Aspects of the Magnus Property (joint with Benjamin Klopsch and Carsten Feldkamp)

$\boxed{1930}$ Magnus publishes his famous Freiheitssatz.
In the same paper he proves the following theorem:

Thm Let F be a free group and let $a, b \in F$.
If the normal closures of a and b coincide,
then either a is conjugate to b or a is conjugate
to b^{-1}.

$$\langle a \rangle^F = \langle b \rangle^F \implies a \sim_{\pm} b.$$

Def A group G has the Magnus property (MP) if for all $g, h \in G$

$$\langle g \rangle^G = \langle h \rangle^G \implies g \sim_{\pm} h.$$

The normal closure problem is a lesser known sibling of the word and
the conjugacy problem. For groups with (MP) it reduces to the
conjugacy problem.

There are two (related) imposing questions:

I What groups do have (MP)
II Are there classes of groups where having (MP) is closed under certain operations? (Products, extensions, subgroups, ...)

Some first observations:

The following groups have (MP): $\mathbb{Z}^d$, $C_2^3 \wr C_2$, $\mathbb{Z} \rtimes \mathbb{Z}$, Q, $\mathrm{Hei}(3,\mathbb{Z})$

G (MP) $\Rightarrow$ $Z(G)$ (MP)

$G \times H$ (MP) $\Rightarrow$ G (MP)

A abelian, $B \leq A$ A (MP) $\Rightarrow$ B (MP)

A cyclic group C has (MP) if and only if $|C| \in \{1,2,3,4,6,\infty\}$.
(Look at $\varphi(|C|)$.)

One can express (MP) in first order logic, hence the class of groups having (ME) is closed under elementary equivalence.

What about finite groups?

Up to order 8 : $1, C_2, C_3, C_2^2, C_4, C_6, S_3, D_{2\cdot 4}, Q, C_2^3$

Up to order 128: Very many.

Lemma Let G be finite having (MP). Then every quotient has (MP).

Proof Let $N \trianglelefteq G$ and $Q = G/N$. Let $xN, yN \in Q$ such that

$$\langle xN \rangle^Q = \langle yN \rangle^Q.$$

There are $n_0, \ldots, n_k, m_0, \ldots, m_e \in \mathbb{Z}$, $g_0 \ldots, g_k, h_0 \ldots h_e \in G$ such that

$$((xN)^{n_0})^{g_0 N} \ldots ((xN)^{n_k})^{g_k N} = yN$$

$$((yN)^{m_0})^{h_0 N} \ldots ((yN)^{m_e})^{h_e N} = xN.$$

Choose $x_m \in xN$ such that $\langle x_m \rangle^G$ is minimal among $\{ \langle x_0 \rangle^G \mid x_0 \in xN \}$. Consider

Consider

$$(x_m^{n_0})^{g_0} \;\_\_\_\_\; (x_m^{n_k})^{g_k} = y_m \in yN$$

$$(y_m^{m_0})^{h_0} \;\_\_\_\_\; (y_m^{m_\ell})^{h_\ell} = x' \in xN.$$

Hence

$$\langle x' \rangle^G \leq \langle y_m \rangle^G \leq \langle x_m \rangle^G$$

and by minimality $\langle x' \rangle^G = \langle y_m \rangle^G = \langle x_m \rangle^G$. Since G has (MP), there exists $g \in G$ such that

$$y_m^g = x_m \quad \text{or} \quad y_m^g = x_m^{-1}.$$

Consequently $(yN)^{gN} = y_m^g N = x_m^{\pm 1} N = (xN)^{\pm 1}$. $\boxed{}$

Closer inspection shows that this proof does not need finiteness of G, but the descending chain condition for normally one-generated normal subgroups.

We obtain that every finite group with (MP) is soluble, but there are non-nilpotent groups having (MP). Let us have a look at a similar property:

Def A group G is called semi-rational if for all $g,h \in G$

$$\langle g \rangle = \langle h \rangle \implies g \sim_{\pm} h.$$

Any semi-rational group has the property that for all $g \in G$ and $\chi \in \mathrm{Irr}\, G$

$$[\mathbb{Q}(\chi(g)) : \mathbb{Q}] \in \{1, 2\},$$

generalising rational groups that have $\langle g \rangle = \langle h \rangle \Rightarrow g \sim h$ or equivalently all character values rational.

