ILLINOIS JOURNAL OF MATHEMATICS
Volume 40, Number 1, Spring 1996

INDEPENDENCE AND MAXIMAL SUBGROUPS

MICHAEL WEIDNER[1]

Dedicated to O. H. Kegel on the occasion of his 60th birthday

1. Introduction

In this paper G denotes a finite group and $M(G)$ the set of all maximal subgroups of G.

Recall that a matroid $(M, \mathcal{I})$ is a finite set M together with a set $\mathcal{I}$ of subsets of M (we call $X \subseteq M$ independent if and only if $X \in \mathcal{I}$) such that:

every subset of an independent set is independent, and every one-element subset is independent (i.e. $(M, \mathcal{I})$ is a simplicial complex)

and

if $A, B \in \mathcal{I}$ and $|A| < |B|$, then there is an $x \in B \setminus A$ such that $A \cup \{x\}$ is independent.

Examples of matroids are:

1. Let M be the (non-trivial) vectors of a finite vectorspace, $\mathcal{I}$ the linear independent sets.
2. Let M be the set of edges of a graph Γ and $\mathcal{I}$ the set of all circuit-free subsets of M.
3. Let $M = M_1 \cup M_2 \cup \cdots \cup M_l$ be a partition of M and

$$\mathcal{I} := \{X \subseteq M \colon |X \cap M_i| \leq 1 \text{ for all } i \leq l\}.$$

   Then $(M, \mathcal{I})$ is a matroid. This matroid is called the partition matroid of the partition $(M_i)_{i \leq l}$ of M.

Let $\mathcal{H} := (H_0 > H_1 > \cdots > H_l)$ denote a chief-series of G (i.e., a maximal chain of normal subgroups of G). Then $M(G)$ is the disjoint union of the sets $\mathcal{K}_i := \{U \in M(G) \colon H_i U = G, H_{i+1} \leq U\}$.

So, with $\mathcal{I}_{\mathcal{H}} := \{X \subseteq M(G) \colon |X \cap \mathcal{K}_i| \leq 1 \text{ for all } i < l\}$, we have a partition matroid $(M(G), \mathcal{I}_{\mathcal{H}})$. We call the independent subsets (i.e., the elements of $\mathcal{I}_{\mathcal{H}}$) $\mathcal{H}$-independent.

Received October 22, 1993
1991 Mathematics Subject Classification. Primary 20C20, 05B35.
[1]The main part of this paper was written during a stay at the University of Chicago. The author would like to thank the "Deutsche Forschungsgemeinschaft" for their generous support.

If we have sets $\mathcal{I}_i$, such that $(M, \mathcal{I}_i)$ is a matroid, then $(M, \bigcup \mathcal{I}_i)$ is not necessarily a matroid (see Example 2.2.4). However: if $\mathcal{C}$ is the set of all chief-series of G and $\mathcal{I}_{\mathcal{C}} := \bigcup_{\mathcal{H}\in\mathcal{C}} \mathcal{I}_{\mathcal{H}}$, then $(M(G), \mathcal{I}_{\mathcal{C}})$ is a matroid.

Call a set of subgroups $\mathcal{U}$ of G a $\mathcal{W}$-independent set, if $\prod_{U\in\mathcal{U}}[G : U] = [G: \bigcap_{U\in\mathcal{U}} U]$. Let $\mathcal{I}_{\mathcal{W}}$ denote the set of all $\mathcal{W}$-independent set of subgroups of G. There are various applications (Wielandt's independence definition [Wi], Galois theory, probability theory, factorisations of groups, orbit posets) of this definition (see Section 5).

For $\mathcal{I} \subseteq \{Y \subseteq M\}$ and $X \subseteq M$ define $\mathcal{I}(X) := \{Y \subseteq X\colon Y \in \mathcal{I}\}$. For a prime p let $M^p(G) := \{U \in M(G)\colon [G : U] \text{ is a power of } p\}$. If π is the set of all primes, then $(\bigcup_{p\in\pi} M^p(G), \mathcal{I}_{\mathcal{W}}(\bigcup_{p\in\pi} M^p(G)))$ is a matroid.

So $M^p(G)$ together with each of the sets $\mathcal{I}_{\mathcal{H}}(M^p), \mathcal{I}_{\mathcal{C}}(M^p)$ and $\mathcal{I}_{\mathcal{W}}(M^p)$ is a matroid. For $\mathcal{X} \in \{\mathcal{H}, \mathcal{C}, \mathcal{W}\}$ let $\mathcal{I}_{\mathcal{X}}(M^p(G))^{\cap} := \{\bigcap_{x\in X} x\colon X \in \mathcal{I}_{\mathcal{X}}(M^p(G))\}$. Although no two of the sets $\mathcal{I}_{\mathcal{H}}(M^p)$, $\mathcal{I}_{\mathcal{C}}(M^p)$ and $\mathcal{I}_{\mathcal{W}}(M^p)$ need be equal we have $\mathcal{I}_{\mathcal{H}}(M^p(G))^{\cap} = \mathcal{I}_{\mathcal{C}}(M^p(G))^{\cap} = \mathcal{I}_{\mathcal{W}}(M^p(G))^{\cap} = S_c^p(G)$, where $S_c^p(G)$ is the set of all those subgroups U of p-power index in G for which the Möbius number $\mu(U, G)$ is not zero (see [We2]). The partially ordered set $S_c^p(G)$ was studied in [WW]. It plays a crucial role in the homology theory of the partially ordered set of all subgroups of p-power index in G.

In p-solvable groups we have a certain class of subgroups called p-Prefrattini-groups (see [DH] page 422ff., [Ga], [We1]). The results of this paper justify to define (for all groups) p-Prefrattinigroups as the minimal elements of S_c^p.

2. Preliminaries

2.1. About matroids.

DEFINITION 2.1.1. A *simplicial complex* $(M, \mathcal{I})$ is a finite set M and a set $\mathcal{I}$ of subsets of M such that:

1. If $m \in M$, then $\{m\} \in \mathcal{I}$.
2. If $A \in \mathcal{I}$ and $B \subset A$, then $B \in \mathcal{I}$.

A *matroid* is a simplicial complex $(M, \mathcal{I})$ such that whenever $A, B \in \mathcal{I}$ and $|A| < |B|$, then there is a $b \in B \setminus A$ such that $A \cup \{b\} \in \mathcal{I}$.

A subset X of M is called an independent set if and only if it is in $\mathcal{I}$.

The last condition implies that all maximal independent sets of a matroid have the same cardinality.

THEOREM 2.1.2. *Fix a simplicial complex* $(M, \mathcal{I})$.

1. *For* $A \subseteq M$ *define* $\mathcal{I}(A) := \{A \cap X\colon X \in \mathcal{I}\}$. *Then* $(A, \mathcal{I}) := (A, \mathcal{I}(A))$ *is a simplicial complex. If* $(M, \mathcal{I})$ *is a matroid, then so is* $(A, \mathcal{I})$.

2. *If $M = A \cup B$ is a disjoint union such that $X \subseteq M$ is in $\mathcal{I}$ if and only if $X \cap A$ and $X \cap B$ are in $\mathcal{I}$, we call $(M, \mathcal{I})$ the direct product of $(A, \mathcal{I}(A))$ and $(B, \mathcal{I}(B))$.*

If $(A, \mathcal{I})$ and $(B, \mathcal{I})$ are matroids, then so is $(M, \mathcal{I})$.

3. *Suppose $(M, \mathcal{I})$ is a simplicial complex and $f\colon M \to \bar{M}$ is a map. Assume*

$$\mathcal{I} = \{Y \subseteq M\colon \exists X \in \mathcal{I}\ s.t.\ |X| = |Y| = |f(X)| \text{ and } f(X) = f(Y)\}.$$

Then $(f(M), f(\mathcal{I}))$ is a simplicial complex.

Moreover, $(M, \mathcal{I})$ is a matroid if and only if $(f(M), f(\mathcal{I}))$ is.

4. *For a matroid $(M, \mathcal{I})$ and $m \in M$ let*

$$\mathbf{proj}(m) := \{x \in M\colon \{x, m\} \notin \mathcal{I}\} \cup \{m\}.$$

For $X \subseteq M$ define $\mathbf{proj}(X) := \{\mathbf{proj}(m)\colon m \in X\}$ *and* $\mathbf{proj}(\mathcal{I}) := \{\mathbf{proj}(X)\colon X \in \mathcal{I}\}$.

Then $(\mathbf{proj}(M), \mathbf{proj}(\mathcal{I}))$ *is a matroid. We will call this matroid the projective matroid of $(M, \mathcal{I})$.*

Proof. 1. See [Ai], Proposition 6.33.

2. See [Ai], Proposition 6.44.

3. (a) Suppose $(M, \mathcal{I})$ is a matroid and $fX, fY \in f(\mathcal{I})$ are such that $|fX| < |fY|$. Fix $X, Y \in \mathcal{I}$ such that $f(X) = fX$, $f(Y) = fY$, $|f(X)| = |X|$ and $|f(Y)| = |Y|$. By assumption we find a $y \in Y \setminus X$ such that $X \cup \{y\} \in \mathcal{I}$. But now $f(y) \in fY \setminus fX$ and $fX \cup \{f(y)\} = f(X \cup \{y\}) \in f(\mathcal{I})$. Thus $(f(M), f(\mathcal{I}))$ is a matroid.

(b) Suppose $(f(M), f(\mathcal{I}))$ is a matroid. Let $X, Y \in \mathcal{I}$ and $|X| < |Y|$. The assumptions on $\mathcal{I}$ imply $|X| = f(X) < f(Y) = |Y|$ and so there is a $fy \in f(Y) \setminus f(X)$ such that $f(X) \cup \{fy\} \in f(\mathcal{I})$.

Fix $y \in Y$ such that $f(y) = fy$. Since $f(y) \notin f(X)$ we have $y \notin X$. But $f(X \cup \{y\}) = f(X) \cup \{fy\} \in f(\mathcal{I})$ and so, by assumption, $X \cup \{y\} \in \mathcal{I}$.

Thus $(M, \mathcal{I})$ is a matroid.

4. See [Ai], Theorem 6.1. □

EXAMPLE 2.1.3. 1. Assume K is a finite field and $V \cong K^n$. Let $M := V \setminus \{0\}$ and let $\mathcal{I}$ denote the set of all linear independent subsets of M. Then $(M, \mathcal{I})$ is a matroid. The projective matroid of $(M, \mathcal{I})$ corresponds to the projective space associated to V. The matroid structure of the projective matroid determines n, and if $n \geq 2$ it determines K too.

$(M, \mathcal{I})$ cannot be written as a product of two nontrivial matroids (well known).

2. Suppose Γ is a graph with set of vertices $V(\Gamma)$ and set of edges $E(\Gamma)$ (so $E(\Gamma) \subseteq \{\{i, j\}\colon i, j \in V(\Gamma), i \neq j\}$).

Let $\mathcal{I}_\Gamma$ denote the set of all $X \subseteq E(\Gamma)$ such that $(V(\Gamma), X)$ contains no circle. Then $(E(\Gamma), \mathcal{I}_\Gamma)$ is a matroid (see [Ai], Theorem 6.23 (Whitney)).

2.2. $\mathcal{H}$ and $\mathcal{W}$-independence. Let p denote a prime and G denote a finite group. Then $\mathbb{F}_p$ is the field with p elements, $\mathbb{I}$ is the trivial $\mathbb{F}_pG$-module and E is the trivial subgroup of G.

LEMMA 2.2.1. *Let G denote a finite group and $U \in M(G)$ (i.e., U is a maximal subgroup of G). Fix a chief-series $\mathcal{H} = (H_j)_{j \leq l}$ (i.e., a maximal chain of normal subgroups in G).*
Then $H_i \leq U$ if and only if $H_iU \neq G$. So

$$\{X \in M(G)\colon\ H_iX = G,\, H_{i+1} \leq X\} = \{X \in M(G)\colon\ H_{i+1} \leq X \not\geq H_i\}.$$

Proof. As $\mathcal{H}$ is a maximal chain of normal subgroups, we have $G = H_0$ and $E = H_l$. So $H_l \leq U \leq H_0$, and there exists an unique $i(U)$ such that $H_{i(U)+1} \leq U \not\geq H_{i(U)}$.
For $i \leq i(U)$ we have $H_{i+1} \leq U$ and so $H_{i+1}U = U \neq G$.
For $i \geq i(U)$ we have $H_i \not\leq U$ and so $U \neq H_iU$. As H_i is normal we get $H_iU \leq G$, and as U is maximal we conclude $H_iU = G$. □

DEFINITION 2.2.2. Suppose R is a bounded partially ordered set (i.e. there are $0, 1 \in R$ such $0 \leq r \leq 1$ for all $r \in R$).
Assume $P, Q \subseteq R$ such that $0, 1 \in P$ and $\mathcal{H} = (H_0 > H_1 > \cdots > H_l)$ is a maximal chain in P.
Define $\mathcal{I}_{\mathcal{H}} := \{X \subseteq Q\colon |\{x \in X\colon\ H_{i+1} \leq x \not\geq H_i\}| \leq 1$ for all i $\}$.
Let $\mathcal{C}$ denote the set of all maximal chains in P and let $\mathcal{I}_{\mathcal{C}} := \bigcup_{\mathcal{H}\in\mathcal{C}} \mathcal{I}_{\mathcal{H}}$.

LEMMA 2.2.3. *Notation as above.*
$\bigcup\{x \in Q\colon\ H_{i+1} \leq x \not\geq H_i\}$ is a partition of Q and $(Q, \mathcal{I}_{\mathcal{H}})$ is a (partition) matroid.
$(Q, \mathcal{I}_{\mathcal{C}})$ is a simplicial complex.

Proof. For $U \in Q$ fix $i(U)$ such that $H_{i(U)} \not\leq U \geq H_{i(U)+1}$. Since $H_0 = 1$, $H_l = 0$ and $H_i > H_{i+1}$, there exists exactly one such number $i(U)$.
So $\bigcup_i \{X \in Q\colon\ i(X) = i\}$ is a partition of Q. Thus $(Q, \mathcal{I}_{\mathcal{H}})$ is a partition matroid (see [Ai], Proposition 6.2).
In particular, $(Q, \mathcal{I}_{\mathcal{H}})$ is a simplicial complex for every $\mathcal{H} \in \mathcal{C}$. Thus $(Q, \mathcal{I}_{\mathcal{C}}) := (Q, \bigcup_{\mathcal{H}\in\mathcal{C}} \mathcal{I}_{\mathcal{H}})$ is a simplical complex too. □

EXAMPLE 2.2.4. 1. Let R denote the set of all subgroups of G (partially ordered by inclusion), $Q = M(G)$ the set of maximal subgroups and P the set of all normal subgroups. Then the maximal chains in P are exactly the chief-series of G.
Thus we have redefined (see Lemma 2.2.1) the complexes $(M(G), \mathcal{I}_{\mathcal{H}})$ and $(M(G), \mathcal{I}_{\mathcal{C}})$ of our introduction. Moreover, the first complex is a matroid (see Lemma 2.2.3).

