CHAPTER III

FRAENKEL - MOSTOWSKI - SPECKER MODELS

This chapter is devoted to the study of the socalled "Permutation Models". They provide a method for obtaining independence results. It was for the purpose of obtaining the relative consistency of $\neg$ (AC) and negations of some weakened forms of (AC) that A.A.Fraenkel first introduced the notion of a permutation model:

[20] A.FRAENKEL: Der Begriff "definit" und die Unabhängigkeit des Auswahlaxioms; Sitzungsberichte d. Preussischen Akad. Wiss.,Phys.Math.Klasse,vol.21(1922)p.253-257.

[21] A.FRAENKEL: Ueber eine abgeschwächte Fassung des Auswahlaxioms; J.S.L. 2(1937)p.1-27. [Abstracts: C.R.Acad.Sci.Paris vol. 192(1931)p.1072, and: Jahresberichte der DMV 41(1931) part 2, p.88].

At that time (1922) the distinction between Mathematics and Metamathematics was not yet clear enough and Fraenkel's proof fails in so far as questions concerning the absoluteness of certain notions are not treated. This failing has been observed and corrected by A.Mostowski, partly in collaboration with A.Lindenbaum:

[54] A.LINDENBAUM - A.MOSTOWSKI: Ueber die Unabhängigkeit des Auswahlaxioms und einiger seiner Folgerungen; C.R.Soc.Sci. Lettr.Varsovie, ClasseIII, vol. 31(1938)p.27-32.

[64] A.MOSTOWSKI: Ueber die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip; Fund.Math.32(1939)p.201-252.

Fraenkel has acknowledged the corrections and refinements obtained by Mostowski (see Fraenkel's review of [54] in the J.S.L.4(1939)p. 30-31). The major deficiency of the Fraenkel-Mostowski method is that it does not apply to "ordinary" set theories, id est, to set theories in which all the elements are sets and in which the axiom of foundations holds. The Fraenkel-Mostowski method is applied to set theories which admit the existence of "Urelements", id est objects which are not sets (have no elements and are distinct from the empty set $\emptyset$). These set theories are obtained from "ordinary" set theories (e.g. ZF) what essentially amounts to a weakening of the extensionality and dropping the axiom of foundation. Such a set theory, if obtained from ZF, will be called ZFU (the "U" indicating: with urelements). The FM-method has been ameliorated by E.P.Specker. His method, the socalled FMS-method (Fraenkel-Mostowski-Specker method), applies to set theories which permit the existence of unfounded sets, id est, they permit the existence of sequences of the type

$$\ldots\ldots \varepsilon\ x_n\ \varepsilon \ldots\ldots \varepsilon\ x_3\ \varepsilon\ x_2\ \varepsilon\ x_1 \qquad (n \in \omega)$$

or other similar phenomena such as $x = \{x\}$:

[82] E.SPECKER: Zur Axiomatik der Mengenlehre (Fundierungs- und Auswahlaxiom); Zeitschr.f.math.Logik und Grundlagen d. Math.vol.3(1957)p.173-210.

The set theories to which the FMS-method applies are obtained e.g. from ZF by weakening the axiom of foundation only. For a discussion of these methods we refer our reader to the book "Foundations of Set Theory" by A.Fraenkel - Y.Bar-Hillel (Amsterdam 1958)p.49-54, and to

[49] A.LÉVY: The Fraenkel-Mostowski Method for Independence Proofs in Set Theory; in: Symposium on the Theory of Models (Amsterdam 1965)p.221-228.

In the sequel we present Specker's method. We start with a proof that the existence of "reflexive" sets $x = \{x\}$ is relative consistent.

A) THE INDEPENDENCE OF THE AXIOM OF FOUNDATION

The notion of a well-founded set (ensemble ordinaire) was first considered by D.Mirimanoff (L'Ens.Math.19(1917)p.37-52,p.209-217, and vol.21(1920)p.29-52). A.Fraenkel (Math.Ann.86(1922)p.230-237) has added to the axioms of Zermelo an axiom of restriction (Axiom der Beschränktheit) asserting that every set is well-founded but the formulation was unfortunately not within the ZF-formalism (Frankel formulated it in a way similar to Hilbert's Vollständigkeitsaxiom of the "Grundlagen der Geometrie", 1899, see also Fraenkels paper in the Journal f.Math.141(1911) p.76).
It was Johann von Neumann (1925) who replaced Fraenkel's "axiom" by the axiom: $x \neq \emptyset \rightarrow \bigvee_y (y \in x \wedge x \cap y = \emptyset)$, (axiom(VII) in our list of ZF-axioms). J.v.Neumann's axiom excludes the existence of "extraordinaire" sets as it was the aim of Fraenkel's axiom, and is formulated within the ZF-formalism . Later Zermelo independently introduced this axiom and introduced the name "Axiom der Fundierung" for it (Zermelo, Fund.Math.16(1930) see p.31). The consistency of

