, and it is an automorphism of G so $\varphi\psi\varphi^{-1} \in A$. So $A \trianglelefteq \mathrm{Aut}(G)$.

Similarly $B \trianglelefteq \mathrm{Aut}(G)$.

Now: pick $\varphi \in \mathrm{Aut}(G)$; $\varphi|_H \in \mathrm{Aut}(H)$, say $\underset{\mathrm{Aut}(H)}{\varphi} \mapsto \underset{A}{\varphi_1}$. Similarly $\underset{\mathrm{Aut}(K)}{\varphi} \mapsto \underset{B}{\varphi_2}$.

We will show $\varphi = \varphi_1 \circ \varphi_2$.

Pick $hk \in HK = G$, now:

$$\varphi_1 \circ \varphi_2(hk) = \varphi_1(\underbrace{\varphi_2(h)}_{h}\varphi_2(k)) =$$

$$= \varphi_1(h\varphi_2(k)) = \varphi_1(h)\underbrace{\varphi_1\varphi_2(k)}_{\varphi_2(k)} =$$

$$= \varphi_1(h)\varphi_2(k) = \varphi(h)\varphi(k) =$$

$$= \varphi(hk).$$

Thus $\mathrm{Aut}(G) = \langle AB \rangle = A \times B$

recognition theorem

Alternative: build isomorphism

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$$

$$\sigma \longmapsto (\sigma|_H, \sigma|_K).$$

this heavily uses $H \times K = G$.

$HK =$

(2) - Show that G of $|G| = 2 \cdot 514$ has a normal cyclic subgroup of index 2.

Classify all groups of order 2014.

By Sylow 3 we must have:

$n_{53} = 1$, call it H, it will be normal.

$n_{19} = 1$, call it K, it will be normal.

Now $H \cap K = \{e\}$. Then $HK = H \times K$ and $|H \times K| = 19 \cdot 53 = 1007$. Moreover: $[G : H \times K] = 2$.

Since $19, 53$ are coprime, $\mathbb{Z}_{19} \times \mathbb{Z}_{53} \cong$
$\cong \mathbb{Z}_{1007}$ and $H \times K$ is cyclic of index 2, thus normal.

<u>Rmk</u>: $[G : \overline{G}]$ smallest prime dividing $|G|$ means $\overline{G} \trianglelefteq G$.

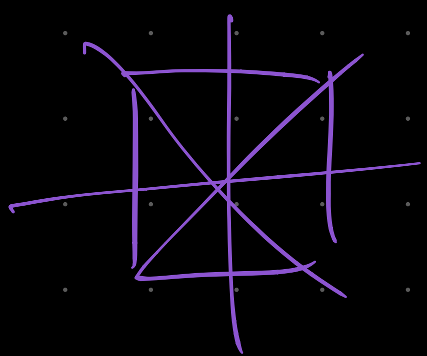
Aside: $H \times K$, H not commutative

K commutative

$H \times K$ has $(1, K)$ as commutative subgroup.

$H \times K / (1, K) \cong H$ not commutative.

D_8, mod out by $\mathbb{Z}_4$.



Classifying them: G must have some cyclic normal subgroup F of order 1007.

So given any 2-Sylow subgroup L, we have that $G \cong F \rtimes_\phi L$.

big classification theorem

We know $F \cong \mathbb{Z}_{19} \times \mathbb{Z}_{53}$, $L \cong \mathbb{Z}_2$, so

$$\phi : \mathbb{Z}_2 \longrightarrow \operatorname{Aut}(\mathbb{Z}_{19} \times \mathbb{Z}_{53}) \cong$$
$$\cong \operatorname{Aut}(\mathbb{Z}_{19}) \times \operatorname{Aut}(\mathbb{Z}_{53}) \cong$$
$$\cong \mathbb{Z}_{18} \times \mathbb{Z}_{52}.$$

ϕ must preserve the order of the elements, so $1 \in \mathbb{Z}_2$ must be sent to $\phi(1)$ of order two. The options are $9 \in \mathbb{Z}_{18}$, $26 \in \mathbb{Z}_{52}$, so we have:

(i) ϕ is trivial (sends everything to zero).

(ii) $1 \longmapsto (9, 0)$.

(iii) $1 \longmapsto (0, 26)$.

(iv) $1 \longmapsto (9, 26)$.

So for each L we have four options for ϕ, so four $F \rtimes_\phi L \cong G$.

(3) - A finite integral domain is a field.