2. Let G denote a finite group and $\mathcal{C}_1 \subset \mathcal{C}$. Then $(M(G), \bigcup_{\mathcal{H}\in\mathcal{C}_1} \mathcal{I}_{\mathcal{H}})$ is not necessarily a matroid.

For example: let $G = \langle a, b, c\rangle$ denote the elementary abelian group of order 8.

Let $\mathcal{H}_1 := (G, \langle a, b\rangle, \langle a\rangle, E)$ and $\mathcal{H}_2 := (G, \langle b, c\rangle, \langle b\rangle, E)$ (so $\mathcal{H}_1$ and $\mathcal{H}_2$ are chief-series of G).

Define $\mathcal{I} := \mathcal{I}_{\mathcal{H}_1} \cup \mathcal{I}_{\mathcal{H}_2}$. We claim that $(M(G), \mathcal{I})$ is not a matroid.

In doing so let $B := \{\langle a, b\rangle, \langle a, c\rangle, \langle ba, c\rangle\} \in \mathcal{I}_{\mathcal{H}_1} \subseteq \mathcal{I}$ and $A := \{\langle ba, c\rangle, \langle b, ca\rangle\} \in \mathcal{I}_{\mathcal{H}_2} \subseteq \mathcal{I}$. So $|A| = 2 < 3 = |B|$. Since $A \notin \mathcal{I}_{\mathcal{H}_1}$ the only $x \in M(G) \setminus A$ for which $A \cup \{x\} \in \mathcal{I}$ is $\langle b, c\rangle$. As $\langle b, c\rangle \notin B$ we see that $(M(G), \mathcal{I})$ is not a matroid.

DEFINITION 2.2.5. A set of subgroups $\mathcal{U}$ of G is $\mathcal{W}$-independent if and only if $[G\colon \bigcap_{U\in\mathcal{U}} U] = \prod_{U\in\mathcal{U}}[G : U]$. Let $\mathcal{I}_{\mathcal{W}}$ denote the set of all $\mathcal{W}$-independent sets of subgroups of G.

For $A, B \leq G$, we define $AB := \{ab\colon a \in A, B \in B\}$.

LEMMA 2.2.6. *If $A, B \leq G$ and $C \leq A$. Then*
(Lagrange): $|AB| = |A||B|/|A \cap B|$.
(Dedekind): $A \cap (CB) = C(A \cap B)$.
If B is normal in G, then $AB \leq G$.

Most parts of the next lemma can be found in [FJ], Chapter 16.3 and [Wi], Kapitel 1.2.

LEMMA 2.2.7. 1. *For a set $\mathcal{U}$ of subgroups the following are equivalent:*
(a) *Every subset of $\mathcal{U}$ is $\mathcal{W}$-independent.*
(b) *$\mathcal{U}$ is $\mathcal{W}$-independent.*
(c) $\prod_{U\in\mathcal{U}}[G : U] \leq [G\colon \bigcap_{U\in\mathcal{U}} U]$.
(d) $\tau_{\mathcal{U}}\colon G/\bigcap_{U\in\mathcal{U}} U \to \times_{U\in\mathcal{U}} G/U$; $\tau_{\mathcal{U}}(g\bigcap_{U\in\mathcal{U}} U) = \times_{U\in\mathcal{U}} gU$ *is (surjective) bijective (Chinese Remainder Theorem).*
(e) *For all $U \in \mathcal{U}$ we have $U(\bigcap_{U\neq\bar{U}\in\mathcal{U}} \bar{U}) = G$ (this is a definition in* [Wi]).
(f) *If $\mathcal{V} \subset \mathcal{U}$ and $\mathcal{L} := \mathcal{U} \setminus \mathcal{V}$, then $\mathcal{V}, \mathcal{L} \in \mathcal{I}_{\mathcal{W}}$ and $(\bigcap_{V\in\mathcal{V}} V)(\bigcap_{L\in\mathcal{L}} L) = G$.*
2. *If (H_i) is a series of normal subgroups and U_i for $i \in I$ are supplements of H_i/H_{i+1}, then $\{U_i\colon i \in I\}$ is $\mathcal{W}$-independent (so $\mathcal{I}_{\mathcal{C}}(M(G)) \subseteq \mathcal{I}_{\mathcal{W}}(M(G))$).*
Furthermore, $H_i(\bigcap_{i\leq j\in I} U_j) = G$ for all i.
3. *If $U \neq U^g$, then $\{U, U^g\}$ is not $\mathcal{W}$-independent.*
4. *If $\mathcal{U}$ is $\mathcal{W}$-independent and $g_U \in G$ for $U \in \mathcal{U}$, then $\{U^{g_U}\colon U \in \mathcal{U}\}$ is $\mathcal{W}$-independent and there is a $g \in G$ such that $\bigcap_{U\in\mathcal{U}} U^g = \bigcap_{U\in\mathcal{U}} U^{g_U}$.*

Proof. For $\mathcal{X}$ a set of subgroups of G, define $\mathcal{X}_\cap := \bigcap_{X\in\mathcal{X}} X$.

1. If $\tau_{\mathcal{U}}(g\mathcal{U}_\cap) = \tau_{\mathcal{U}}(g'\mathcal{U}_\cap)$, then $g^{-1}g' \in U$ for all $U \in \mathcal{U}$. So $\tau_{\mathcal{U}}$ is injective. Hence $[G\colon \mathcal{U}_\cap] \leq \prod_{U\in\mathcal{U}}[G : U]$ and $\tau_{\mathcal{U}}$ is surjective if $[G\colon \mathcal{U}_\cap] = \prod_{U\in\mathcal{U}}[G : U]$.

This proves (b)$\Leftrightarrow$(d)$\Leftrightarrow$(c) and (a)$\Rightarrow$(d). If $\tau_{\mathcal{U}}$ is surjective, then so is $\tau_{\mathcal{V}}$ for every subset $\mathcal{V}$ of $\mathcal{U}$. Thus (d)$\Rightarrow$(a).

For $\mathcal{V} \subset \mathcal{U}$ define $\mathcal{L} := \mathcal{U} \setminus \mathcal{V}$ and let $(\mathrm{f})_{\mathcal{V}}$ denote the assertion $\mathcal{V}, \mathcal{L} \in \mathcal{I}_{\mathcal{W}}$ and $\mathcal{V}_\cap \mathcal{L}_\cap = G$.

If $(\mathrm{f})_{\mathcal{V}}$, then $|\mathcal{V}_\cap \cap \mathcal{L}_\cap| = |\mathcal{V}_\cap||\mathcal{L}_\cap|/|G|$. As $\mathcal{L}, \mathcal{V} \in \mathcal{I}_{\mathcal{W}}$, we can compute both sides of this equation in terms of $|U|$ for $U \in \mathcal{U}$. This gives $(\mathrm{f})_{\mathcal{V}} \Rightarrow$(b).

If (a) is true, then

$$\begin{aligned} |\mathcal{V}_\cap \mathcal{L}_\cap| &= |\mathcal{V}_\cap||\mathcal{L}_\cap|/|\mathcal{V}_\cap \cap \mathcal{L}_\cap| \\ &= |G||\mathcal{V}_\cap|/|G| \qquad |\mathcal{L}_\cap|/|G| \qquad |G|/|\mathcal{U}_\cap| \\ &= |G|\textstyle\prod_{V\in\mathcal{V}} |V|/|G| \quad \prod_{L\in\mathcal{L}} |L|/|G| \quad \prod_{U\in\mathcal{U}} |G|/|U| = |G|. \end{aligned}$$

So (a)$\Rightarrow(\mathrm{f})_{\mathcal{V}}$. As (a) does not depend on $\mathcal{V}$, we have (b)$\Leftrightarrow$(a)$\Leftrightarrow$(f)$\Leftrightarrow(\mathrm{f})_{\mathcal{V}}$.

Of course (f)$\Rightarrow$(e) (just set $\mathcal{V} = \{U\}$).

Suppose (e). Then for every $U \in \mathcal{U}$ and all $X \in \mathcal{U}\setminus\{U\}$, we have $X(\mathcal{U}\setminus\{U\})_\cap = G$. So $\mathcal{U} \setminus \{U\}$ still satisfies (e) and we may assume (induction) $\mathcal{U} \setminus \{U\} \in \mathcal{I}_{\mathcal{W}}$. Hence (e)$\Rightarrow(\mathrm{f})_{\{U\}}\Leftrightarrow$(f).

2. Let $I = \{i_0 > i_1 > \cdots > i_n\}$. Then $H_{i_0} \leq U_{i_j}$ for $j \geq 1$. Hence $U_{i_0}\{U_{i_j}\colon j \geq 1\}_\cap \geq U_{i_0} H_{i_0} = G$.

By induction, $\{U_{i_j}\colon j \geq 1\} \in \mathcal{I}_{\mathcal{W}}$ and so $\{U_{i_j}\colon j \geq 0\} \in \mathcal{I}_{\mathcal{W}}$.

We have

$$\begin{aligned} H_{i_j}(U_{i_0} \cap U_{i_1} \cap \cdots \cap U_{i_j}) &= H_{i_j} H_{i_0}(U_{i_0} \cap U_{i_1} \cap \cdots \cap U_{i_j}) \\ &= H_{i_j}(H_{i_0} U_{i_0} \cap U_{i_1} \cap \cdots \cap U_{i_j}) = H_{i_j}(U_{i_1} \cap \cdots \cap U_{i_j}) \\ &= H_{i_j} U_{i_j} = G \end{aligned}$$

3. $g \in U\,U^g \Leftrightarrow g \in U \Rightarrow U = U^g$.

4. If $\mathcal{U} \in \mathcal{I}_{\mathcal{W}}$, then there is a $g \in G$ such that $g^{-1}U = g_U{}^{-1}U$ for all U (see above). So $\mathcal{U}$ and $\{U^g\colon U \in \mathcal{U}\} = \{U^{g_U}\colon U \in \mathcal{U}\}$ are conjugate.

Since no two elements of $\mathcal{U}$ are conjugate, the same argument works for $\{U^{g_U} : U \in \mathcal{U}\} \in \mathcal{I}_{\mathcal{W}}$. □

DEFINITION 2.2.8. If $G := A_0 \geq A_1 \geq A_2 \geq \cdots \geq A_l \geq A_{l+1} := E$ are normal in G and $\mathcal{H}$ is a chief-series, we say that $\mathcal{H}$ is a chief-series through all A_i's if $A_i \in \mathcal{H}$ for all $i \leq l$.

We call A_1/A_2 a chief-factor, if there is a chief-series $(H_i)_{i\leq k}$ and an i such that $A_1 = H_i$ and $A_2 = H_{i+1}$.

We say that $U \in M(G)$ supplements A_1/A_2 if $A_1 U = G$ and $U \geq A_2$.

We say that the chief-factor C/D is above (resp. below, resp. between) A_1/A_2, if $D \geq A_1$ (resp. $C \leq A_2$, resp. $A_2 \leq D \leq C \leq A_1$).

We say C/D is compatible with $\{A_i : i \leq l\}$, if there exists an $0 \leq i \leq l+1$ such that $A_{i+1} \leq D \leq C \leq A_i$.

3. $\mathcal{C}$-independent sets

In this section we prove:

THEOREM 3.1. *Let G denote a finite group. Then* $(M(G), \mathcal{I}_C)$ *is a matroid.*

If $U, L \in M(G)$ *and* $U \neq L$, *then* $\{U, L\} \notin \mathcal{I}_C$ *if and only if the intersection over all conjugates of U is the intersection over all conjugates of L.*

Let $(\mathbf{proj}(M(G), \mathbf{proj}(\mathcal{I}_C))$ *denote the projective matroid of* $(M(G), \mathcal{I}_C)$.

The minimal direct factors of $(\mathbf{proj}(M(G), \mathbf{proj}(\mathcal{I}_C))$ *are either the matroids constructed from complete graphs or the projective matroids associated to vector spaces* (*see Example* 2.1.3).

Let us sketch the proof:

Theorem 3.2.8 gives some factors (see Theorem 2.1.2.2) of $(M(G), \mathcal{I}_C)$ as simplicial complex.

Lemma 3.3.1 gives a partition of $M(G)$ that enables use to apply Theorem 2.1.2.3 (and later on Theorem 2.1.2.4).

We use this partition and factorisation in Lemmas 3.4.1 and 3.4.3 to construct matroids (like those in Example 2.1.3).

So by Theorem 2.1.2.3 the factors are matroids.

Now Theorem 2.1.2.2 and 4 show that $(M(G), \mathcal{I}_C)$ is a matroid and that we have constructed the associated projective matroid.

The minimal direct factors of $(M(G), \mathcal{I}_C)$ can be deduced from Lemma 3.4.4 and the factorisation of Theorem 3.2.8.

3.1. Core and crown.

DEFINITION 3.1.1. For $U \leq G$ define

$$\operatorname{core}(U) := \bigcap_{g \in G} U^g$$

(so core(U) is the kernel of the permutation action of G on G/U).

Let N denote the product of all minimal normal subgroups of $G/\operatorname{core}(U)$. Define crown(U) by $\operatorname{crown}(U)/\operatorname{core}(U) = N$.

The structure of $\operatorname{crown}(U)/\operatorname{core}(U)$ is rather restricted:

THEOREM 3.1.2 (Baer). *Suppose* $U \in M(G)$ *and* $\operatorname{core}(U) = E$. *Then one of the following hold*:

1. *G has a unique minimal normal subgroup N.*
   N is abelian, $U \cap N = E$ *and* $UN = G$.

2. *G has a unique minimal normal subgroup N.*
   N is non-abelian and $UN = G$.
3. *G has exactly two minimal normal subgroups A, B.*
   A and B are isomorphic but non-abelian. $AB \cap U$ is the diagonal subgroup of AB.
   AB/B (resp. AB/A) is the unique minimal normal subgroup of G/B (resp. G/A).

Furthermore, if A is a non-trivial normal subgroup of G, then $C_G(A)$ is either trivial or a minimal normal subgroup of G.

Hence, if A is a minimal normal subgroup of G, then $AC_G(A)$ is the product of all minimal normal subgroups of G.