the axiom of fundierung (VII) with ZF^0 was proved by J.v.Neumann. The consistency of $\neg$ (VII) with ZF^0 was first proved (independently, using different methods) by P.Bernays [J.S.L. 19(1954) see p.83-84 - this result was announced by Bernays already in 1941(J.S.L. 6, see p.10] and by E.P.Specker in his Habilitationsschrift, Zürich 1951, see [82]. The method for obtaining the indepence of the Fundierungsaxiom (VII) has been modified and simplified in the last 14 years by many authors [e.g. L.Rieger: Czechoslovak Math.J.7(1957)p.323-357; P.Hájek: Zeitschr.math.Logik u.Gr.Math.11(1965)p.103-115; M.Boffa: Zeitschr.math.Logik u.Gr.Math.14(1968)p.329-334]. A number of nice independence results is contained in:

[4] M.BOFFA: Les ensembles extraordinaires; Bull.Soc.Math.Belgique, vol.20(1968)p.3-15.

We shall present Bernays' independence proof but with the modifications due to L.Rieger and M.Boffa.

Permutations of the universe. Let $\Phi(x,y)$ be a ZF-formula having no free variables except x and y. Suppose Φ satisfies the following conditions:

(P.1) $ZF \vdash \bigwedge_x \bigwedge_y \bigwedge_z [\Phi(x,y) \wedge \Phi(x,z) \rightarrow y = z]$

(P.2) $ZF \vdash \bigwedge_x \bigwedge_y \bigwedge_z [\Phi(x,y) \wedge \Phi(z,y) \rightarrow x = z]$

(P.3) $ZF \vdash \bigwedge_x \bigvee_y \Phi(x,y) \wedge \bigwedge_y \bigvee_x \Phi(x,y)$.

Then Φ is said to define a permutation of the universe V. In this case define the class-term $F = \{\langle x,y\rangle ; \Phi(x,y)\}$ and $\langle x,y\rangle \in F \leftrightarrow y = F(x)$. Define a binary predicate $\in_F$ by

$$x \in_F y \underset{\text{Def.}}{\leftrightarrow} F(x) \varepsilon y \leftrightarrow \bigvee_z [\Phi(x,z) \wedge z \varepsilon y].$$

For a ZF-formula Ψ let Rep(F,Ψ) be the formula obtained from Ψ by replacing the symbol ε by $\in_F$ at all places of occurrence.

Theorem 1. Suppose $F = \{\langle x,y\rangle ; \Phi(x,y)\}$ defines a permutation of the universe, then Rep$(F,-)$ is a syntactic model of ZF^0 in ZF, id est $ZF \vdash \text{Rep}(F,\Psi)$ for every axiom Ψ of ZF^0.

Proof: Ad(0): The real empty set $\emptyset = F(a)$ satisfies the requirements of the relativized axiom of Null-set. Ad(I): suppose that $z \in_F x \leftrightarrow z \in_F y$ for all z. We prove $x \subseteq y$: Take $a \varepsilon x$. By (P.3) $a = F(b)$ for some b. Hence $F(b) \varepsilon x$, i.e. $b \in_F x$. The hypothesis yields $b \in_F y$, hence $a = F(b) \varepsilon y$. The part $y \subseteq x$ is proved analogously. By the axiom of extensionality of ZF we get $x = y$ as desired.