There are only finitely many primes occuring in soluble rational groups by a result of Gow, there are similar restrictions for semi-rational soluble groups. Using similar techniques, we prove

Prop Let G be finite having (MP). Then the only primes dividing $|G|$ are $2, 3, 5, 7$.

More results

$\boxed{1989}$ Edjvet : Certain free products have (MP).

(and others don't!)

$\boxed{2008}$ Bogopolski – Sviridov : Certain one-relator groups have (MP)

$C_3 \times C_4 \cong C_{12}$

$\boxed{2016}$ Klopsch – Kuckuck : There are torsion-free groups G, H having (MP) such that $G \times H$ does not have (MP).
However, the class of residually finite-p groups having (MP) is closed under direct products. ($p \neq 2$)

The last result is based on the following observation:

<u>Lemma</u> Let G, H be groups having (MP). Then $G \times H$ has (MP) if and only if for all $(g,h) \in G \times H$, one of the following holds

(i) g and g^{-1} are G-conjugate,
(ii) h and h^{-1} are H-conjugate,
(iii) $\langle (g,h) \rangle^{G \times H} \neq \langle (g, h^{-1}) \rangle^{G \times H}$.

Is there any hope for such a characterisation for more complicated extensions?

We take a step back and revisit the definition.

we restrict ourselves to faithful actions

<u>Def</u> Let G be a group and Γ a group acting on G (from the right). We say G has the Magnus property with respect to Γ $(MP)_\Gamma$ if for all $g, h \in G$

minimal Γ-invariant subgp

$$\langle g \rangle^\Gamma = \langle h \rangle^\Gamma \implies g \sim_\Gamma h.$$

If $\Gamma = \langle \mathrm{Inn}(G), x \mapsto x^{-1} \rangle \cong \mathrm{Inn}(G) \times \langle x \mapsto x^{-1} \rangle$ this coincides with our previous definition.

Let $G = N . \Gamma$. If G has (MP), the normal subgroup N has $(MP)_\Gamma$ with respect to the action $N \curvearrowleft \Gamma$ given by G.

Another point of view:

Let G be a group. The set $M(G)$ of all functions $G \to G$ has the structure of a nearring:

Def. A set R with two operations $+, \cdot$ is called a (left)-nearring if

(i) $(R, +)$ is a group.
(ii) $(R, \cdot)$ is a semi-group.
(iii) Left-distributivity: $\forall a, b, c \in R \quad c\cdot(a+b) = c\cdot a + c\cdot b$.

(Fun/horrible fact: In general, $0 \cdot a \neq 0$!)

We look at the sub-nearring generated by

$$R(G,\Gamma) = \langle x \mapsto x^n,\ x \mapsto x^\gamma \mid n \in \mathbb{Z},\ \gamma \in \Gamma \rangle_{\text{nearring}} \leq M(G).$$

Notice that in case $\Gamma = G$ abelian, this is a proper ring, in fact, a quotient of the group ring $\mathbb{Z}[G]$.

Lemma Let G be a group and let Γ act on G by endomorphisms. The following statements are equivalent:

(i) G has $(MP)_\Gamma$

(ii) For every $r \in R$ with non-trivial fixed point g and every product $r = s \cdot t$, $s, t \in R$, there is an element of the form $\pm (x \mapsto x^n) = u$ such that $g \cdot s = g \cdot u$.

This (vaguely) resembles the property of some group rings to have only trivial units, i.e. $\mathbb{Z}[G]^\times = \pm G$.

Coming back to the extensions, we get a closer resemblance if we consider the "easiest" case: $G = A \rtimes \Gamma$, A free abelian, Γ finite.

We have already established that we need to check if A has Γ. Luckily, $R(A, \Gamma)$ is in fact a ring, sitting inside the endomorphism ring of A.

We identify A with $\mathbb{Z}^d$, and since Γ acts by automorphisms, we identify it with the corresponding subgroup of $GL_d(\mathbb{Z})$.

Lemma Let $\mathbb{Z}^d$ have $(MP)_\Gamma$. There is a decomposition

$$\mathbb{Z}^d = V_1 \oplus \dots \oplus V_k$$

into Γ-invariant free submodules such that for all $\gamma \in \Gamma$ $\gamma|_{V_i}$ acts fixed point free for all $i = 1, \dots, k$.