Proof. See [Baer], Section 2. □

LEMMA 3.1.3. *Fix $U \in M(G)$.*

1. *If $B \leq A$ are normal in G and $B \leq$ core$(U) \not\geq A$, then there exists a chief-factor $\bar{A}/\bar{B}$ such that $B \leq \bar{B} \leq$ core$(U) \not\geq \bar{A} \leq A$.*
2. *If A/B is a chief-factor, then U supplements A/B if and only if $B \leq$ core$(U) \not\geq A$.*
3. *Suppose U supplements the chief-factor A/B.*
   Then crown$(U) = C_G(A/B)A$ *and* $A/B \cong A\text{core}(U)/\text{core}(U)$ *as groups with G-action.*
   If in addition A/B is abelian, then crown$(U) = C_G(A/B)$ *and*
   $$\text{crown}(U)/\text{core}(U) \cong A/B \text{ as } G\text{-modules.}$$
   Recall: A/B is an elementary abelian p-group for some prime p. Now the conjugation action of G on A/B gives A/B the structure of an (irreducible) $\mathbb{F}_pG$-module ($\mathbb{F}_p$ is the field with p elements).
4. *If A/B and C/D are chief-factors and U supplements both, then $A/B \cong C/D$ as groups.*

Proof. 1. Let $\bar{B} := A \cap \text{core}(U)$, then $B \leq \bar{B} < A$. Hence there exists a normal subgroup $\bar{A}$ such that $\bar{A}/\bar{B}$ is a chief-factor and $\bar{A} \leq A$. If $\bar{A} \leq \text{core}(U)$, then $\bar{A} \leq A \cap \text{core}(U) = \bar{B}$, a contradiction.

2. U supplements $A/B \Leftrightarrow B \leq U \not\geq A$ (Lemma 2.2.1) $\Leftrightarrow B \leq U^g \not\geq A$ (as A and B are normal) $\Leftrightarrow B \leq \text{core}(U) \not\geq A$.

3. The map $aB \to a\,\text{core}(U)$ is an isomorphism (as groups with G-action) from A/B onto $A\text{core}(U)/\text{core}(U)$ (this map is an epimorphism and, since A/B is a chief-factor and $A\text{core}(U) \neq \text{core}(U)$, it has to be an isomorphism). So $A/B \cong A\text{core}(U)/\text{core}(U)$ as groups with G-action. Hence $\text{core}(U) \leq C_G(A/B)$. Now (see Theorem 3.1.2 (Baer)) $\text{crown}(U) = C_G(A/B)A$.

If $\mathrm{crown}(U)/\mathrm{core}(U)$ is a chief-factor (and this is true if A/B is abelian), then Theorem 3.1.2 gives $A/B \cong \mathrm{crown}(U)/\mathrm{core}(U)$ as groups with G-action. If A/B is abelian, then $A \leq C_G(A/B)$.

4. As already proved, A/B and C/D are isomorphic (as groups with G-action) to some minimal normal subgroups of $\mathrm{crown}(U)/\mathrm{core}(U)$. But all these subgroups are isomorphic as groups (see Baer), and so $A/B \cong C/D$ (as groups). □

3.2. Direct factors and types.

DEFINITION 3.2.1. Suppose $U, \bar{U} \in M(G)$. We say that U and $\bar{U}$ have the same type, if

1. $\mathrm{crown}(U) = \mathrm{crown}(\bar{U})$ and
2. $\mathrm{crown}(U)/\mathrm{core}(U)$ and $\mathrm{crown}(\bar{U})/\mathrm{core}(\bar{U})$ are, either both abelian and isomorphic as G-modules, or both non-abelian.

So "type" is an equivalence relation. Let Θ denote the set of all types.

For $\mathbf{T} \in \Theta$ let $\mathrm{crown}(\mathbf{T}) := \mathrm{crown}(U)$ for some $U \in \mathbf{T}$ (this is independent of the chosen U) and $\mathrm{core}(\mathbf{T}) := \bigcap_{U \in \mathbf{T}} \mathrm{core}(U)$.

If A/B is a chief-factor and $U \in \mathbf{T}$ supplements A/B, then we say that A/B has type $\mathbf{T}$ (note that the type of A/B is not defined if A/B possesses no supplement in $M(G)$).

LEMMA 3.2.2. *Suppose N is an abelian normal subgroup and $UN = G$. Then $U \cap N$ is normal in G.*

Suppose $U \cap N \neq N$. Then $U \in M(G)$ if and only if $N/(N \cap U)$ is a chief-factor.

Assume $\mathcal{X} \subseteq M(G)$ is minimal under the condition $\bigcap_{X \in \mathcal{X}} X \cap N = E$. Then $\bigcap_{X \in \mathcal{X}} X$ is a complement of N in G and $\bar{N}(\bigcap_{X \in \mathcal{X}} X)$ is a complement of $N/\bar{N}$ for all G-normal subgroups $\bar{N}$ of G.

Proof. Since N is normal, we have $U \leq N_G(N \cap U)$, and as N is abelian, we have $N \leq N_G(U \cap N)$. Hence $N_G(U \cap N) \geq UN = G$. So $N \cap U$ is normal in G.

If $U \in M(G)$ and $U \cap N < B \leq N$ for some normal subgroup B, then $B \not\leq U$ and therefore $BU = G$. Since $U \cap B = U \cap N$, we have $|B| = |G||U \cap B|/|U| = |N|$. Hence $B = N$ and $N/(N \cap U)$ is a chief-factor.

If $N/(N \cap U)$ is a chief-factor and $U \leq X \in M(G)$, then $U \cap N = X \cap N$ and so $|X||N|/|U \cap N| = |G| = |U||N|/|U \cap N|$. Hence $U = X \in M(G)$.

Fix an enumeration $\mathcal{X} = \{X_1, \ldots, X_l\}$ of $\mathcal{X}$. Let $N_0 := N$ and $N_i := \bigcap_{j<i} X_j \cap N$. Then $N_i > N_{i+1}$ by minimality of $\mathcal{X}$.

Thus X_i supplements N_i/N_{i+1} and Lemma 2.2.7 proves $N \bigcap_{X \in \mathcal{X}} X = G$.

If $\bar{N} \leq N$ is normal, then $\bar{N} \bigcap_{X \in \mathcal{X}} X$ is a complement of $N/\bar{N}$ in $G/\bar{N}$. □

LEMMA 3.2.3. *Suppose* $\mathbf{T} \in \Theta$ *and* A/B *is a chief-factor.*

1. *If* $U \in \mathbf{T}$ *and* $\bar{U} \in M(G)$ *supplements* A/B, *then* $\bar{U} \in \mathbf{T}$.
   Thus every chief-factor has at most one type.
2. *There is an* $X \subseteq \mathbf{T}$ *such that* $\mathrm{crown}(U)/\mathrm{core}(U)$ *is a chief-factor for all* $U \in X$ *and* $\mathrm{crown}(\mathbf{T})/\mathrm{core}(\mathbf{T}) = \mathrm{crown}(\mathbf{T})/\bigcap_{U\in X}\mathrm{core}(U) \cong \bigoplus_{U\in X}\mathrm{crown}(U)/\mathrm{core}(U)$.
3. *If* A/B *is a chief-factor compatible with* $\mathrm{crown}(\mathbf{T})/\mathrm{core}(\mathbf{T})$, *then* A/B *has type* $\mathbf{T}$ *if and only if* A/B *is between* $\mathrm{crown}(\mathbf{T})/\mathrm{core}(\mathbf{T})$.

Proof. 1. By assumption $\mathrm{crown}(U) = AC_G(A/B) = \mathrm{crown}(\bar{U})$.
Suppose A/B is abelian; then

$$\mathrm{crown}(U)/\mathrm{core}(U) \cong A/B \cong \mathrm{crown}(\bar{U})/\mathrm{core}(\bar{U})$$

as groups with G-action. So $\bar{U} \in \mathbf{T}$.

Suppose A/B is non-abelian; then so are $A\,\mathrm{core}(U)/\mathrm{core}(U)$ and $\mathrm{crown}(U)/\mathrm{core}(U)$. Similar for $\bar{U}$. Hence $\bar{U} \in \mathbf{T}$ in this case, too.

2. If N is normal and $X, Y \leq N$ are normal, then $N/(X\cap Y)$ is an epimorphic image of $N/X \oplus N/Y$ as groups with G-action. If N/Y is a chief-factor and $X \cap Y \neq Y$, then $N/(X\cap Y) \cong N/X \oplus N/Y$ as groups with G-action.

Therefore it is enough to prove that $\mathrm{core}(\mathbf{T})$ is an intersection of those $\mathrm{core}(U)$'s with $U \in \mathbf{T}$ and $\mathrm{crown}(U)/\mathrm{core}(U)$ a chief-factor.

Fix $U \in \mathbf{T}$ such that $\mathrm{crown}(U)/\mathrm{core}(U)$ is not a chief-factor. We will construct $U_1, U_2 \in \mathbf{T}$ such that $\mathrm{crown}(\mathbf{T})/\mathrm{core}(U_i)$ is a chief-factor and $\mathrm{core}(U_1)\cap\mathrm{core}(U_2) = \mathrm{core}(U)$ (this will be sufficient to prove this part of our lemma).

In doing so, we may assume $\mathrm{core}(U) = E$.

By Theorem 3.1.2 (Baer) we find minimal non-abelian normal subgroups X, Y of $\mathrm{crown}(U)$ such that $XY = \mathrm{crown}(U)$. Let S_1 denote a non-trivial Sylow subgroup of X (so S_1 is a proper subgroup of X since, X is non-abelian). Then $N_G(S)\mathrm{crown}(U) = G$ (Frattini argument) and $Y \leq N_G(S) \cap \mathrm{crown}(U) \leq \mathrm{crown}(U)$. Fix U_1 with $N_G(S) \leq U_1 \in M(G)$. This U_1 is a supplement of X. Since U is also a supplement of X we have $U_1 \in \mathbf{T}$. Furthermore $\mathrm{crown}(U_1)/\mathrm{core}(U_1) = \mathrm{crown}(\mathbf{T})/Y$ is a chief-factor. Similarly we find $U_2 \in \mathbf{T}$ that supplements Y such that $\mathrm{core}(U_2) = X$. So $U_2 \in \mathbf{T}$ and $\mathrm{core}(U) = E = Y \cap X = \mathrm{core}(U_1) \cap \mathrm{core}(U_2)$.

3. Suppose A/B has type $\mathbf{T}$. We have to show that $A \not\leq \mathrm{core}(\mathbf{T})$ (i.e., A/B is not below $\mathrm{core}(\mathbf{T})$) and $B \not\geq \mathrm{crown}(\mathbf{T})$ (i.e. A/B is not above $\mathrm{crown}(\mathbf{T})$).

Since $A/B \in \mathbf{T}$, there exists a $U \in \mathbf{T}$ such that $B \leq \mathrm{core}(U) \not\geq A$.

So $B < A \leq AC_G(A/B) = \mathrm{crown}(\mathbf{T})$ and $A \not\leq \mathrm{core}(U) \geq \mathrm{core}(\mathbf{T})$.

This proves this case.

Suppose $\mathrm{core}(\mathbf{T}) \leq B < A \leq \mathrm{crown}(\mathbf{T})$. We may assume $\mathrm{core}(\mathbf{T}) = E$.

As already shown, there is an l and supplements $U_i \in \mathbf{T}$ of the chief-factor $M_i := \mathrm{crown}(U_i)/\mathrm{core}(U_i)$ such that $\bigcap U_i \cap \mathrm{crown}(\mathbf{T}) = E$ and $\mathrm{crown}(\mathbf{T})/\mathrm{core}(\mathbf{T}) \cong \oplus_{i\leq l} M_i$. Let N_i denote the preimage of $\bigcap_{i\neq j\leq l} M_j$.

Suppose A/B is non-abelian. Then all N_i's are non-abelian, and so there exists an a such that $A = B \oplus N_a$. Hence $U_a A = G$ and $B \leq U_a$. Thus A/B has type **T**.

Suppose A/B is abelian. Then so is crown(**T**). Hence $K := \bigcap_{i \in I} U_i$ satisfies Kcrown(**T**) $= G$ and $K \cap$ crown(**T**) $= E$ (see Lemma 3.2.2). As crown(**T**) is a direct product of minimal normal subgroups, we find a normal subgroup N such that $NA =$ crown(**T**) and $N \cap A = B$. Now $KNA = G$ and $KN \geq B$. Since $[G : KN] = |A/B| \neq 1$, it follows that $KN \in M(G)$ and crown$(KN) = C_G(A/B) = C_G(M_i) =$ crown(**T**). So $KN \in \mathbf{T}$ is a supplement of A/B. □

LEMMA 3.2.4. *Let* $\mathbf{T} \in \Theta$ *and* $X \subseteq \mathbf{T}$. *Then* X *is* $\mathcal{C}$*-independent if and only if there exists a chief-series* $\mathcal{L}$ *through* crown(**T**) *and* core(**T**) *such that* X *is* $\mathcal{L}$*-independent.*

Proof. If X is $\mathcal{L}$-independent for some chief-series $\mathcal{L}$ as above, then X is $\mathcal{C}$-independent.

So suppose $\mathcal{H}$ is a chief-series and $X \subseteq \mathbf{T}$ is $\mathcal{H}$-independent.

We project $\mathcal{H}$ to crown(**T**)/core(**T**) as follows:

Define $L_i :=$ crown(**T**) $\cap$ ($H_i$core(**T**)), then

$$\text{crown}(\mathbf{T}) \geq L_i \geq L_{i+1} \geq \text{core}(\mathbf{T}).$$

If there is a $U \in X$ that supplements H_i/H_{i+1}, then $H_i \leq H_i C_G(H_i/H_{i+1}) =$ crown(**T**) and so $L_i = H_i$core(**T**). Thus $UL_i = G$. Moreover, $L_{i+1} = H_{i+1}$core(**T**) $\leq L_i \cap U$.

This proves that U supplements (some chief-factor between) L_i/L_{i+1}.

So every chief-series $\mathcal{L}$ that contains all L_i's, crown(**T**) and core(**T**) satisfies the conclusion of our lemma (and at least one such $\mathcal{L}$ exists, as already shown). □

COROLLARY 3.2.5. *Suppose* $X \subseteq \mathbf{T} \in \Theta$ *and* $\bigcap_{x \in X}$ core$(x) = Y$. *Then* $X \in \mathcal{I}_{\mathcal{C}}$ *if and only if there exists a chief-series* $\mathcal{H}$ *through* crown(**T**) *and* Y *such that* X *is* $\mathcal{H}$*-independent.*

Proof. In the proof of the last lemma replace core(**T**) by Y. □

LEMMA 3.2.6. *Suppose* $\mathbf{T} \in \Theta$. *Let* $M \leq$ crown(**T**) *denote a normal subgroup of* G *such that* $MU = G$ *for all* $U \in \mathbf{T}$ *and let* $N := M \cap$ core(**T**).

Then M core(**T**) $=$ crown(**T**).

Furthermore $X \subseteq \mathbf{T}$ *is in* $\mathcal{I}_{\mathcal{C}}$ *if and only if* $X \in \mathcal{I}_{\mathcal{L}}$ *for some chief-series* $\mathcal{L}$ *through* M *and* N.