Ad(II): Let x and y be given. Put $z = \{F(x),F(y)\}$. Then $u \in_F z \leftrightarrow F(u) \varepsilon z$. Hence either $F(u) = F(x)$ or $F(u) = F(y)$. But the latter holds by (P.2) iff either $u = x$ or $u = y$. Ad(III): Let x be given and put $y = \{F(z); \bigvee_u (F(z) \varepsilon u \wedge F(u) \varepsilon x)\}$; then $z \in_F y \leftrightarrow \bigvee_u (z \in_F u \wedge u \in_F x)$ as required. The set y exists by virtue of the axioms of union and replacement of ZF. Ad(IV): Define (in ZF) a function f with domain ω by: $f(0) = \emptyset$, $f(1) = \{F(f(0))\}$, $f(n+1) = f(n) \cup \{F(f(n))\}$. Finally, define $x = \{F(f(i)); i \varepsilon \omega\}$. We have that $z \in_F x \leftrightarrow z = f(i)$ for some i and $f(i) \subset_F f(i+1) = f(i) \cup_F \{f(i)\}_F$, where $\subset_F$ expresses proper F-inclusion i.e. "Inclusion" with respect to $\in_F$). Hence x satisfies the requirements of the relativized axiom of infinity.
Ad(V): For a set x the power-set in the sense of the model is the set $y = \{F(t); t \subseteq x\}$. In fact: $z \in_F y \leftrightarrow z \subseteq x$ (by (P.2)), therefore: $u \in_F z \in_F y \rightarrow F(u) \varepsilon z \wedge z \subseteq x$. Hence $F(u) \varepsilon x$, i.e. $u \in_F x$. Ad(VI): Let $\Gamma(x,y)$ be a ZF-formula with precisely two free variables x and y and let $\Psi(x,y)$ be $\mathrm{Rep}(F,\Gamma(x,y))$. Suppose that for every x there is precisely one y such that $\Psi(x,y)$. Let a be any set. Define $a^* = \{F^{-1}(x); x \varepsilon a\}$. By the axiom of replacement (of ZF) corresponding to Ψ and a^* there is a set b^* such that

$$\bigwedge_y [y \varepsilon b^* \leftrightarrow \bigvee_u (u \varepsilon a^* \wedge \Psi(u,y))]$$

Define $b = \{F(y); y \varepsilon b^*\}$, then b satisfies the relativized replacement axiom corresponding to Ψ and a. Thus the theorem is proved.

Theorem 2: Suppose $F = \{\langle x,y \rangle ; \Phi(x,y)\}$ defines a permutation of the universe V. If $\langle V,\varepsilon \rangle$ satisfies the axiom of choice, then $\langle V,\in_F \rangle$ satisfies the axiom of choice too, id est: $ZF + (AC) \vdash \mathrm{Rep}(F, (AC))$.

Proof: Consider a set s such that s is "not empty" with respect to $\in_F$ and such that the F-elements of s are not F-empty and pairwise F-disjoint (the suffix "F" in front of a notion N indicates that the corresponding "notion in the sense of the model" is meant, id est: Rep(F,N)). Define

$$a^* = \{\{x; F(x) \varepsilon y\}; F(y) \varepsilon a\}$$

a^* is a set of non-empty, pairwise disjoint sets (with respect to ε). By (AC) there is a set b^* such that: $b^* \cap y$ is a singleton for each $y \varepsilon a^*$. Now $b = \{F(x); x \varepsilon b^*\}$ is a F-choice set for a, i.e. satisfies the condition:

$$\bigwedge_y [y \in_F a \to \overset{1}{\bigvee}_z (z \in_F b \wedge z \in_F y)].$$

This proves theorem 2.

<u>Definition</u>. A set x is called reflexiv iff $x = \{x\}$, id est iff the condition $\bigwedge_y (y \varepsilon x \leftrightarrow y = x)$ holds. The existence of reflexive sets contradicts the axiom of Fundierung.

<u>Theorem 3</u>. If ZF^0 is consistent, then $ZF^0 + \overset{1}{\bigvee}_x (x = \{x\})$ is also consistent.

<u>Proof</u>. Let $\Phi(x,y)$ be the formula $(x = 0 \wedge y = 1) \vee (x = 1 \wedge y = 0) \vee (x \neq 0 \wedge x \neq 1 \wedge x = y)$. Hence Φ defines a permutation of the universe such that only the ordinals 0 and 1 are interchanged. Let F be the one-to-one function $\{\langle x,y\rangle ; \Phi(x,y)\}$. Then $F(1) = 0 \in 1 = F(0)$, hence $1 \in_F 1$ and $1 = \{1\}_F$. Hence Rep(F,-) is a syntactic model of $ZF^0 + \overset{1}{\bigvee}_x x = \{x\}$ in ZF. The relative consistency follows from a theorem in chapt.I, section D. page 9, q.e.d.

<u>Corollary</u>: If ZF is consistent, then ZF^0 + "negation of the axiom of foundation" is consistent and ZF^0 + (AC) + "negation of the axiom of foundation" is consistent too.