Idea Show that the eigenmodules wrt the eigenvalue 1 are Γ-invariant.

Consequently Γ is a subdirect product (i.e. a subgroup of the direct product with surjective projections to every component) of some groups Γ_i of elements without fixed points.

To continue, we may assume that $\Gamma = \Gamma_i$, i.e. that no non-trivial automorphism has a fixed point.

Lemma Let $\mathbb{Z}^d$ have $(MP)_\Gamma$. Then $R(\mathbb{Z}^d,\Gamma)$ has only trivial units.

Proof Let $v \in \mathbb{Z}^d$. All elements $v^{R(\mathbb{Z}^d,\Gamma)^\times}$ are different, since $\gamma \in \Gamma$ acts fixed point free, and generate the same Γ-invariant subgroup.

But the set of Γ-conjugates and inverse Γ-conjugates is precisely $v^{\pm\Gamma} \subsetneq v^{R(\mathbb{Z}^d,\Gamma)^\times}$. $\square$

Lemma Let $\mathbb{Z}^d$ have $(MP)_\Gamma$. Then Γ has only elements of order $1, 2, 3, 4, 6$.

Proof (prime power case) Let $\gamma \in \Gamma$ have order p^m. Then γ has a primitive p^m-th root of unity as an eigenvalue. Write Φ_{p^m} for the p^m-th cyclotomic polynomial, and set $V = \ker \Phi_{p^m}(\gamma)$. $V \neq 0$, since $\Phi_{p^m}(\gamma)$ has an eigenvalue 0.

The matrix $\gamma|_V$ has only p^m-roots of unity as eigenvalues. Consequently the ring generated by $\mathbb{1}_V$ and $\gamma|_V$ is isomorphic to $\mathbb{Z}[\zeta_{p^m}]$, which has an infinitude of units if $p^m \notin \{2,3,4\}$ by Dirichlet's unit theorem. $\square$

We can classify our fixed point free Γ:

It is a classical result that the only groups Γ having a faithful representation by fixed point-free matrices have cyclic Sylow-p-subgroups for p odd and cyclic or $\underbrace{\text{generalised quaternion}}_{\langle a, b \mid a^n = b^2,\ a^{2n} = 1,\ a^b = a^{-1} \rangle}$ Sylow-2-subgroups.

Looking at the exponent of such groups, we see that might ignore the word "generalised", and

$$|\Gamma| \mid 2^3 \cdot 3 .$$

Sylow-3 cyclic

Checking by hand, the only groups Γ that are left are

$$1,\ C_2,\ C_3,\ C_4,\ C_6,\ Q,\ Dic_3,\ SL_2(3).$$

Going back to the "global" case of any finite Γ, we get:

Every finite $\Gamma \leq GL_d(\mathbb{Z})$ such that $\mathbb{Z}^d$ has $(MP)_\Gamma$ is a subdirect product of

$$C_2, C_3, Q, Dic_3, SL_2(3).$$

Every finite group Γ such that $\mathbb{Z}[\Gamma]^\times = \pm\Gamma$ is a direct product of

$$C_2, C_3, Q.$$

(Classical result of Higman)

Furthermore, all groups do occur!

For all "atomic" groups there is precisely one reprensentation allowing $(MP)_\Gamma$.

Lemma All groups $G = \mathbb{Z}^d \rtimes \Gamma$ with $\Gamma \in \{Q, \mathrm{Dic}_3, SL_2(3)\}$ acting by fixed point free matrices do not have (MP).

Eg. $\Gamma = Q$. The only representation with the required property is

$$i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad d = 4.$$

Write $c = i^2 = -\mathbb{1}$ for the central element, let $v, w \in \mathbb{Z}^4$. Then

$$(vc)^w = v w^{-1} w^c c = v w^{-2} c.$$

Consequently $\bigcup_{\eta \in G} v^\eta 2\mathbb{Z}^4 c$ is the set of conjugates of vc.

We want to show that there is an element outside vc^G normally generating the same normal subgroup as vc. We might calculate modulo $2\mathbb{Z}^4$.