Let D a f.i.d., pick $a \in D$ not zero. Look at $D \supseteq \{a^n : n \in \mathbb{N}\}$, we have $a^n = a^m$ by finiteness.
finite $n \neq m$

WLOG let $n > m$, then $a^{n-m} = 1$, so:

$$a \cdot (a^{n-m-1}) = 1$$

where $n-m \in \mathbb{N} \setminus \{0\}$ so $n-m-1 \in \mathbb{N}$.

Hence $a^{n-m-1} \in D$ is a^{-1}.

Prove that every prime ideal in a finite commutative ring is maximal.

Let R be finite comm. ring, P prime ideal.

Then R/P is finite integral domain.

So by the above R/P is a field, so P is maximal.

(4) - R commutative ring. Prove $\mathrm{Hom}_R(A, ?)$ is

left exact.

$$0 \longrightarrow L \xrightarrow{e} M \xrightarrow{f} N.$$ Apply $\mathrm{Hom}_R(A, ?)$:

$$0 \longrightarrow \mathrm{Hom}_R(A,L) \xrightarrow{e_*} \mathrm{Hom}_R(A,M) \xrightarrow{f_*} \mathrm{Hom}_R(A,N)$$

$\varphi : A \to L$ $\qquad e_*(\varphi) : A \longrightarrow M$

$$e_*(\varphi) : A \xrightarrow{\varphi} L \xrightarrow{e} M$$

$$e_* := e \circ ?$$

To show that this second sequence is exact we need: (i) $\mathrm{Ker}(e_*) = \{0\}$, i.e. e_* injective.

(ii) $\mathrm{Ker}(f_*) = \mathrm{im}(e_*)$.

(i) Suppose $\phi \in \mathrm{Ker}(e_*)$, $\phi : A \longrightarrow L$, with $0 = e_*(\phi) = e \circ \phi : A \longrightarrow M$. Take $a \in A$, now: $0 = e \circ \phi(a) = e(\phi(a))$, since e is injective $\phi(a) = 0$, so $\phi = 0$.

(ii) $\mathrm{im}(e_*) \subseteq \mathrm{Ker}(f_*)$.

$h : A \longrightarrow M$, $h \in \mathrm{im}(e_*)$, so there is

$g: A \longrightarrow L$ with $e \circ g = h$.

We know $\mathrm{im}(e) \subseteq \mathrm{Ker}(f)$, so applying f:

$$f_*(h) = f \circ h = f \circ e \circ g = f(\underbrace{e \circ g}_{\in \mathrm{im}(e)}) = 0$$

$\mathrm{Ker}(f_*) \subseteq \mathrm{im}(e_*)$.

$g \in \mathrm{Ker}(f_*)$; $g: A \longrightarrow M$ and $f \circ g = 0$.

Since $\mathrm{Ker}(f) \subseteq \mathrm{im}(e)$, for all $a \in A$ we

have $g(a) \in \mathrm{im}(e)$, so there is a

$b \in L$ with $g(a) = e(b)$.

We want to define:

$$e_*(h) = g$$

$$e \circ h = g \rightsquigarrow e(h(a)) = g(a) = e(b)$$

$$h: A \longrightarrow L$$
$$a \longmapsto b$$

Define $h: A \longrightarrow L$. This is well
$a \longmapsto b$

defined because e injective means that if there are b, b' with $e(b) = g(a) = e(b')$ then $b = b'$.

mult. $r \in R$
$a_1 + a_2 \rightsquigarrow$

<u>Claim:</u> h is a morphism. Suppose $a \in A$, then $g(a) = e(b)$ for some $b \in L$. Now pick $r \in R$

then: $g(r \cdot a) = r \cdot g(a) = r \cdot e(b) = e(r \cdot b)$

$\Rightarrow h(r \cdot a) = r \cdot b = r \cdot h(a)$.

Suppose $a_1, a_2 \in A$ with $g(a_1) = e(b_1)$,
$g(a_2) = e(b_2)$

$$g(a_1 + a_2) = g(a_1) + g(a_2) = e(b_1) + e(b_2) = e(b_1 + b_2)$$

$\Rightarrow h(a_1 + a_2) = b_1 + b_2 = h(a_1) + h(a_2)$.

Now indeed: $e \circ h(a) = e(b) = g(a)$ so

$g \in \operatorname{im}(e_*)$

Prove $\mathrm{Hom}_R(?, A)$ is left exact.

$$\mathrm{Hom}_R(M,A) \xleftarrow{f^*} \underbrace{\mathrm{Hom}_R(N,A)}_{\mathrm{im}(g^*) = \ker(f^*)} \xleftarrow{g^*} \underbrace{\mathrm{Hom}_R(P,A)}_{\ker(g^*) = \{0\}} \longleftarrow 0$$

$\subseteq$ ok.