This follows from theorems 2 and 3 and Gödel's consistency result. Hence the axiom of foundation is independent from ZF^0 + (AC).

Our next question is whether the axiom of foundation can be violated in such a form where there exists a countable set of reflexive sets or where there exists a proper class of reflexive sets which is in one-to-one correspondence with the class of all ordinals Both questions have been answered in the positive way by E.P.Specker (see also M.Boffa, Zeitschr.math.Logik u.Gr.d.Math. <u>14</u>(1968)p.329-334 and [4]).

<u>Theorem 4</u>: If ZF is consistent, then ZF^0 + "there exists a set R of reflexive sets such that R is equipotent with ω" is consistent too.

<u>Proof</u>: Consider the following permutation F of the universe: $F(x) = \{x\}$ iff $x \varepsilon \omega^*$, $F(x) = y$ iff $x = \{y\}$ for $y \varepsilon \omega^*$ and $F(x) = x$ in all other cases; here ω^* is difined to be $\omega - \{1\} = \{0,2,3,4,..\}$. For $x \varepsilon \omega^*$, $\{x\}$ is never in ω^* and F is well-defined. In particular we have: $F(0) = 1$, $F(1) = 0$, $F(2) = \{2\}$, $F(\{2\}) = 2$, etc. Hence $1 \in_F 1$ (since $F(1) = 0 \varepsilon 1$), id est: $\{0\} \in_F \{0\}$. Further $\{2\} \in_F \{2\}$, $\{3\} \in_F \{3\}$, etc. and obviously $F(x) \varepsilon \omega^* \to x = \{F(x)\} = \{x\}_F$.

We shall show that there is a F-correspondence between the F-set of reflexive sets $\mathbf{n} = \{n\}_F$ for $n \geq 1$ and ω.

The unordered pair in the model-sense of x and y is $\{F(x), F(y)\}$. The ordered pair in the sense of the model is hence

$\langle x,y \rangle_F = \{F(\{F(x)\}), F(\{F(x), F(y)\})\}$

The natural numbers in the sense of the model are the sets $f(0) = \emptyset$, $f(n+1) = f(n) \cup \{F(f(n))\}$ (see the proof of th.1). The function

$g = \{\langle f(n). \{n+2\}\rangle_F; n \in \omega\}_F = \{F(\langle f(n), \{n+2\}\rangle_F; n \in \omega\}$

is a function in the F-sense between $\omega_F = \{f(n); n \in \omega\}_F = \{F(f(n)); n \in \omega\}$, the F-set of F-natural numbers, and some F-reflexive sets $\{n+2\} = \{F(\{n+2\})\}$ for $n \in \omega$.

Corollary: If ZF is consistent, then ZF^0 + "there exists a proper class $\mathbf{R}$ of reflexive sets such that there is a one-to-one correspondence between the class of all ordinals and R" is consistent too.

Proof. Consider the following permutation of the universe: $F(x) = \{x\}$ iff $x \in On^*$, $F(x) = y$ iff $x = \{y\}$ for $y \in On^*$ and $F(x) = x$ otherwise. Here On is the class of all ordinal-numbers and $On^* = On - \{1\}$. Now proceed as in the proof of th.4.

Remark. By theorem 2 it is possible to add (AC) to ZF^0 in th.4 and its corollary above. Further, in the model of theorem 3 the (GCH) holds. Hence the axiom of foundation is indepentent from ZF^0 + (AC) + (GCH). This cannot be strengthened by adding V = L, since obviously the axiom of foundation follows from V = L. For further consistency results like those proved in theorems 3 and 4 and its corollary consult the papers of M.Boffa (those already cited and Boffa's papers in the C.R.Acad.Sc.Paris vol.264(1967)p.221-222,vol.265(1967) p.205-206, vol.266(1968)p.545-546, vol.268(1969)p.205). In particular Boffa's second C.R.-paper contains the following fine result:

Theorem (M.Boffa): Let $\langle s,< \rangle$ be any partially ordered set. If ZF is consistent, then so is ZF^0 + (AC) + "there is a transitive set t such that $\langle s,< \rangle$ and $\langle t,\in \rangle$ are isomorphic".

In particular $\langle s,< \rangle$ can be taken to be any linearly ordered set (e.g. a dense totally ordered set).