Now $1 + i + j \equiv_2 \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ is invertible mod 2,
and choosing $v = (1,0,0,0)$

$$(vc)^i (vc)^j \, vc \equiv_2 v^{1+i+j} c \equiv_2 (1,1,1,0) c$$

But the number of entries $\equiv_2 1$ of v does not change upon conjugation, hence $vc \not\sim_{\pm 1} v^{1+i+j} c$. $\boxed{\text{☑}}$

However, the group $\mathbb{Z}^2 \rtimes \langle \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}}_{=M} \rangle$ does have (MP).

- $\mathbb{Z}^2$ has $(MP)_{\langle M \rangle}$: $R(\mathbb{Z}^2, \langle M \rangle) = \left\{ n \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + m \cdot M^2 \mid n, m \in \mathbb{Z} \right\}$, since $M = -(M^2 + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$. A generic element has the form

$$\det \begin{pmatrix} n-m & m \\ -m & n \end{pmatrix} = \left(n^2 + m^2 + (n-m)^2 \right) 1/2$$

which does not have fixed points, and ... hence the only units are

$$\begin{matrix} n = \pm 1 \\ m = 0 \end{matrix} \rightsquigarrow \pm \mathbb{1} \qquad \begin{matrix} n = 0 \\ m = \pm 1 \end{matrix} \rightsquigarrow \pm M^2 \qquad n = m = \pm 1 \rightsquigarrow \pm M.$$

- Look (wlog) at vM, $v \in \mathbb{Z}^2$. Then for $w \in \mathbb{Z}^2$

$$(vM)^w = v\, w^{M^2 - 1} M.$$

Consequently we may calculate mod $(\mathbb{Z}^2)^{M^2-1} = \{(u,v) \mid u+v \equiv_3 0\}$.
Since $M(M^2-1) = (M^2-1)M$ both M and M^2 define an action on

$$\mathbb{Z}^2 / (\mathbb{Z}^2)^{M^2-1} \cong C_3 ,$$

but

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}^M = \begin{pmatrix} -1 \\ -1 \end{pmatrix} \equiv \begin{pmatrix} -1 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

hence the action is trivial. Write $\bar{v}$ for a representative of v

$$\langle vM \rangle^G = \left\{ \bar{v}^{M^{i_0}} w_0 M \ \bar{v}^{M^{i_1}} w_1 M \ \ldots \ \bar{v}^{M^{i_k}} w_k M \ \middle| \ \begin{array}{l} i_0, \ldots, i_k \in \mathbb{Z} \\ w_0, \ldots, w_k \in (\mathbb{Z}^2)^{M^2-1} \end{array} \right\}$$

$$= \{ (\bar{v})^k w M^k \mid k \in \{0,1,2\}, w \in (\mathbb{Z}^2)^{M^2-1} \}.$$

All other elements generating this normal subgrp have the form $\bar{v} w M$ or $\bar{v}^2 w M^2$ for some $w \in (\mathbb{Z}^2)^{M^2-1}$.

But all elements of this form are conjugate or inverse conjugate to vM. $\boxtimes$

Let us take another look at the definition.

<u>Def</u> Let G be a group and Γ a group acting on G (from the right). We say G has the Magnus property with respect to Γ if for all $g, h \in G$ $(MP)_\Gamma$

$$\langle g \rangle^\Gamma = \langle h \rangle^\Gamma \implies g \sim_\Gamma h .$$

It is easy to formulate some variations:

i) Let $\Gamma = \mathrm{Inn}(G)$. This is akin to looking at rational instead of semi-rational groups. Having $(MP)_{\mathrm{Inn}(\cdot)}$ is closed under direct products.

ii) Let $\Gamma = \langle \{ x \longmapsto x^n \mid n \in \mathbb{Z} \} \cup \mathrm{Inn}(G) \rangle$. This a strictly weaker property, less sensitive to torsion elements. All abelian groups have $(MP)_\Gamma$.

iii) Let $\Gamma = \langle \{ x \longmapsto x^{-1} \} \cup \mathrm{Aut}(G) \rangle$, the "characteristic" Magnus property. It is closed under characteristic subgroups. Free abelian groups have $(MP)_\Gamma$, but free group <u>do not</u>.

~ Fin ~