Proof. If Mcore(**T**) $<$ crown(**T**), then there is a $U \in \mathbf{T}$ that supplements a chief-factor between crown(**T**) and M core(**T**), hence (by Lemma 3.2.3) $MU \leq M$ core(**T**)$U = U$, a contradiction.

If $\mathcal{H}$ is a chief-series through M and N and X is $\mathcal{H}$-independent, then X is $\mathcal{C}$-independent.

So suppose $X \in \mathcal{I}_{\mathcal{C}}$. By Lemma 3.2.4 we find a chief-series $\mathcal{H}$ through crown(**T**) and core(**T**) such that X is $\mathcal{H}$-independent. Let $H_{i_1} = \text{crown}(\mathbf{T})$ and $H_{i_2} = \text{core}(\mathbf{T})$. The isomorphism

$$M/N \cong M\text{core}(\mathbf{T})/\text{core}(\mathbf{T}) = \text{crown}(\mathbf{T})/\text{core}(\mathbf{T}) = H_{i_1}/H_{i_2}$$

gives L_i's such that $N \leq L_i \leq M$ and $L_i\text{core}(\mathbf{T}) = H_i$ for $i_1 \leq i \leq i_2$.

If U_i supplements H_i/H_{i+1} and $i_1 + 1 \leq i \leq i_2$, then $U_i L_i = U_i\text{core}(\mathbf{T})L_i = U_i H_i = G$ and $U_i \geq H_{i+1} \geq L_{i+1}$. Therefore X is $\mathcal{L}$-independent for any chief-series $\mathcal{L}$ through $\{L_i\colon i_1 \leq i \leq i_2\}$. As already shown at least one such $\mathcal{L}$ exists and $M, N \in \mathcal{L}$. □

DEFINITION 3.2.7. We now define (inductively) a series of normal subgroups of G.

Let $M_0 := G$, $N_0 := G$, $\mathbf{T}_0 := \{G\}$ and $\Theta_0 := \Theta$.

If, for all $j < i \geq 1$, we have defined M_j, N_j, $\mathbf{T}_j$ and Θ_j, and if $\Theta_{i-1} \neq \emptyset$, then define M_i, N_i, $\mathbf{T}_i$ and Θ_i by the following procedure:

1. Chose a $\mathbf{T}_i \in \Theta_{i-1}$ such that crown$(\mathbf{T}_i) \cap N_{i-1}$ is maximal in

$$\{\text{crown}(X) \cap N_{i-1}\colon X \in \Theta_{i-1}\}.$$

2. Define $M_i := \text{crown}(\mathbf{T}_i) \cap N_{i-1}$, $N_i := M_i \cap \text{core}(\mathbf{T}_i)$ and $\Theta_i := \Theta_{i-1} \setminus \{\mathbf{T}_i\}$.

Remark. Fix l such that $\Theta_{l-1} \neq \emptyset = \Theta_l$. The above definition gives an enumeration $\Theta = \{\mathbf{T}_i\colon 1 \leq i \leq l\}$ of Θ and a series $M_1 > N_1 \geq M_2 > N_2 \geq \cdots \geq M_l > N_l$ of normal subgroups, such that if $\mathcal{H}$ is a chief-series through all N_i's and M_i's and A/B is a chief-factor in $\mathcal{H}$, then A/B has type $\mathbf{T}_i$ if and only if A/B is between M_i/N_i.

This follows from the proof of the next theorem.

THEOREM 3.2.8. *Let $\mathcal{H}$ denote a chief-series. Then there exists a chief-series $\mathcal{L}$ through all M_i and N_i (defined as above) such that $\mathcal{I}_{\mathcal{H}} = \mathcal{I}_{\mathcal{L}}$. Hence $(M(G), \mathcal{I}_{\mathcal{C}})$ is the direct product of all $(\mathbf{T}, \mathcal{I}_{\mathcal{C}})$'s with $\mathbf{T} \in \Theta$.*

Proof. We claim that the M_i's and N_i's satisfy the hypothesis of the last lemma for $\mathbf{T} = \mathbf{T}_i$.

In doing so, we make an induction on i. The case $i = 1$ is trivial. Suppose our claim is true for $j < i$ and false for i.

Since $M_i \leq \text{crown}(\mathbf{T}_i)$ and $N_i = M_i \cap \text{core}(\mathbf{T}_i)$, this gives us a $U \in \mathbf{T}_i$ such that $M_i U \neq G$. Thus U supplements some chief-factor between M_j/N_j or N_j/M_{j+1}

for some $j < i$. In the first case $U \in \mathbf{T}_j \neq \mathbf{T}_i$, a contradiction. The second case cannot appear, for if A/B is a chief-factor between N_j/M_{j+1} with supplement U, then $N_j \cap \text{crown}(U) \geq A > B \geq M_{j+1}$ a contradiction to the choice of M_{j+1}.

This proves our claim.

Now, if X is $\mathcal{H}$-independent, then each $X_{\mathbf{T}_i} := X \cap \mathbf{T}_i$ is $\mathcal{H}$-independent and the two last lemmas show, that $X_{\mathbf{T}_i}$ is independent for a chief-series $\mathcal{L}_i$ through M_i/N_i. This is still true if we vary $\mathcal{L}_i$ above M_i and below N_i. Let Y_i denote the set of all normal subgroups in L_i between M_i and N_i. Then $Y := \bigcup Y_i$ is linearly ordered and every chief-series $\mathcal{L}$ through Y satisfies $\mathcal{I}_{\mathcal{L}} = \mathcal{I}_{\mathcal{H}}$.

Hence $(M(G), \mathcal{I}_{\mathcal{C}})$ is the direct product of the $\mathbf{T}$'s with $\mathbf{T} \in \Theta$. □

3.3. Projective $\mathcal{C}$-independence.

LEMMA 3.3.1. 1. *Suppose U, L are two different elements of $M(G)$. Then $\{L, U\} \in \mathcal{I}_{\mathcal{C}}$ if and only if* $\text{core}(U) \neq \text{core}(L)$.

2. *Suppose $X \subseteq M(G)$ and every two-element subset of X is in $\mathcal{I}_{\mathcal{C}}$. Fix $y_x \in M(G)$ such that* $\text{core}(y_x) = \text{core}(x)$ *and* $\text{crown}(y_x) = \text{crown}(x)$ *for all $x \in X$. Then $Y := \{y_x \colon x \in X\}$ is in $\mathcal{I}_{\mathcal{C}}$ if and only if X is.*

Proof. 1. Suppose $\text{core}(U) = \text{core}(L)$ and let $\mathcal{H}$ denote a chief-series such that U supplements H_i/H_{i+1} and L supplements H_j/H_{j+1} with $i < j$. Then $H_j \leq H_{i+1} \leq \text{core}(U) = \text{core}(L) \leq L$. So $LH_j = L < G$. A contradiction. Since $\mathcal{H}$ was arbitrary, we conclude $\{U, L\} \notin \mathcal{I}_{\mathcal{C}}$.

Suppose $\text{core}(U) \neq \text{core}(L)$. We may assume $\text{core}(U) \not\leq \text{core}(L)$. Then $\text{core}(U)L \not\leq L$. As L is a maximal subgroup, we get $\text{core}(U)L = G$. So U supplements some chief-factor above $\text{core}(U)$ and L some below. Hence, if $\text{core}(U) \in \mathcal{H} \in \mathcal{C}$, then $\{U, L\} \in \mathcal{I}_{\mathcal{H}} \subseteq \mathcal{I}_{\mathcal{C}}$.

2. Suppose $\mathcal{H}$ is a chief-series, X as above and X is $\mathcal{H}$-independent.

If $x \in X$ is a supplement of H_i/H_{i+1}, then $H_{i+1} \leq \text{core}(x) \not\geq H_{i+1}$ and y_x is a supplement of H_i/H_{i+1}, too. So Y is $\mathcal{H}$-independent.

On the other hand, the assumption about the two-element subsets of X implies that the map $x \to y_x$ is bijective.

Reversing the roles of Y and X shows that X is $\mathcal{H}$-independent if and only if Y is. Varying over all chief-series $\mathcal{H}$ finishes the proof of our lemma. □

3.4. Geometric and graphic factors. Lemma 3.3.1 and Theorem 2.1.2 show that the question of when a subset of $M(G)$ is $\mathcal{C}$-independent is a question about normal subgroups.

More explicit (we use Theorem 2.1.2, 3.2.8 and Lemma 3.3.1):

Let $P(G)$ denote the lattice of all normal subgroups of G and $N(G) := \{\text{core}(U)\colon U \in M(G)\}$. Define $(N(G), \mathcal{I}_{\mathcal{C}})$ as in Definition 2.2.2 (with $R = P = P(G)$ and $Q = N(G)$).

Then $(M(G), \mathcal{I}_{\mathcal{C}})$ is a matroid if and only if $(N(G), \mathcal{I}_{\mathcal{C}})$ is.

If $(M(G), \mathcal{I}_C)$ is a matroid, then $(N(G), \mathcal{I}_C)$ is the corresponding projective matroid.

Furthermore, for $\mathbf{T} \in \Theta$ let $N(\mathbf{T}) := \{\text{core}(U)\colon U \in \mathbf{T}\}$. Then the $N(\mathbf{T})$'s are the direct factors of $N(G)$ and so $(N(G), \mathcal{I}_C)$ is a matroid if and only if each $(N(\mathbf{T}), \mathcal{I}_C)$ is.

LEMMA 3.4.1. *Suppose that* $\mathbf{T} \in \Theta$ *and* $\text{crown}(\mathbf{T})/\text{core}(\mathbf{T})$ *is abelian.*

Then there is a prime p, an irreducible $\mathbb{F}_p G$*-module W and an n such that* $\text{crown}(\mathbf{T})/\text{core}(\mathbf{T}) \cong W^n$.

Let $K := \text{Hom}_G(W, W)$ *(so K is a field).*

Then $(N(\mathbf{T}), \mathcal{I}_C)$ *is isomorphic to the projective matroid of* K^n *(see Example* 2.1.3.1).

Proof. The existence of W and n is trivial. The map $\tau\colon \text{crown}(\mathbf{T}) \to W^n$ with kernel core($\mathbf{T}$) induces a bijection between $N(\mathbf{T})$ and the maximal submodules of W^n (see Lemma 3.2.2). This submodules correspond to the kernels of the non-trivial maps in $\text{Hom}_G(W^n, W) \cong K^n$. Tracing back the linear independence of the projective matroid of K^n to $N(\mathbf{T})$ proves our lemma. □

3.4.1. *The non-abelian case.* Suppose that $\mathbf{T} \in \Theta$ and $\text{crown}(\mathbf{T})/\text{core}(\mathbf{T})$ is non-abelian. Doing our calculations in $G/\text{core}(\mathbf{T})$, we may assume $\text{core}(\mathbf{T}) = E$.

So $\text{crown}(\mathbf{T}) \cong \times_{i \le j_0} N_i$, where $N_1, \ldots, N_{j_0}$ are the minimal (non-abelian) G-normal subgroups of crown($\mathbf{T}$). Define $J := \{i\colon 1 \le i \le j_0\}$ and let $\mathbb{P}(J)$ denote the set of all subsets of J ordered by inclusion. For $I \in \mathbb{P}(J)$ let $N_I := \times_{i \in I} N_i$ (so $N_i = N_{\{i\}}$ and $N_\emptyset := E$). Since N_i is non-abelian, the map $\varphi\colon N_I \to I$ is a lattice isomorphism from the lattice of all G-normal subgroups of crown($\mathbf{T}$) to $\mathbb{P}(J)$.

Let $(N(J), \mathcal{I}_{-C})$ denote the image of $(N(\mathbf{T}), \mathcal{I}_C)$ under $\lambda\colon N_I \to J \setminus I$. So $N(J) = \{I \subseteq J\colon N_{J \setminus I} \in N(\mathbf{T})\}$.

LEMMA 3.4.2. $X \subseteq N(J)$ *is in* $\mathcal{I}_{-C}$ *if and only if there is a chain*

$$\emptyset =: I_0 \subset I_1 \subset \cdots \subset I_{|J|} := J$$

such that

$$|\{x \in X\colon I_{i+1} \cap x = \emptyset \neq I_i \cap x\}| \le 1 \textit{ for all } 1 \le i \le |J|.$$

In this case X is (by definition) $(I_i)_{i \in J}$*-independent.*

Proof. Suppose $X \in \mathcal{I}_{-C}$, then $Z := \lambda^{-1}(X) \in \mathcal{I}_C$. Hence there is a chief-series (H_i) through crown($\mathbf{T}$) such that (with $H_{i_0} = \text{crown}(\mathbf{T})$ and $H_{i_1} = E$):

$$|\{z \in Z\colon H_{i+1} \le z \not\ge H_i\}| \le 1 \text{ for all } i_1 > i \ge i_0.$$

For $0 \le i \le i_1 - i_0$, define $I_i := \varphi(H_{i_1 - i})$.

For $x \in X$, define $\lambda(x) = N_{J\setminus x} =: z$. Note: $H_{i_1-i} \leq z$ if and only if $I_i \subseteq (J \setminus x)$ hence $H_{i_1-(i+1)} \leq z \not\geq H_{i_1-i}$ if and only if $I_{i+1} \cap x = \emptyset \neq I_i \cap x$.

This proves one direction of our lemma, the opposite direction follows similarly. □

Note that $I \in N(J)$ implies $|I| \in \{1, 2\}$ (Baer). Every one-element subset of J is in $N(J)$ (see Lemma 3.2.3).

LEMMA 3.4.3. *Notation as above. Choose $\omega \notin J$. Let*

$$E := \{\{i, j\}: i, j \in J \cup \{\omega\}, i \neq j, J \setminus (\{i, j\} \setminus \{\omega\}) \in N(J)\}.$$

Then $\Gamma = (J \cup \{\omega\}, E)$ is a graph.

Moreover $(N(\mathbf{T}), \mathcal{I}_C) \cong (N(J), \mathcal{I}_{-C}) \cong (E, \mathcal{I}_\Gamma)$; in particular, $(N(\mathbf{T}), \mathcal{I}_C)$ and $(\mathbf{T}, \mathcal{I}_C)$ are matroids.

Proof. We claim that τ: $N(J) \to E$; $\tau(\{i\}) := \{i, \omega\}$, $\tau(\{i, j\}) := \{i, j\}$ for $i \neq j \in J$ gives an isomorphism between $(N(J), \mathcal{I}_{-C})$ and $(E, \mathcal{I}_\Gamma)$.

Let τ also denote the map from all subsets of $N(J)$ to all subsets of E induced by τ. Note that τ is a bijection.