$\supseteq$

$\ker(f^*) \subseteq \mathrm{im}(g^*)$: $\varphi : N \longrightarrow A$ such that $\varphi \circ f = 0$.

Note: $\ker(g) \subseteq \ker(\varphi) \subseteq N$, because if $n \in \ker(g)$ then $n \in \mathrm{im}(f) = \ker(g)$, so there is $m \in M$ with $f(m) = n$, so $\varphi(n) = \varphi(f(m)) = 0$.

So $\varphi : N \longrightarrow A$ factors through the kernel: $\overline{\varphi} : \underbrace{N/\ker(g)}_{\cong} \longrightarrow A$ (universal property of kernels).

P because $g : N \longrightarrow P$ and is surjective (F.I.T.).

Then: $\phi : P \longrightarrow A$ can be defined or: $\phi(p) := \overline{\varphi}(n + \ker(g))$ where $p = \overline{n}$.

This gives ϕ is a morphism for free.

<u>Claim:</u> $g^*(\phi) = \varphi$.

$$g^*(\phi)(n) = \phi \circ g(n) = \phi(n + \ker(g)) =$$
$$= \phi(p) = \overline{\varphi}(n + \ker(g)) = \varphi(n).$$

⑤ - For the future.

⑥ - $\mathbb{F}$ finite field with p^n elements.

(a) Why every element of $\mathbb{F}$ is a root of $x^{p^n} - x$.

0 is a root of $x^{p^n} - x$.

Take $a \in \mathbb{F} \setminus \{0\}$, then $a \in \mathbb{F}^\times$ the group of units, which has order $p^n - 1$. Hence:

Δ $\quad a^{p^n - 1} = 1$ so $a^{p^n} = a$ so a is root.

(b) If $r \mid p^n - 1$ then all the roots of $x^r - 1$ live in $\mathbb{F}$.

Suppose a is a root of $x^r - 1$, so $a^r = 1$. Now $r \mid p^n - 1$, so there is d with $rd = p^n - 1$.

$1 = 1^d = (a^r)^d = a^{rd} = a^{rd} = a^{p^n - 1}$. So the roots of $x^r - 1$ are also roots of $x^{p^n} - x$. So by part (1) the roots of $x^r - 1$ live in $\mathbb{F}$.

(a) $\mathbb{F}$ has p^n distinct elements, and every one of them is a root of $x^{p^n} - x$. But $x^{p^n} - x$ has at most p^n roots. So the roots of $x^{p^n} - x$ are exactly the elements in $\mathbb{F}$.

(c) Show that $x^4 + 1$ is reducible over any finite field.

Rmk: $x^4 + 1 = x^4 - (-1)$, so if we see that -1

is always a square, we are done.

If x^4+1 is reducible over $\mathbb{F}_p$, p prime, it is also reducible over $\mathbb{F}_{p^n}$ for all $n \in \mathbb{N}$. (because $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is its prime subfield).

If $p=2$ then $x^4+1=(x+1)^4$, reducible over $\mathbb{F}_2$.

"Thinking techniques": we are told to use p^2-1.

The way of going from p to p^2-1 is looking at the units of $\mathbb{F}_{p^2}$.

Consider the field extension $\mathbb{F}_{p^2}$. We have $\mathbb{F}_{p^2}^\times$ has p^2-1 elements. Notice $8 \mid p^2-1$, and $\mathbb{F}_{p^2}^\times$ is cyclic.

So there is a unit $u \in \mathbb{F}_{p^2}^\times$ with $|u|=8$. In particular since $x^8-1=(x^4-1)(x^4+1)$, we have u a root of x^4+1. So u is algebraic over

$\mathbb{F}_p \subseteq \underset{\alpha}{\underset{\cup}{\mathbb{F}_{p^2}}}$, so $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$. Thus $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \leq$

$\leq [\mathbb{F}_{p^2}(\alpha) : \mathbb{F}_p] = 2$. The minimal irreducible polynomial

Hungerford V.1.6. f of this extension has degree 2 or less. (f not zero)

Since α is a root of x^4+1, we must have

$f \mid x^4+1$, so x^4+1 is divisible by an irreducible polynomial with coefficients in $\mathbb{F}_p$. So x^4+1 is reducible.