It is known that in ZF + (AC) + "There are strongly inaccessible cardinal numbers "the class of Grothendiek-universa is totally ordered by $\subseteq$ (see G.Sabbagh, Archiv d. Math. 20(1969)p.449-

456). U.Felgner has shown that it is consistent with ZF^0 + (AC) + $\bigwedge_x \bigvee_y (\bar{\bar{x}} < \bar{\bar{y}} \wedge In(\bar{\bar{y}}))$ that given any partially ordered set $\langle s, \leqslant \rangle$ there is a set t of Grothendiek-universa, such that $\langle s, \leqslant \rangle$ and $\langle t, \subseteq \rangle$ are isomorphic (see U.Fg.Archiv d.Math.20(1969)p.561-566: [17], and M.Boffa - G.Sabbagh [5] .

B) THE FRAENKEL-MOSTOWSKI-SPECKER METHOD

A weak axiom of foundation, compatible with the existence of reflexive sets.

Let A be a set of reflexive sets. Define $R_0(A) = A$, $R_\alpha(A) = \bigcup\{P(R_\beta(A)); \beta < \alpha\}$ for $\alpha > 0$, and $W(A) = \bigcup\{R_\alpha(A); \alpha \in On\}$
One proves that $\alpha \leqslant \beta \rightarrow R_\alpha(A) \subseteq R_\beta(A)$ and that all sets $R_\alpha(A)$ are transitiv. It is not provable that $\bigvee_x (V = W(x))$ (see the corollary in the preceeding section!) but it is consistent with ZF^0 (same proof as in the consistency proof for $V = \bigcup V_\alpha$). In W(A) it holds that every set is wellfounded relative to A:

(WF) Axiom of weak foundation: $\bigvee_A (\bigwedge_x x \neq \emptyset \rightarrow \bigvee_y (y \in x \wedge (y \cap x = \emptyset \vee \vee A \ni y = \{y\})))$.

All models considered from now on (in this chapter) will satisfy this axiom. From now on we assume the axiom $\bigvee_x (V = W(x)) \wedge \bigwedge_y (y \in x \rightarrow y = \{y\}))$.

Automorphisms of the universe. An automorphism of V is a one-to-one mapping τ from V onto V such that $x \in y \leftrightarrow \tau(x) \in \tau(y)$.
Let A be a basis of reflexive sets for V, id est $V = W(A)$, and let π be any permutation of A (i.e. one-to-one mapping from A onto A), then π can be extended in a unique way to an automorphism π^* of V. This is done by induction: suppose we have extended π so that π acts on all sets of $R_\alpha(A)$. Let $x \in R_{\alpha+1}(A)$ and define

$$\pi(x) = \{\pi(y); y \in x\}$$

The uniqueness follows from the fact that a notion of rank, $\rho(x)$, can be defined: $\rho(x) = Min\{\alpha; x \subseteq R_\alpha(A)\}$. This shows that every automorphism τ of V is uniquely determined by a permutation of A. If π permutes A and π^* is its extension, then

$$(\pi^{-1})^* = (\pi^*)^{-1} \quad \text{and} \quad (\pi_1\pi_2)^* = \pi_1^*\pi_2^*.$$

Hence the group of permutations of A and the automorphism group of V (written as $Aut(V,\varepsilon)$) are isomorphic and we need not to distinguish between them.

Filters of subgroups. If G is any (multiplicatively written) group, H a subgroup of G, and $g \in G$, then $g^{-1}Hg$ is called a conjugate subgroup of G, conjugate with respect to H.

Definition. A non-empty set F of subgroups of a group G is called a filter (of subgroups of G) iff the following three conditions hold:

(i) $H \in F \wedge g \in G \rightarrow g^{-1}Hg \in F$.

(ii) $H_1 \in F \wedge H_1 \leqslant H_2 \wedge H_2 \leqslant G \rightarrow H_2 \in F$.

(iii) $H_1 \in F \wedge H_2 \in F \rightarrow H_1 \cap H_2 \in F$.

Here $H_1 \leqslant H_2$ means that H_1 is a subgroup of H_2. We shall show that every filter F of subgroups of any subgroup G of $\mathrm{Aut}(V,\varepsilon)$ determines a model of ZF^0.