1. Assume $X \subseteq E$ is not in $\mathcal{I}_\Gamma$. Then X contains a minimal circuit Y. Suppose $Z := \tau^{-1}(Y)$ (so $|Z| = |Y|$) is $(I_i)_{i \in J}$-independent for some (I_i). Let J' denote the set of all $j \in J$ with: $\{j, j'\} \notin Z$ for all $j' \in J$. Then Z is $(I'_j)_{j \in J}$-independent for every chain (I'_j) with $I'_{j+|J'|} = I_j \cup J'$. So $|Z| \leq |J| - |J'|$ and, if no one-element set is in Z, then $|Z| \leq |J| - |J'| - 1$ (since in this case we may add $J \setminus I'_{|J|} \in N(J)$ to Z and still get an (I'_i)-independent set).

We now use the fact that Y is a circuit.

First, assume that some $\{j\}$ is in Z. Then $((J \setminus J') \cup \{\omega\}, Y)$ is a cyclic graph and so $|Y| = |(J \setminus J') \cup \{\omega\}| = |J| - |J'| + 1 \neq |Z|$, a contradiction.

If there is no $(j, \omega) \in Y$, then $((J \setminus J'), Y)$ is a cyclic graph and so $|Y| = |(J \setminus J')| = |J| - |J'| \neq |Z|$, a contradiction, too.

Hence $Z \notin \mathcal{I}_{-C}$ and $\tau^{-1}(X) \notin \mathcal{I}_{-C}$.

2. Now suppose $X \subseteq E$ is in $\mathcal{I}_\Gamma$. We have to show that $Z := \tau(X) \in \mathcal{I}_{-C}$. Therefore we may assume that X is maximal in $\mathcal{I}_\Gamma$ (hence $(J \cup \{\omega\}, X)$ is a spanning tree since Γ is connected). So there is some $\{j_1, \omega\} \in X$.

We now define I_i and X_i inductively.

Let $I_1 := \{j_1\}$ and $X_1 := \{\{j_1, \omega\}\}$.

Suppose I_j, X_j is defined for all $j \leq i < |J|$.

Choose $\{a_{i+1}, b_{i+1}\} \in X \setminus X_i$ such that $a_{i+1} \in I_i \cup \{\omega\}$ and $b_{i+1} \in J \setminus I$.

Define $I_{i+1} := I_i \cup \{b_{i+1}\}$ and $X_{i+1} := X_i \cup \{\{a_i, b_i\}\}$.

We have to show that this is possible. In doing so, it is enough to find $a_{i+1} \in I_i \cup \{\omega\}$ and $b_{i+1} \in J \setminus X_i$ such that $\{a_{i+1}, b_{i+1}\} \in X$.

Note (or take as additional induction hypothesis) that $|I_i| = i = |X_i|$ and $(I_i \cup \{\omega\}, X_i)$ is a connected subgraph of $(J \cup \{\omega\}, X)$.

Since $|I_i| < |J|$ and X is a spanning tree we find $b \in J \setminus I_i$ and a path $b := y_0, y_1, \dots, y_l := \omega$ in X (so $\{y_r, y_{r+1}\} \in X$). Let r_0 denote the largest r such that $\{y_r, y_{r+1}\} \notin X_i$ (as $\{y_0, y_1\} \notin X_i$, this is possible).

Then $y_{r_0+1} = y_l$ or $\{y_{r_0+1}, y_{r_0+2}\} \in X_i$. In both cases, we have

$$y_{r_0+1} \in I_i \cup \{\omega\}.$$

If $y_{r_0} \in I_i \cup \{\omega\}$, there would be a path in X_i from y_{r_0} (to ω and from ω) to y_{r_0+1}. But this gives a circuit in X. Hence $y_{r_0} \notin I_i \cup \{\omega\}$. Therefore we may define $a_{i+1} := y_{r_0+1}$ and $b_{i+1} := y_{r_0}$. This proves that our inductive definition of X_i and I_i works.

Now, it is easy to verify that Z is (I_j)-independent.

So $(E, \mathcal{I}_\Gamma) \cong (N(J), \mathcal{I}_{-C})$: $\cong (N(\mathbf{T}), \mathcal{I}_C)$ as simplicial complexes, and $(E, \mathcal{I}_\Gamma)$ is a matroid (see Example 2.1.3.2). This proves our lemma. □

LEMMA 3.4.4. *If $\{j_1, j_2, j_3\}$ is a three-element subset of J and $\{j_1, j_2\}$ and $\{j_2, j_3\}$ are in $N(J)$, then $\{j_1, j_3\} \in N(J)$.*

In addition: $(N(\mathbf{T}), \mathcal{I}_C)$ is a direct product of matroids of complete graphs.

Proof. In proving $\{j_1, j_3\} \in N(J)$, we may assume $j_i = i$ and $|J| = 3$.

Therefore crown$(\mathbf{T}) = N_1 \times N_2 \times N_3$ and there is $\tau_{1,2} \in \mathrm{Hom}(N_1, N_2)$ such that $U_{1,2} := \{g \in G\colon \tau_{1,2}(n^g) = \tau_{1,2}(n)^g \text{ for all } n \in N_1\} \in M(G)$ and core$(U_{1,2}) = N_3$ (Baer). Similarly we find $\tau_{2,3}$ and $U_{2,3}$.

Hence $\tau_{1,3} := \tau_{2,3}\tau_{1,2}$ is an isomorphism from N_1 to N_3. Define $U_{1,3} := \{g \in G\colon \tau_{1,3}(n^g) = \tau_{1,3}(n)^g \text{ for all } n \in N_1\}$ so $U_{1,3} < G$. We have $U_{1,3} \geq (U_{1,2} \cap U_{2,3})N_2$. Now $U_{1,3}N_1 \geq (U_{1,2} \cap U_{2,3})N_1N_2 = (U_{1,2}N_1 \cap U_{2,3})N_2 = G$ and similarly $U_{1,3}N_3 = G$. Fix $U_{1,3} \leq X \in M(G)$. Then $XN_1 = XN_3 = G$ and core$(X) = N_2 \in N(\mathbf{T})$. This proves $\{1, 3\} \in N(J)$.

Consider now the graph $\Gamma = (J \cup \{\omega\}, E)$. It follows from the first part of our lemma that the graph $\Gamma' := (J, E \setminus \{\{\omega, j\}\colon j \in J\})$ is a disjoint union of complete graphs $\Gamma'_i := (J_i, E_i)$.

Define $\Gamma_i := (J_i \cup \{\omega\}, E_i \cup \{\{\omega, j\}\colon j \in J_i\})$. Then $V(\Gamma) = \bigcup V(\Gamma_i)$ and $E(\Gamma) = \bigcup E(\Gamma_i)$. So $X \in \mathcal{I}_\Gamma$ if and only if all $X_i := X \cap E(\Gamma_i) \in \mathcal{I}_{\Gamma_i}$. □

We have thus proved Theorem 3.1.

4. $\mathcal{W}$-independence

In this section we prove:

THEOREM 4.1. *Let G denote a finite group, π the set of all primes, $M^p(G)$ the set of all maximal subgroups of p-power index and let $M^\pi(G) := \bigcup_{p\in\pi} M^p(G)$.*

Then $(M^\pi(G), \mathcal{I}_\mathcal{W})$ is a matroid.

It is the direct product over all $(M^p(G), \mathcal{I}_\mathcal{W})$'s there p runs over π.

If $2 \neq p \in \pi$, then $(M^p(G), \mathcal{I}_{\mathcal{W}}) = (M^p(G), \mathcal{I}_{\mathcal{C}})$.
Furthermore for p a prime,

$$\mathcal{I}_{\mathcal{H}}(M^p(G))^{\cap} = \mathcal{I}_{\mathcal{C}}(M^p(G))^{\cap} = \mathcal{I}_{\mathcal{W}}(M^p(G))^{\cap} = S_c^p(G).$$

Here $S_c^p(G)$ is the set of all those subgroups U of p-power index in G for which the Möbius number $\mu(U, G)$ is not zero.

We would like to give a 'reason' why this theorem should be true:

Assume $\mathbf{T} \in \Theta$, core($\mathbf{T}$) $= 1$ and crown($\mathbf{T}$) $\cong W^m$ for an irreducible $\mathbb{F}_p G$ module W.

As $\mathcal{W}$-independence behaves well under conjugation (see Lemma 2.2.7), we look at conjugation classes of elements of $\mathbf{T}$. These conjugation classes correspond to pairs $(a, b) \in N(\mathbf{T}) \times H^1(G/\text{crown}(\mathbf{T}), W)$ (here $N(\mathbf{T}) = \{\text{core}(U)\colon U \in \mathbf{T}\}$ is the set of all maximal G-normal subgroup of crown($\mathbf{T}$)). ($\mathcal{C}$-independence just looks at $N(\mathbf{T})$ and it is true that $\mathcal{I}_{\mathcal{C}}(\mathbf{T}) = \mathcal{I}_{\mathcal{W}}(\mathbf{T})$ if $H^1(G/\text{crown}(\mathbf{T}), W) = 0$; see Lemma 4.3.3).

The elements of $H^1(G/\text{crown}(\mathbf{T}), W)$ and the G-module automorphisms of crown($\mathbf{T}$) correspond to certain automorphisms of G.

So we expect that the maximal $\mathcal{W}$-independent subsets of $\mathbf{T}$ have the form X^λ with λ running over all automorphisms of G and X running over a small, well-known set of $\mathcal{W}$-independent subsets of $\mathbf{T}$ (see Lemma 4.5.3). Once we have such a description of $\mathcal{I}_{\mathcal{W}}(\mathbf{T})$, we can check directly that $(\mathbf{T}, \mathcal{I}_{\mathcal{W}})$ is a matroid (compare Lemma 4.5.4).

In general however, it is not true that $\mathbf{T}$ is a factor of $(M^p(G), \mathcal{I}_{\mathcal{W}})$, so we have to modify the above ideas.

Furthermore, we have to be careful about the supplements of non-abelian chief-factor. This is one reason, why we restrict our attention to subgroups of prime power index.

EXAMPLE 4.2. *We construct some groups G such that $(M(G), \mathcal{I}_{\mathcal{W}})$ is not a matroid.*

Let S denote a simple group and $\mathcal{U}$ a maximal subset of $(M(S), \mathcal{I}_{\mathcal{W}})$ with $|\mathcal{U}| \geq 2$ (such a $\mathcal{U}$ exists for $S \cong A_5$).

Define $G := S \times S$, $\Delta := \{(g, g)\colon g \in S\} \leq G$, $\mathcal{U}_1 := \{(U, S), (S, U)\colon U \in \mathcal{U}\}$ and $\mathcal{U}_2 := \{(U, S), \Delta\colon U \in \mathcal{U}\}$.

Then $\mathcal{U}_1$ and $\mathcal{U}_2$ are maximal in $\mathcal{I}_{\mathcal{W}}(M(G))$ and $|\mathcal{U}_1| = 2|\mathcal{U}| > |\mathcal{U}| + 1 = |\mathcal{U}_2|$. Hence $(M(G), \mathcal{I}_{\mathcal{W}})$ is not a matroid.

4.1. A decomposition of $\mathcal{I}_{\mathcal{W}}$.

LEMMA 4.1.1. *If $\mathcal{U}$ is a $\mathcal{W}$-independent subset of $M^p(G)$, then $\bigcap_{U \in \mathcal{U}} U$ has p-power index in G.*

$(\bigcup M^p(G), \bigcup \mathcal{I}_{\mathcal{W}})$ is the direct product (as simplicial complexes) of all $(M^p, \mathcal{I}_{\mathcal{W}})$'s with p a prime dividing $|G|$.

Proof. The first assertion follows from $[G\colon \bigcap_{U\in\mathcal{U}} U] = \prod_{U\in\mathcal{U}}[G : U]$.

If U and V have coprime index, then $[G : U]$, $[G : V]$ and $[G : U][G : V]$ divide $[G : U \cap V]$. So $|UV| = |U||V|/|U \cap V| \geq |G|$.

Fix a set π of primes and let π' denote the set of all primes not in π. For $X \subset \bigcup_{p\in\pi\cup\pi'} M^p(G)$ let $X_\pi := \{x \in X\colon \exists p \in \pi \text{ s.t. } x \in M^p(G)\}$ and define $X_{\pi'}$ similarly.

If X is $\mathcal{W}$-independent, then so are X_π and $X_{\pi'}$. Now

$$\left(\bigcap_{x\in X_\pi} x\right)\left(\bigcap_{x\in X_{\pi'}} x\right) = G ,$$

since $[G\colon \bigcap_{x\in X_\pi} x]$ and $[G\colon \bigcap_{x\in X_{\pi'}} x]$ are coprime. So $X_\pi \cup X_{\pi'}$ is in $\mathcal{I}_\mathcal{W}$ (see Lemma 2.2.7). □

LEMMA 4.1.2. *If $U \in M^p(G)$, then $G/\text{core}(U)$ has a unique minimal normal subgroup.*

Suppose A/B is a non-abelian chief-factor. Then $\{U \in M^p(G)\colon AU = G, U \geq B\}$ is a direct factor of $(M^p(G), \mathcal{I}_\mathcal{C})$.

Proof. If $G/\text{core}(U)$ has two different minimal normal subgroups A and B, then A is non-abelian and $[G : U] = |A|$ is divisible by more than one prime. So $U \notin M^p(G)$ (Baer).

Let $U \in \mathbf{T} \in \Theta$ with $\text{crown}(\mathbf{T})/\text{core}(\mathbf{T})$ non-abelian. The projective matroid associated to $(\mathbf{T} \cap M^p(G), \mathcal{I}_\mathcal{C})$ is a direct product of graph matroids. But the edges (notation as in Lemma 3.4.3, 3.4.4) $\{i, j\}$ with $i, j \in J$ do not correspond to subgroups in M^p (by the first part of this lemma). So the projective matroid is the direct product of all one-element subsets of $\mathbf{proj}(\mathbf{T} \cap M^p(G))$. Since $\mathbf{proj}(\mathbf{T} \cap M^p(G))$ is a direct factor of $(\mathbf{proj}(M^p(G)), \mathbf{proj}(\mathcal{I}_\mathcal{C}))$, this proves our lemma. □

THEOREM 4.1.3. *Suppose p is a prime such that each pair $\{U, L\} \subseteq M^p(G)$ is $\mathcal{W}$-independent if and only if it is $\mathcal{C}$-independent.*

Then $\mathcal{I}_\mathcal{W}(M^p(G)) = \mathcal{I}_\mathcal{C}(M^p(G))$.

Remark. Once we know that $(M^p(G), \mathcal{I}_\mathcal{W})$ is a matroid we can reformulate this theorem as follows:

If $(\mathbf{proj}_\mathcal{W}(M^p(G)), \mathbf{proj}_\mathcal{W}(\mathcal{I}_\mathcal{W}))$ (resp. $(\mathbf{proj}_\mathcal{C}(M^p(G)), \mathbf{proj}_\mathcal{C}(\mathcal{I}_\mathcal{C}))$) denotes the projective matroid of $(M^p(G), \mathcal{I}_\mathcal{W})$ (resp. $(M^p(G), \mathcal{I}_\mathcal{C})$), then

$$\mathbf{proj}_\mathcal{W}(M^p(G)) = \mathbf{proj}_\mathcal{C}(M^p(G)) \text{ implies } \mathcal{I}_\mathcal{W}(M^p(G)) = \mathcal{I}_\mathcal{C}(M^p(G)).$$

Proof. We already know that $\mathcal{I}_\mathcal{C}(M^p(G)) \subseteq \mathcal{I}_\mathcal{W}(M^p(G))$ (see Lemma 2.2.7). Suppose now $X \in \mathcal{I}_\mathcal{W}(M^p(G)) \setminus \mathcal{I}_\mathcal{C}(M^p(G))$. Then there is a type $\mathbf{T}$ such that $X \cap \mathbf{T} \notin \mathcal{I}_\mathcal{C}$ and we may assume $X \subseteq \mathbf{T}$.

Case 1. crown($\mathbf{T}$)/core($\mathbf{T}$) is non-abelian.

Then there is a minimal direct factor $\mathbf{T}_1$ of $(\mathbf{T} \cap M^p(G), \mathcal{I}_C)$ such that $X \cap \mathbf{T}_1 \notin \mathcal{I}_C$. We may assume $X \subseteq \mathbf{T}_1$.

Since no two-element set is in $\mathcal{I}_C(\mathbf{T}_1)$ (see Lemma 4.1.2) no two-element subset is in $\mathcal{I}_C(\mathbf{T}_1)$ by assumption. Since all one-element subsets are in $\mathcal{I}_C$, we have $\mathcal{I}_{\mathcal{W}}(M^p(G)) = \mathcal{I}_C(M^p(G))$ in this case.

Case 2. crown($\mathbf{T}$)/core($\mathbf{T}$) is abelian. We may assume core($\mathbf{T}$) $= E$ and that X is a maximal subset of $\mathcal{I}_{\mathcal{W}}(\mathbf{T})$.

Let X' denote a maximal $\mathcal{C}$-independent subset of X.

Then $\bigcap_{x \in X} x \cap \text{crown}(\mathbf{T}) = \bigcap_{x \in X'} x \cap \text{crown}(\mathbf{T}) = E$ (see Lemma 3.2.3). So $K := \bigcap_{x \in X'} x$ is a complement of crown($\mathbf{T}$) in G (see Lemmas 2.2.7 and 3.2.2).

By assumption we, find $x \in X \setminus X'$. Then $K_1 := K\text{core}(x)$ complements crown($\mathbf{T}$)/core(x) and so $K_1 \in \mathbf{T}$ and $xK_1 \geq x \bigcap_{x \in X'} x = G$, since X is $\mathcal{W}$-independent. But core(K_1) = core(x), so x and K_1 are not $\mathcal{C}$-independent, a contradiction. □

Remark. We will see that for $p \neq 2$ the assumptions of the last theorem are satisfied.

4.2. Simple groups and Cohomology. In this section we quote those results of [AS], [Gu] and [We2] we need in this paper and derive some corollaries.

THEOREM 4.2.1 (Guralnick). *Let G denote a non-abelian simple group, p a prime and $H < G$ such that $[G : H] = p^a$ for some $a \in \mathbb{N}$. Then $H \in M(G)$ and one of the following holds:*

1. $G = A_n$ *and* $H \cong A_{n-1}$ *with* $n = p^a$.
2. $G = PSL_n(q)$ *and H is the stabilizer of a line or hyperplane. Then* $p^a = (q^n - 1)/(q - 1)$.
3. $G = PSL_2(11)$ *and* $H \cong A_5$.
4. $G = M_{23}$ *and* $H \cong M_{22}$ *or* $G = M_{11}$ *and* $H \cong M_{10}$.
5. $G = PSU_4(2) \cong PSp_4(3)$ *and H is a parabolic subgroup,* $p^a = 27$.

Note that in item 2, for $n > 2$, and in 3 there are two conjugation classes of H which are fused in Aut(G). *Also H is a p-complement except if $G \cong A_n$ and $a > 1$ or $G \cong PSU_4(2)$.*

Proof. See [Gu]. □

Remark. The above theorem uses the classification of the finite simple groups.

COROLLARY 4.2.2. *Suppose N is a non-abelian minimal normal subgroup of G. If $U < G$ has p-power index in G and $NU = G$, then $U \in M^p(G)$ and $N \cap U$ is a minimal subgroup of p-power index in N.*

Furthermore $U = N_G(N \cap U)$ and no two supplements of N are $\mathcal{W}$-independent.

Proof. For $U \in M^p(G)$ and the fact that $U \cap N$ is minimal among all subgroups of p-power index in N see [We2], 4.3–4.5.

Note that $N_G(N \cap U) \geq U$ and $N \cap U$ is not normal in N. So $U = N_G(N \cap U)$, as U is maximal.

Suppose $XN = G$ and $X \in M^p(G)$. If $\{X, U\} \in \mathcal{I}_{\mathcal{W}}$, then $[N\colon N \cap X \cap U]$ is a power of p, this implies $N \cap X = N \cap U$ (by the first part of this lemma) and so $U = X$. □

LEMMA 4.2.3. *Suppose W is a faithful $\mathbb{F}_p\langle a\rangle$-module and $|\langle a\rangle| = p^n$. Then* $\dim W \geq p^{n-1} + 1$.

Proof. If $\dim W = w$, then the characteristic polynom of a on W is $(a-1)^w$. If $p^{n-1} \geq w$, we have $0 = (a-1)^w = (a-1)^{p^{n-1}} = a^{p^{n-1}} - 1$. So $a^{p^{n-1}}$ fixes every element of W, a contradiction. Thus $w \geq p^{n-1} + 1$. □

LEMMA 4.2.4. *Suppose S is a non-abelian simple group, $S \leq G \leq \mathrm{Aut}(S)$ and V is a faithful, irreducible $\mathbb{F}_p G$-module. Let p_S denote the maximal index of a subgroup of p-power index in S, $P(x)$ the p-part of the natural number x and $OS := |\mathrm{Out}(S)|$.*

Assume $|V| \leq p_S P(OS)$ and $p_S \neq 1$.

Then $S \cong PSL_2(7)$ and $p = 2$.

Proof. Since $p_S \neq 1$, we just have to check the groups in Guralnick's classification (see 4.2.1).

1. Case $S \cong PSL_a(q)$

We have a prime r and a, b such that $q = r^b$ and $p^n = (q^a - 1)/(q-1)$. Then $|\mathrm{Out}(S)|$ divides $(q-1)|\mathrm{Aut}(\mathbb{F}_q)|2 = 2b(r^b - 1)$.

(a) Case $p \neq 2$ or $a > 2$.

Then there is a cyclic subgroup (Singer cycle) of order p^n in S (see [We2], Korollar 5.3) and $P(2b(r^b-1)) \leq p^n$. So $p^{p^{n-1}+1} \leq |V| \leq p_S P(OS) \leq p^n p^n$ and $p^{n-1}+1 \leq 2n$. Hence $n = 1$ (since $p^n \geq 5$). If $n = 1$, then $P(2b(r^b-1)) = 1$ and therefore $p^{n-1} + 1 \leq n$, a contradiction.

(b) Case $p = 2 = a$.

Then $2^n = r^b + 1$ and $|\mathrm{Out}(S)|$ divides $b(2^n - 1)$. Furthermore there is a cyclic subgroup of order 2^{n-1} in S. So $2^{2^{n-2}+1} \leq |V| \leq p_S P(b(r^b-1)) = 2^n P(2b) \leq 2^{2n}$. Hence $2^{n-2} + 1 \leq 2n$, a contradiction for $n \geq 6$. If $n = 5$, then $r^b = 31$, so $P(b) = 1$ and $2^3 + 1 \leq 6$, a contradiction. If $n = 4$, then $r^b = 15$, a contradiction. The case $n = 3$ gives $S \cong PSL_2(7)$.

2. Case $S \cong A_{p^n}$.

Then $|\mathrm{Out}(S)| = 2$ (since $p^n \neq 6$).

(a) For $p \neq 2$ we have a cyclic subgroup of order p^n in S. So $p^{p^{n-1}+1} \leq |V| \leq p_S P(OS) = p^n$, a contradiction.

(b) Suppose $p = 2$. Then $n \geq 3$ and there is a cyclic subgroup of order 2^{n-1} and so $2^{2^{n-2}+1} \leq |V| \leq 2^{n+1}$. This is not possible for $n \geq 5$.

We leave the two cases $S \cong A_8$ and $S \cong A_{16}$ to the reader (see [ATLAS] or [GAP]).

3. The remaining four cases can be excluded by [ATLAS] or [GAP]. □

LEMMA 4.2.5. *Suppose N is a minimal normal p-subgroup of G and M/N is a minimal normal subgroup of G/N.*

Suppose M/N has exactly one M/N-conjugation class of p-complements and $C_M(N) = N$.

Then M has exactly one M-conjugation class of p-complements. For every p-complement H of M we have $N_G(H)M = G$. For every complement U of N in G there is a g_U such that $U^{g_U} \geq N_G(H)$.

Proof. The assumptions about M/N imply that M possesses exactly one conjugation class of p-complements (Schur-Zassenhaus). So H exits and $N_G(H)M = G$ (Frattini argument).

Suppose $e \neq n \in N \cap N_G(H)$ and $h \in H$. Then $[n, h] \in N \cap H = E$, hence $C_N(H) \neq E$. So the trivial $\mathbb{F}_pH$-module $\mathbb{I}_H$ is a submodule of $N|_H$ and (Nakayama-Reciprocity) an irreducible submodule of $N|_{M/N}$ (this is N regarded as an M/N-module) is a factor module of $\mathbb{I}_{HN/N} \uparrow^{M/N}$ (this is the trivial HN/N-module induced to M/N). Since $[M/N : HN/N]$ is a power of p the only irreducible factor module of $\mathbf{I}_{HN/N} \uparrow^{M/N}$ is the trivial M/N-module (see [We2], Lemma 3.1). So a submodule of $N|_M$ is the trivial module. Now Clifford theory shows that $C_M(N) = M$, a contradiction. Therefore $N_N(H) = E$.

By Guralnick (Theorem 4.2.1) $N_{M/N}(HN/N) = HN/N$, so $H = N_G(H) \cap M$.

Suppose U is a complement of N in G. As $(U \cap M)N = UN \cap M = M$ and $U \cap N = E$, we get $U \cong M/N$. So there is a g_U such that $U^{g_U} \geq H$. We may assume $g_U = e$ and have to prove that $U \geq N_G(H)$.

In doing so suppose $g \in N_G(H)$. Since $UN = G$ we can write $g = nu$ with $u \in U$ and $n \in N$. Then $[h, n] = ([h, u]^{-1}[h, nu])^{u^{-1}} \in U \cap N = E$. As above, we conclude $n = e \in E$ and hence $U \geq N_G(H)$. □

THEOREM 4.2.6 (Aschbacher, Scott). *Suppose N is a faithful irreducible $\mathbb{F}_pG$-module such that $H^1(G, N) \neq 0$.*

Then G has a unique minimal normal subgroup M.

Furthermore, let S denote a minimal normal subgroup of M. Then S is a non-abelian simple group. Fix m such that $M \cong S^m$ (S^m is a direct product of m copies of S). Then there exists a faithful S-module V with $H^1(S, V) \neq 0$ and $N|_M \cong \oplus V_i$ (here V_i is the S^m-module on which the i-th component of S^m acts as S on V and all other components act trivial).

Proof. See [AS], Theorem 3. □

COROLLARY 4.2.7. *Suppose N is a minimal normal p-subgroup of G, $U, L \in M^p(G)$ and $UL = UN = LN = G$. Assume N is a faithful G/N-module.*

Then $H^1(G/N, N) \neq 0$. Let M/N denote the unique minimal normal subgroup of G/N. Then $(M \cap U \cap L)N/N$ is a proper subgroup of p-power index in M/N.

Proof. Since U and L are not conjugate (see Lemma 2.2.7) we have $H^1(G/N, N) \neq 0$.

So the assertions about M follow from Theorem 4.2.6. Moreover, since $U \cap L$ is a subgroup of p-power index, we have either $M \cap ((U \cap L)N) = M$ or the conclusion of our lemma holds.

So suppose $M \leq (U \cap L)N$. Then $M \cap U \cap L$ is a complement of N in M (just compute the order of $N(M \cap U \cap L)$). Similarly, $U \cap M$ is a complement of N in M and $U \cap M = U \cap L \cap M = L \cap M$. But $N_G(U \cap M) \geq U$. So, since U was maximal and N the minimal normal subgroup of G, we conclude that $U = N_G(U \cap M) = N_G(L \cap M) = L$, a contradiction. □

4.3. Reductions.

LEMMA 4.3.1. *For L normal in G let $M^L := \{U \in M^p(G) \colon U \geq L\}$ and $M_L := \{U \in M^p(G) \colon UL = G\}$. So $M^p(G)$ is the disjoint union of M^L and M_L (, but in general this is not a direct product of simplicial complexes). Then $(M^L, \mathcal{I}_{\mathcal{W}}) \cong (M^p(G/L), \mathcal{I}_{\mathcal{W}})$.*

If we have $L \bigcap_{U \in \mathcal{U}} U = G$, for every $\mathcal{W}$-independent subset $\mathcal{U}$ of M_L, then $(M^p(G), \mathcal{I}_{\mathcal{W}})$ is the direct product of $(M^L, \mathcal{I}_{\mathcal{W}})$ and $(M_L, \mathcal{I}_{\mathcal{W}})$ (as simplicial complexes).

Proof. The natural epimorphism from G onto G/L gives a simplicial isomorphism, $(M^L, \mathcal{I}_{\mathcal{W}}) \cong (M^p(G/L), \mathcal{I}_{\mathcal{W}})$.

If $\mathcal{V} \in \mathcal{I}_{\mathcal{W}}(M^L)$, then $\bigcap_{V \in \mathcal{V}} V \geq L$. If $\mathcal{U} \in \mathcal{I}_{\mathcal{W}}(M_L)$ and $L \bigcap_{U \in \mathcal{U}} U = G$, then $\bigcap_{V \in \mathcal{V}} V \bigcap_{U \in \mathcal{U}} U = G$. So $\mathcal{V} \cup \mathcal{U} \in \mathcal{I}_{\mathcal{W}}$ (Lemma 2.2.7). □

THEOREM 4.3.2. *One of the following holds.*

1. *G is an elementary abelian p-group and $(M^p(G), \mathcal{I}_{\mathcal{W}}) = (M^p(G), \mathcal{I}_{\mathcal{C}})$ is a matroid without a non-trivial decomposition.*
2. *$\Phi^p(G) := \bigcap_{U \in M^p(G)} U > E$ and $(M^p(G), \mathcal{I}_{\mathcal{W}}) \cong (M^p(G/\Phi^p), \mathcal{I}_{\mathcal{W}})$.*
3. *G has a minimal normal non-abelian subgroup N, and $(M^p(G), \mathcal{I}_{\mathcal{W}}) \cong (M^p(G/N), \mathcal{I}_{\mathcal{W}}) \times (M_N, \mathcal{I}_{\mathcal{C}})$.*
4. *G is not an elementary abelian p-group, $\Phi^p(G) = E$ and every minimal normal subgroup is abelian.*

   Let M denote a normal subgroup of G, minimal under the condition that M is not an elementary abelian p-group. Let N denote a maximal G-normal *subgroup of M. Then:*

(a) *M/N is not a p-group.*

(b) *N has a complement in G. Every chief-factor below N is a complemented p-chief-factor on which M/N acts faithfully.*

Proof. 1. Trivial.