Definition of the model $\mathfrak{M}[G,F]$. Let $G \leqslant \mathrm{Aut}(V,\varepsilon)$ and F a filter on G. For any set x let $H[x] = \{\tau \in G;\ \tau''x = x\}$ where $\tau''x = \{\tau(y);\ y \in x\}$. Obviously $H[x]$ is a subgroup of G. Again let $C(x)$ denote the transitive closure of x, i.e. $C(x) = \{x\} \cup x \cup \bigcup x \cup \ldots$ Now define $M = \{x;\ \bigwedge_y (y \in C(x) \rightarrow H[y] \in F)\}$.
Sets of the "model" $\mathfrak{M}[G,F]$ are thus elements of M and the membership-relation of $\mathfrak{M}[G,F]$ is the one of the whole universe V. We shall prove that

$$\mathfrak{M} \triangleq \mathfrak{M}[G,F] \triangleq \langle M,\varepsilon \rangle$$

is a model of ZF^0. But first we list some properties of $\langle M,\varepsilon \rangle$.
(α) M is a transitive class.
(β) If x is a subset of M, then $x \in M$ iff $H[x] \in F$.

Theorem (Specker [82] p.196): (In $ZF^0 + V = W(A)$): $\mathfrak{M}[G,F] \triangleq \langle M,\varepsilon \rangle$ is a model of ZF^0.

Proof. Ad(0): Since $H[\emptyset] = G \in F$ and $\emptyset \subseteq M$, $\emptyset \in M$ and $\emptyset$ satisfies the axiom of Null-set in $\mathfrak{M}$.
Ad(I): The axiom of extensionality in $\mathfrak{M}$ follows from (α).
Ad(II): If x and y are sets of $\mathfrak{M}$, then $H[x] \in F$ and $H[y] \in F$. Since F is a filter: $H[x] \cap H[y] \in F$. But $H[x] \cap H[y] \leqslant H[\{x,y\}]$, hence $H[\{x,y\}] \in F$. By (β) is $\{x,y\}$ a set of $\mathfrak{M}$.
Ad(III): Let x be a set of $\mathfrak{M}$; hence $H[x] \in F$. We shall show that $H[x] \leqslant H[\bigcup x]$. $\bigcup x = \{z;\ \bigvee_y (z \in y \in x)\}$. For $\tau \in H[x]$: $z \in y \in x \rightarrow \tau(z) \in \tau(y) \in \tau(x)$ since τ is an automorphism. But $\tau \in H[x] \rightarrow \tau(x) = x$ and $\tau(y) = y' \in x$. Thus: $\bigvee_y (z \in y \in x) \leftrightarrow \bigvee_y (\tau(z) \in y \in x)$ for $\tau \in H[x]$. Hence $\tau(\bigcup x) = \tau\{z;\ \bigvee_y (z \in y \in x)\} = \{\tau(z);\ \bigvee_y (z \in y \in x)\} \subseteq \bigcup x$. But similar $\tau^{-1}(\bigcup x) \subseteq \bigcup x$ follows. Hence (if 1 denotes the identical mapping):

$$\bigcup x = 1(\bigcup x) = \tau\tau^{-1}(\bigcup x) \subseteq \tau(\bigcup x) \subseteq \bigcup x.$$

Thus $\tau \in H[\bigcup x]$. Now by (ii) of the filter-definition $H[\bigcup x] \in F$. By (β) $\bigcup x \in M$.

Ad(IV): By induction one shows that M contains all ordinals (using (II) and (III) already proved). Hence $\omega \in M$ and ω satisfies the requirements of the axiom of infinity.

Ad(V): Let x be any set. We shall show that $P(x) \cap M \in M$. If $y \subseteq x$ and $\tau \in H[x]$, then $\tau(y) \subseteq x$; hence $\tau(P(x)) \subseteq P(x)$. Moreover, if $y \subseteq x$ and $y \in M$, then $\tau(y) \in M$ (see the lemma 1 below) and therefore

$$\tau(P(x) \cap M) \subseteq P(x) \cap M.$$

The same holds for τ^{-1}. Hence $\tau(P(x) \cap M) = P(x) \cap M$ (as above) and $H[x] \subseteq H[P(x) \cap M]$. Thus $P(x) \cap M \in M$. The set $P(x) \cap M$ satisfies the requirements of the power-set axiom relativized to $\mathfrak{M}$.