2. The natural epimorphism from G to G/Φ^p induces a bijection between $M^p(G)$ and $M^p(G/\Phi^p)$. This map is the desired isomorphism.

3. See Corollary 4.2.2 and Lemma 4.3.1.

4. Suppose $\Phi^p = E$ and G is not an elementary abelian p-group. Let M, N be as in the theorem.

If M/N (and so M) is a p-group, then $\Phi(M) \leq \Phi^p(G) = E$ and thus M is elementary abelian, a contradiction. Therefore M is not a p-group.

Since $\Phi^p = E$ every minimal normal subgroup of G is supplemented by some $U \in M^p(G)$.

N is an elementary abelian p-group (by construction of M).

As $\Phi^p(G) = E$ there is an $X \subseteq M^p(G)$ such that $\bigcap_{x \in X} x \cap N = E$. If we chose X minimal, then $N \cong \oplus_{x \in X} \mathrm{crown}(x)/\mathrm{core}(x)$ as $\mathbb{F}_pG$-modules (compare with Lemma 3.2.3). Moreover N is complemented (Lemma 3.2.2). Hence G is the semidirect product of G/M with the semisimple module N.

Suppose V is a minimal G-normal subgroup of N. Let K denote a complement of V in G. Then K and V normalize $K \cap C_G(V)$ and therefore $K \cap C_G(V)$ is normal in G. Furthermore, $C_G(V)/K \cap C_G(V)$ is a p-group. If $M \leq C_G(V)$, then $M \cap K$ is a proper G-normal subgroup of M which is not a p-group. Thus $M \not\leq C_G(V)$. □

LEMMA 4.3.3. *Let M, N as in Theorem 4.3.2.4 and $N/\bar{N}$ a chief-factor. Suppose no two complements of $N/\bar{N}$ satisfy $UL = G$.*

Let X denote the product of all minimal normal subgroups of N that are isomorphic to $N/\bar{N}$ as G-modules (so $X \neq E$).

Then $(M^p(G), \mathcal{I}_{\mathcal{W}})$ is the direct product of $(M^X, \mathcal{I}_{\mathcal{W}})$ and $(M_X, \mathcal{I}_{\mathcal{W}})$. Furthermore, $(M_X, \mathcal{I}_{\mathcal{W}}) = (M_X, \mathcal{I}_{\mathcal{C}})$ is a matroid.

Proof. In view of Lemmas 4.3.1 and 2.2.7 it is enough to show that $\mathcal{U} \in \mathcal{I}_{\mathcal{W}}(M_X)$ implies that there is a chief-series $\mathcal{H}$ through X such that $\mathcal{U}$ is $\mathcal{H}$-independent.

In doing so, fix an enumeration $\mathcal{U} = \{U_1, \ldots, U_l\}$. Define $H_1 := X$ and $H_{i+1} := H_i \cap U_i$. Let i_0 denote the largest i such that U_j complements H_j/H_{j+1} for all $j < i$. If $i_0 = l+1$ we are done. So suppose $i_0 \leq l$.

Then $H_{i_0} \leq U_{i_0} =: U$. Let $K_1 := \bigcap_{i<i_0} U_i$ and $K := K_1\mathrm{core}(U)$. Then $KU \geq K_1U = G$ and $K \in M_X$.

Note that $G/\bar{N}$ is the semidirect product of G/N and $N/\bar{N}$. Since $N/\bar{N} \cong \mathrm{crown}(U)/\mathrm{core}(U)$, we have $G/\bar{N} \cong G/\mathrm{core}(U)$. Now the preimages of $K/\mathrm{core}(K)$ and $U/\mathrm{core}(K)$ give a contradiction to our assumptions. (Compare: Theorem 4.1.3.)

□

($*$) Let M and N denote normal subgroups of G such that:
1. M/N is a chief-factor which is not a p-group.
2. $N \neq E$ is the direct product of complemented minimal normal p-subgroups.
3. If A/B is a chief-factor below N, then $C_M(A/B) = N$.
4. Every chief-factor N/X has two complements L, U such that $LU = G$.

COROLLARY 4.3.4. *Suppose $(M^p(G/X), \mathcal{I}_\mathcal{C})$ is a matroid for every non-trivial normal subgroup X, but ($*$) is not satisfied for any pair (M, N) of normal subgroups of G.*

Then $(M^p(G), \mathcal{I}_\mathcal{W})$ is a matroid.

If in addition $\mathcal{I}_\mathcal{W}(M^p(G/X)) = \mathcal{I}_\mathcal{C}(M^p(G/X))$ for all non-trivial normal subgroups X, then $\mathcal{I}_\mathcal{W}(M^p(G)) = \mathcal{I}_\mathcal{C}(M^p(G))$.

Proof. Theorem 4.3.2, Lemma 4.3.1, 4.3.3. □

4.4. Projective $\mathcal{W}$-Independence.

LEMMA 4.4.1. *Assume ($*$).*

Fix a chief-factor N/B. Then N/B is a faithful, irreducible $G/C_G(N/B)$ module with $H^1(G/C_G(N/B), N/B) \neq 0$.

Furthermore, let S denote a minimal normal subgroup of M/N. Then S is a non-abelian simple group and $M/N \cong S^m$ for some m. There exists a faithful S-module V such that $A/B|_{M/N} \cong \oplus V_i$ (here V_i is the S^m-module on which the i-th component of S^m acts as S acts on V and all other components act trivial). In addition $H^1(S, V) \neq 1$.

Proof. By assumption, there are two complements U, L of N/B such that $UL = G$.

Since $C_M(N/B) = N$, no chief-factor above M is isomorphic to N/B.

Therefore $\{U, L\}$ is not $\mathcal{C}$-independent, but $\operatorname{core}(U) = \operatorname{core}(L)$ (see Lemmas 3.2.4 and 3.3.1). This implies that U and L are two non-conjugate (see Lemma 2.2.7) complements of $N\operatorname{core}(U)/\operatorname{core}(U)$ in $G/\operatorname{core}(U)$.

Thus $H^1(G/C_G(N/B), N/B) \neq 0$, since $N\operatorname{core}(U) = C_G(N/B)$.

Now Theorem 4.2.6 completes the proof of our lemma. □

Let M, S, m, V be as in the last lemma. Then $|V|^m = |N|$, since $N|_M \cong \oplus_{i \leq m} V_i$ and

$$|N| = |G|/|U| = (|G|/|U|)|G|/(|N||L|) = |G|/(|N||U \cap L|) = [G\colon (U \cap L)N].$$

So G/N is a group that has a subgroup (namely $(U \cap L)N/N$) of index equal to the cardinality of a faithful $\mathbb{F}_pG/N$-module (namely N) such that $H^1(G/N, N) \neq 1$.

This gives strong restrictions on S, V and p.

LEMMA 4.4.2. *Let M, N, S, m, V, U, L and p be as above.*

Let p_S denote the maximal index of a subgroup of p-power index in S, $m!$ the order of the symmetric group $S(m)$ on m letters and $OS = |\mathrm{Out}(S)|$. Let $P(x)$ denote the p-part of x.

Then $|V|^m = |N| = [G: (N(U \cap L))] \le (p_S P(OS))^m P(m!)$ and $1 \neq p_S$.

In particular, $|V| \le p_S P(OS)$ since $P(m!) < p^m$.

Proof. $|V|^m = |N| = [G: (N(U \cap L))]$ was shown just above.

If $X \le G$ and Y is normal in G, then $[G : X] = [G : XY][Y : X \cap Y]$.

Applying this to G, $(U \cap L)N$ and M gives

$$|N| = [G: (U \cap L)N] = [G: M(U \cap L)][M: M \cap (N(U \cap L))].$$

Obviously, $[M: M \cap (N(U \cap L))] = [M/N: (M \cap U \cap L)N/N] \le p_S^m$.

Consider the map from G/M to $S(m)$ (i.e., the permutation of G/M on the direct summands of M/N). The kernel K of this map is the core of $N_{G/N}(SN/N)/(M/N)$ and is contained in an m-fold direct sum of Out(S). The image is contained in $S(m)$. So

$$[G: M(U \cap L)] = [G: K(U \cap L)][K: K \cap (M(U \cap L))] \le P(m!)P(OS)^m.$$

Putting these bounds together gives our bound on $|N|$.

Corollary 4.2.7 shows $p_S \neq 1$. □

COROLLARY 4.4.3. *Assume* $(*)$.

1. *$M/N \cong PSL_2(7)^m$ and $p = 2$.*
2. *M has exactly one conjugation class of p-complements. Let H denote any p-complement and $K := N_G(H)$. Then $KN \in M(G)$.*
3. *For $U \in M_M$ there is a g_U such that $U^{g_U} \ge K$.*
4. *For $X \subseteq M_M$ let $\bar{X} := \{U^{g_U}: U \in X\}$. Then X is $\mathcal{C}$-independent (resp. $\mathcal{W}$-independent) if and only if no two different conjugate subgroups are in X and $\bar{X}$ is C-independent (resp. $\mathcal{W}$-independent).*

Proof. 1. Lemma 4.2.4.

2. Lemma 4.2.5 and Corollary 4.2.2.

3. If $U \in M_N$, we find g_U by Lemma 4.2.5.

If $U \in M_M \setminus M_N$, then $M \cap U/N$ is a p-complement of M/N and so there is a g_U with $U = N_G(U \cap M) = N_G(H^{g_U}N) = K^{g_U}N$.

4. Theorem 3.1 and Lemma 2.2.7. □

So far we have proved Theorem 4.1 for odd primes; if G is a minimal counterexample to 4.1, then:

$(**)$ In addition to G, M, N as in $(*)$, define m, K, p as in Corollary 4.4.3.

Note that this implies $p = 2$ and $M/N \cong PSL_2(7)^m$.

4.5. The case $S \cong PSL_2(7)$.

LEMMA 4.5.1. *Assume (∗∗). Suppose N is a minimal normal subgroup of G and U, L are two non-conjugate complements of N. Then $UL = G$ and $|U| = |KN|$.*

Proof. By (∗∗) there are $g_U, g_L \in G$ such that $U^{g_U} \cap L^{g_L} \geq K$. As $UL = G$ if and only if $U^{g_U}L^{g_L} = G$, we may assume $g_U = g_L = e$.

Now $(U \cap L)N \geq KN$ and therefore $(U \cap L)N = KN$ (as $KN \in M(G)$ by Corollary 4.4.3 and $|(U \cap L)N| = |U \cap L||N| < |U||N| = |G|$).

But $|U \cap L| = |(U \cap L)N|/|N| = |KN|/|N| = |K|$ so $U \cap L = K$.

Let $\bar{U}, \bar{L}$ denote two non-conjugate complements of N such that $\bar{U}\bar{L} = G$ (such a pair exists by (∗)). Then $\bar{U}^{g_{\bar{U}}}\bar{L}^{g_{\bar{L}}} = G$ and we may assume $\bar{U}, \bar{L} \geq K$ (see (∗∗)). As above we have $\bar{U} \cap \bar{L} = K$.

Now $|UL| = |U||L|/|K| = |\bar{U}||\bar{L}|/|K| = |\bar{U}\bar{L}| = |G|$ (because $[G : U] = |N| = [G : \bar{U}]$). Thus $UL = G$.

Since $KN \cap L = (U \cap L)N \cap L = (U \cap L)(N \cap L) = U \cap L$ and $\{KN, L\}, \{U, L\} \in \mathcal{I}_{\mathcal{W}}$, we conclude $|KN| = |U|$. □

COROLLARY 4.5.2. *Assume (∗∗).*

1. *If $U \in M_M$, then $|U| = |KN|$.*
2. *If $\mathcal{U} \in \mathcal{I}_{\mathcal{W}}(M_M)$, then $[G : \bigcap_{U \in \mathcal{U}} U] = [G : KN]^{|\mathcal{U}|}$.*
3. *Suppose $|N| = [G : KN]^r$. If $\mathcal{U}$ is a maximal in $\mathcal{I}_{\mathcal{C}}(M_M)$, then $|\mathcal{U}| = r + 1$ and $\bigcap_{U \in \mathcal{U}} U^{g_U} = K$.*
4. *If $\mathcal{V} \in \mathcal{I}_{\mathcal{W}}(M_M)$, then $|\mathcal{V}| \leq r + 1$.*

Proof. 1. If $U \in M_N$, then U complements $N/(N \cap \mathrm{core}(U))$ and so $|U| = |KN|$ (see Lemma 4.5.1). If $U \in M_M \setminus M_N$, then $U^{g_U} = U^{g_U}N \geq KN \in M(G)$ and so $|U| = |KN|$.

2. If $\mathcal{U} \in \mathcal{I}_{\mathcal{W}}(M_M)$, then $[G\colon \bigcap_{U \in \mathcal{U}} U] = \prod_{U \in \mathcal{U}}[G : U] = [G : KN]^{|\mathcal{U}|}$.

3. Note that N is a direct product of some chief-factors below N and all these chief-factors have order $[G : KN]$ (see above). Since KN is a supplement of the chief-factor M/N, we conclude, $|\mathcal{U}| = r + 1$.

We may suppose $g_U = e$. Thus $\bigcap_{U \in \mathcal{U}} U \geq K$. Equality follows from: $[G : K] = [G : KN]|N| = [G : KN]^{r+1} = [G\colon \bigcap_{U \in \mathcal{U}} U]$.

4. Again we may assume $\bigcap_{V \in \mathcal{V}} V \geq K$.

So $[G : KN]^{|\mathcal{V}|} = [G\colon \bigcap_{V \in \mathcal{V}} V] \leq [G : K] = [G : KN]^{r+1}$. Hence $|\mathcal{V}| \leq r+1$. □

LEMMA 4.5.3. *Assume (∗∗).*

Then $X \subseteq M_M$ is a maximal $\mathcal{W}$-independent subset of M_M if and only if $X = X' \cup \{y\}$ for some maximal $X' \in \mathcal{I}_{\mathcal{C}}(M_N)$ and some $y \in M_M$ with $y \not\geq \bigcap_{x \in X'} x^g$ for all $g \in G$.