Instead of proving directly that the replacement schema is true in the model we shall prove first that the Aussonderungsschema holds in it. Let $\Phi(x,x_1,\ldots,x_n)$ be a ZF-formula with no free variables other than $x,x_1,\ldots,x_n$. We have to show that if $x_1,\ldots,x_n,y \in M$ then there is a set $z \in M$ such that

$$\bigwedge_x [x \in z \leftrightarrow x \in y \wedge \mathrm{Rel}(M,\Phi(x,x_1,\ldots,x_n))]$$

First one shows by induction on the length of Φ that for every $\tau \in G$: $x,x_1,\ldots,x_n \in M \rightarrow (\mathrm{Rel}(M,\Phi(x,x_1,\ldots,x_n)) \leftrightarrow \mathrm{Rel}(M,\Phi(\tau(x),\ldots,\tau(x_n))))$. In our present case, since $x_1,\ldots,x_n,y \in M$, thus $H[x_1],\ldots,H[x_n],H[y] \in F$, hence $H[x_1]\cap\ldots\cap H[x_n] \cap H[y] = H_0 \in F$, we can assume that all of $x_1,\ldots,x_n,y$ are H_0-symmetric (i.e. invariant under automorphisms $\tau \in H_0$). Consider the set

$$z = \{x;\ x \in y \wedge \mathrm{Rel}(M,\Phi(x,x_1,\ldots,x_n))\}.$$

In order to show that $z \in M$ it is by (β) enough to prove that z is H_0-symmetric. Then $H_0 \leq H[z]$, hence by (ii) $H[z] \in F$ which implies by (β) that z is in M.

Hence take $\tau \in H_0$ and $x \in z$. Then $x \in y$ and $\tau(x) \in \tau(y) = y$ since $H_0 < H[y]$ by definition of H_0. Also, since $x \in z$ we have $\mathrm{Rel}(M,\Phi(x,x_1,\ldots,x_n))$, hence $\mathrm{Rel}(M,\Phi(\tau(x),\tau(x_1),\ldots,\tau(x_n)))$. But since $\tau \in H_0 \leq H[x_i]$ $(1 \leq i \leq n)$, $\tau(x_i) = x_i$, and therefore $\tau(x) \in z$. Altogether: $\tau \in H_0 \rightarrow \tau(z) \subseteq z$. Hence $\tau(z) = z$ (proved as in (III)), and z is H_0-symmetric, q.e.d.

So far we have shown, that $\mathfrak{M} \triangleq \mathfrak{M}[G,F]$ is a model of Zermelo-set theory Z. In order to prove that $\mathfrak{M}$ satisfies the replacement-axiom we need a lemma

Lemma 1. If $x \in M$ and $\tau \in G$, then $\tau(x) \in M$.

Proof by induction on the ε-relation.
$x \in M \rightarrow H[x] \in F$. We claim that

$$H[\tau(x)] \geqslant \tau H[x] \tau^{-1}.$$

Hence take $\sigma \in H[x]$. Then $(\tau\sigma\tau^{-1})\tau(x) = \tau\sigma(\tau^{-1}\tau)(x) = \tau\sigma(x) = \tau(x)$. Thus $\tau\sigma\tau^{-1} \in H[\tau(x)]$. It follows by (i) and (ii) of the filter definition that $H[\tau(x)] \in F$. Now, if x is reflexive (id est $x \in R_0(A)$), then $\tau(x)$ is by definition of the action of τ also in $R_0(A)$, hence reflexive. But $y \in C(\tau(x)) \rightarrow y = \tau(x)$. Hence $y \in C(\tau(x)) \rightarrow H[y] = H[\tau(x)] \in F$ and we get $x \in M$. If $x \in R_\alpha(A)$ and $y \in M \rightarrow \tau(y) \in M$ for all $y \in R_\beta(A)$ for $\beta < \alpha$, then $x \in M$ implies $x \subseteq M$, hence $\tau(x) \subseteq M$. Thus, by (β), $H[\tau(x)] \in F$ implies $\tau(x) \in M$, q.e.d.

Now we return to the proof of Specker's theorem. In the presence of the axiom schema of subsets (Aussonderung) the axiom schema of replacement is equivalent to the schema

$$\bigwedge_u \bigwedge_v \bigwedge_w [\Phi(u,v) \wedge \Phi(u,w) \rightarrow v = w] \rightarrow \bigwedge_y \bigvee_z \bigwedge_u \bigwedge_v (u \in y \wedge \Phi(u,v) \rightarrow v \in z).$$

where $\Phi(u,v)$ is a ZF-formula. Now let $\Phi(u,v)$ be such a formula with no free varibles other than $u,v,x_1,\dots,x_n$. Assume that for $x_1,\dots,x_n \in M$ and all $u,v,w \in M$ we have that $\mathrm{Rel}(M,\Phi(u,v)) \wedge \mathrm{Rel}(M,\Phi(u,w))$ implies $v = w$. Let y be a set, $y \in M$. Define