If $X = X' \cup \{y\} \in \mathcal{I}_{\mathcal{W}}(M_M)$ is such a decomposition, then there exists y' such that $Y := X' \cup \{y'\}$ is $\mathcal{C}$-independent and $\bigcap_{x \in X} x = \bigcap_{y \in Y} y$.

Proof. Let X denote a maximal set in $\mathcal{I}_{\mathcal{W}}(M_M)$. If X is $\mathcal{C}$-independent set $X' := X \cap M_N$ and $\{y\} := X \setminus X'$. This proves that case.

So suppose X is not $\mathcal{C}$-independent and X' is a maximal $\mathcal{C}$-independent subset of $X \cap M_N$. We may suppose $U \geq K$ for all $U \in X$ (for K see (**) and Corollary 4.4.3).

If $\bigcap_{x \in X} \mathrm{core}(x) \cap N \neq E$, then some $U \in M_M$ supplements some chief-factor below $\bigcap_{x \in X} \mathrm{core}(x) \cap N \neq E$, contradicting the maximality of X (see Lemma 2.2.7, 4.3.1).

Hence we may assume $\bigcap_{x \in X} \mathrm{core}(x) \cap N = E$. If $\bigcap_{x \in X'} \mathrm{core}(x) \cap N \neq E$, then there is a $U \in X$ that supplements some chief-factor below $\bigcap_{x \in X} \mathrm{core}(x) \cap N \neq E$ contradicting the maximality of X'. So $Y' := X' \cup \{KN\}$ is maximal in $\mathcal{I}_{\mathcal{C}}(M_M)$. Now (Corollary 4.5.2) $X \setminus X' = \{y\}$ for some y and (with $y' = KN$): $\bigcap_{x \in X} x = K = \bigcap_{x \in X'} x \cap y'$.

Note that y does not contain a conjugate of $\bigcap_{x \in X'} x'$ by Lemma 2.2.7.

Suppose now X' is a maximal $\mathcal{C}$-independent subset of M_N and $y \in M_M$ is such that $y^g \not\geq \bigcap_{x \in X'} x$ for all $g \in G$.

If $y \geq N$, then $\{y\} \cup X' \in \mathcal{I}_{\mathcal{C}} \subseteq \mathcal{I}_{\mathcal{W}}$. So suppose $yN = G$.

Define $K_1 := \bigcap_{x \in X'} x$ (this is a complement of N in G) and $K_2 := K_1 \mathrm{core}(y)$. Now K_2 is not conjugate to y by assumption and so $K_1 y = K_2 y = G$ (see Lemma 4.5.1). Hence $X' \cup \{y\}$ is $\mathcal{W}$-independent. The maximality follows from the first part of our lemma.

Therefore, for every $\mathcal{W}$-independent subset $\mathcal{U}$ of M_M we have $M \bigcap_{U \in \mathcal{U}} U = G$ (see Lemma 2.2.7). Now Lemma 4.3.1 shows that $(M^p(G), \mathcal{I}_{\mathcal{W}})$ is the direct product of $(M^M, \mathcal{I}_{\mathcal{W}})$ and $(M_M, \mathcal{I}_{\mathcal{W}})$. □

LEMMA 4.5.4. *$(M_M, \mathcal{I}_{\mathcal{W}})$ is a matroid; $(M^p(G), \mathcal{I}_{\mathcal{W}})$ is the direct product of $(M^M, \mathcal{I}_{\mathcal{W}})$ and $(M_M, \mathcal{I}_{\mathcal{W}})$.*

Proof. Let $\mathcal{A}, \mathcal{B} \in \mathcal{I}_{\mathcal{W}}(M_M)$ and $|\mathcal{A}| < |\mathcal{B}|$.

We have to find a $B \in \mathcal{B} \setminus \mathcal{A}$ such that $\mathcal{A} \cup \{B\}$ is $\mathcal{W}$-independent.

Let $C_{\mathcal{B}} := \bigcap_{B \in \mathcal{B}} \mathrm{core}(B)$ and $C_{\mathcal{A}} := \bigcap_{A \in \mathcal{A}} \mathrm{core}(A)$. If $C_{\mathcal{A}} \cap C_{\mathcal{B}} \neq E$ an induction argument provides such a B.

If $C_{\mathcal{B}} \cap C_{\mathcal{A}} < C_{\mathcal{A}}$, then every $B \in \mathcal{B}$ with $\mathrm{core}(B) \cap C_{\mathcal{A}} < C_{\mathcal{A}}$ satisfies $\mathcal{A} \cup \{B\} \in \mathcal{I}_{\mathcal{W}}$ and $B \in \mathcal{B} \setminus \mathcal{A}$.

So we may suppose $E = C_{\mathcal{A}}$. This implies that $\mathcal{A}$ is a maximal $\mathcal{C}$-independent subset of M_N.

Suppose that for all $B \in \mathcal{B}$ there is a $g_B \in G$ such that $B^{g_B} \geq \bigcap_{A \in \mathcal{A}} A$. Then we find a $g \in G$ such that $\bigcap_{B \in \mathcal{B}} B^g = \bigcap_{B \in \mathcal{B}} B^{g_B} \geq \bigcap_{A \in \mathcal{A}} A$, which is a contradiction to $|\mathcal{B}| > |\mathcal{A}|$ (as $[G\colon \bigcap_{B \in \mathcal{B}} B] = [G : KN]^{|\mathcal{B}|}$).

So some $B \in \mathcal{B}$ does not contain any conjugate of $\bigcap_{A \in \mathcal{A}} A$ and so this B is not in $\mathcal{A}$. Now $\mathcal{A} \cup \{B\} \in \mathcal{I}_{\mathcal{W}}$ (Lemma 4.5.3). □

We can now prove Theorem 4.1: Lemma 4.1.1, Corollary 4.3.4, 4.4.3 and Lemma 4.5.4 proves the first part.

Now Lemma 4.5.3 (and Corollary 4.3.4) proves $\mathcal{I}_{\mathcal{W}}(X)^{\cap} = \mathcal{I}_{\mathcal{C}}(X)^{\cap}$ for every factor X of $\mathcal{I}_{\mathcal{W}}(M^p(G))$ and so $\mathcal{I}_{\mathcal{W}}(M^p(G))^{\cap} = \mathcal{I}_{\mathcal{C}}(M^p(G))^{\cap}$.

It was shown in [We2] Satz 4.8 that $\mathcal{I}_{\mathcal{H}}(M^p(G))^{\cap} = S_c^p$. Since μ does not depend on $\mathcal{H}$ and by definition of $\mathcal{C}$ we have, $\mathcal{I}_{\mathcal{C}}(M^p(G))^{\cap} = S_c^p$. □

EXAMPLE 4.5.5. We construct a group G with $\mathcal{I}_{\mathcal{C}}(M^2(G)) \neq \mathcal{I}_{\mathcal{W}}(M^2(G))$.

Let $G_1 := PSL_2(7) \cong SL_3(2)$ and $p = 2$.

If V is an irreducible $\mathbb{F}_2G_1$ module, then $H^1(G_1, V) \neq 0$ if and only if $\dim V = 3$ and -up to isomorphism- exactly two such modules V_1, V_2 exist. We have $|H^1(G_1, V_i)| = 2$.

Let G denote the semidirect product of G_1 with $V_1 \oplus V_2$. Then G satisfies the assumptions of Lemma 4.5.3 (with $G = M$). Two subgroups are not $\mathcal{W}$-independent if and only if they are conjugate. So $\mathbf{proj}_{\mathcal{W}}(M^2(G))$ is the set of the five conjugation classes in $M^2(G)$. Let K_0 denote the conjugation class of supplements of $G/V_1 \oplus V_2$ and K_i^j for $i, j \in \{1, 2\}$ the two conjugation classes of complements of V_i in G.

So $\mathbf{proj}_{\mathcal{W}}(M^2(G)) = \{K_0, K_i^j\colon i, j \in \{1, 2\}\}$.

X is maximal in $\mathbf{proj}_{\mathcal{W}}(\mathcal{I}_{\mathcal{W}}(M^2(G))$ if and only if

$$X \in \{\{K_0, K_1^j, K_2^{j'}\}, \{K_i^1, K_i^2, K_j^{j'}\}\colon i, j, j' \in \{1, 2\} \text{ and } i \neq j\}.$$

5. Applications of $\mathcal{W}$-independence

1. Recall the probability theoretic independence definition: If (X, B, m) is a probability space (i.e., X is a set, B is the set of measurable subsets of X and m is a measure such that $m(X) = 1$), we call a subset Y of B independent, if for all finite subsets Z of Y, we have $\prod_{z \in Z} m(z) = m(\bigcap_{z \in Z} z)$.

The probability space we are interested in is the group G with the Haar measure i.e. $m(U) = |U|/|G|$ for all subsets U of G. As $[G : U] = |G|/|U|$, Lemma 2.2.7 shows that $\mathcal{W}$-independence coincides with probability independence restricted to the set of subgroups.

2. A (finite) set $\mathcal{L}$ of field extensions of K is linear disjoint (by definition) if for every $\mathcal{U} \subseteq \mathcal{L}$ the ring $\otimes_{L \in \mathcal{L}} L$ is a field.

If G is represented as a separable Galois group, then a set of subgroups is $\mathcal{W}$-independent if and only if the corresponding fixed fields are linearly disjoint (see [FJ] Lemma 16.11).

3. A set $\mathcal{F}$ of subgroups of G is a factorisation of G if and only if $AB = BA$ for all $A, B \in \mathcal{F}$ and $G = \prod_{A \in \mathcal{F}} A$.

Recall that two subgroups A, B commute (i.e., $AB = BA$) if and only if AB is a subgroup of G.

THEOREM 5.1. *(a) For* $\mathcal{U} \in \mathcal{I}_{\mathcal{W}}$ *and* $U \in \mathcal{U}$ *define* $\bar{U} := \bigcap_{U \neq X \in \mathcal{U}} X$. *Then* $\bar{\mathcal{U}} := \{\bar{U}\colon U \in \mathcal{U}\}$ *is a factorisation.*

(b) Let $\mathcal{F}$ *denote a factorisation. For* $F \in \mathcal{F}$ *let* $\tilde{F} := \prod_{F \neq U \in \mathcal{F}} U$. *Then* $\tilde{\mathcal{F}} := \{\tilde{F}\colon F \in \mathcal{F}\} \in \mathcal{I}_{\mathcal{W}}$.

Proof. (a) If $U_1, U_2 \in \mathcal{U}$, then (with $U_{1,2} := \bigcap_{U_1,U_2 \neq U \in \mathcal{U}} U$): $\bar{U}_1\bar{U}_2 = (U_{1,2} \cap U_1)(U_{1,2} \cap U_2) = U_{1,2} \cap ((U_{1,2} \cap U_1)U_2) = U_{1,2} \cap \bar{U}_2 U_2 = U_{1,2} = \bar{U}_2\bar{U}_1$ and $\prod_{U \in \mathcal{U}} \bar{U} = U_{1,2} \prod_{U_1,U_2 \neq U \in \mathcal{U}} \bar{U}$. Let $\mathcal{V} := \mathcal{U} \setminus \{U_1, U_2\} \cup \{U_1 \cap U_2\}$. Then $\mathcal{V} \in \mathcal{I}_{\mathcal{W}}$ and $|\mathcal{V}| < |\mathcal{U}|$. Induction gives: $G = \prod_{V \in \mathcal{V}} \bar{V} = U_{1,2} \prod_{U_1, U_2 \neq U \in \mathcal{U}} \bar{U} = \prod_{U \in \mathcal{U}} \bar{U} = G$.

(b) If $F \in \mathcal{F}$, then $\tilde{F} \leq G$. If $F \neq U \in \mathcal{F}$, then $F \leq \tilde{U}$ and thus $\tilde{F} \bigcap_{\tilde{F} \neq \tilde{U}, U \in \mathcal{F}} \tilde{U} \geq \tilde{F}F = G$. □

4. Suppose X is a set with a partial order $\leq_X$ such that G acts in an order-preserving fashion on X. The orbit poset X^G is the set of all orbits with the partial order defined by $\{x^g\colon g \in G\} \leq_{X^G} \{y^g\colon g \in G\}$ if and only if there is a $g \in G$ such that $x \leq_X y^g$.

Suppose there are $a, b \in X$ such that $\{x \in X\colon x \leq a, x \leq b\}$ possesses a unique maximal element $a \wedge b$. This does not imply that there is a unique maximal element $a^G \wedge b^G \in \{x^G \in X^G\colon x^G \leq a^G, x^G \leq b^G\}$. However, if $C_G(a)C_G(b) = G$, then $(a \wedge b)^G$ is the unique maximal element in $\{x^G \in X^G\colon x^G \leq a^G, x^G \leq b^G\}$ (as $\{a^{g_1} \times b^{g_2}\colon g_i \in G\} = \{a^g\colon g \in G\} \times \{b^g\colon g \in G\}$ by Lemma 2.2.7).

The chain complex $C(X)$ is the set of all linearly ordered subsets of X. This is a partially ordered set (inclusion). Now $C(X)^G = C(X^G)$ if and only if we have $[G\colon \bigcap_{y \in Y} C_G(y)] = \prod_{y \in Y}[G/C_G(y)]$, for every $Y \in C(X)$.

REFERENCES

[Ai] M. Aigner, *Combinatorial theory*, Springer-Verlag, New York, 1979.

[AS] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), 44–80.

[ATLAS] J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *Atlas of finite groups*, Oxford University Press, Oxford, 1985.

[Ba] R. Baer, *Classes of finite groups and their properties*, Illinois J. **1** (1957), 115–187.

[DH] K. Doerk and T. Hawkes, *Finite soluble groups*, de Gruyter, New York, 1992.

[FJ] M. Fried and M. Jarden, *Field arithmetic*, Springer-Verlag, New York, 1986.

[Ga] W. Gaschütz, *Praefrattinigruppen*, Arch. Math. **13** (1962), 418–426.

[GAP] Martin Schönert et al, *GAP – Groups, algorithms, and programming*, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, third edition, 1993.

[Gu] R. M. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra **81** (1983), 304–311.

[We1] M. Weidner, *Praefrattinigruppen und Matroide*, Results in Mathematics **20** (1991), 577–583.

[We2] ———, *Galoisverbindungen zwischen Untergruppenverbänden und Modulverbänden*, Results in Mathematics **21** (1992), 422–443.

[Wi] H. Wielandt, *Topics in the theory of composite groups*, Lecture Notes, Madison, 1967.
[WW] M. Weidner and V. Welker, *The combinatorics and the homology of the poset of subgroups of p-power index*, J. Pure Appl. Algebra **90** (1993), 253–274.

UNIVERSITÄT FREIBURG
FREIBURG, GERMANY