$$t = \{v \in M;\ \bigvee_u (u \in y \wedge \mathrm{Rel}(M,\Phi(u,v)))\}$$

By the replacementaxiom in ZF, t is a set. Put $z = \bigcup\{\tau(t);\ \tau \in G\}$. Again by the replacementaxiom of ZF, z is a set since G is a set. Further $t \subseteq M$, hence $\tau(t) \subseteq M$, by lemma 1, thus $z \subseteq M$. Since G contains the identical mapping: $t \subseteq z$. Further z is G-symmetric, id est $\tau(z) = z$ for all $\tau \in G$, since as a group G is closed under products. Hence $H[z] = G \in F$, and by (β): $z \in M$. Thus the relativized weakened form of the replacement schema holds. This finishes the proof of Specker's theorem.

The model $\mathfrak{M}[G,F]$ was constructed relative to the <u>set</u> A of reflexive sets such that $\mathfrak{M}[G,F]$ is a subclass of $W(A) = \bigcup_\alpha R_\alpha(A)$. It is remarkable that neither A nor the elements of A are always sets in the model $\mathfrak{M}[G,F]$. But in all applications of the Fraenkel-Mostowski-Specker method we just want to have A as a set in $\mathfrak{M}$. This will be the case if the filter F satisfies the following additional condition:

(iv) $\bigwedge_x [x \in A \rightarrow H[x] \in F]$

It is easily seen (see the proof of lemma 1) that for $\mathfrak{M}[G,F] \triangleq \langle M,\varepsilon\rangle$ and F satisfying (i), (ii)(iii)(iv), $A \subseteq M$, hence $A \in M$ (since $H[A] = G \in F$) by (β), holds.
Further , if F satisfies (i),...,(iv) then in $\mathfrak{M}[G,F]$ the weak axiom of foundation (WF) holds (if in the surrounding set-theory (WF) holds).

By definition $\tau \in H[x] \rightarrow \tau''x = x$, but τ need not to be the identical mapping on x. Define for any set x:

$$K[x] = \{\tau \in G;\ \tau \restriction x = 1_x\}$$

where 1_x is the identical mapping on x and $\tau \restriction x$ is the restriction of τ to x. Remark that always $K[x] \leqslant H[x] \leqslant G$. If $H[x] \in F$ then $K[x]$ need not to be in F, but if $K[x] \in F$ then there is a wellordering of x in $\mathfrak{M}[G,F]$, if the axiom of choice holds in the surrounding set theory.

<u>Lemma 2</u>: Every $\tau \in G$ acts as the identity on the well-founded part $M \cap \bigcup_\alpha V_\alpha$ of M.

Proof by induction on the Mirmanoff-rank $\rho(x)$ for well-founded sets x.

<u>Lemma 3</u>: (In ZF^0 + (WF) + (AC)): If $G \leqslant Aut(V,\varepsilon)$ and F is a filter of subgroups of G satisfying conditions (i), (ii), (iii), then $\mathfrak{M}[G,F]$ contains wellordering relations for each well-founded set x of $\mathfrak{M}[G,F]$. Hence the axiom of choice holds in the well-founded part of $\mathfrak{M}[G,F]$.

Proof. If x is well-founded, then by lemma 2: $H[x] = K[x] = G \in F$. Since the (AC) holds in the surrounding set theory x can be mapped one-to one on an ordinal α. But obviously (by lemma 2) every well-founded set of the surrounding set theory is contained in $\mathfrak{M}[G,F]$ (the well-founded sets of $\mathfrak{M}[G,F]$ are just the well-founded sets of the surrounding set theory!) and hence α is in $\mathfrak{M}[G,F]$ and the one-to-one mapping f from x onto α is also a well-founded set, hence also in $\mathfrak{M}[G,F]$.

<u>Lemma 4</u>: (In ZF^0 + (WF) + (AC)): If $G \leqslant Aut(V,\varepsilon)$ and F is a filter of subgroups of G satisfying (i), (ii) and (iii) then a set x of $\mathfrak{M}[G,F]$ can be mapped in $\mathfrak{M}[G,F]$ in a one-to-one fashion onto a well-founded set y of $\mathfrak{M}[G,F]$ iff $K[x] \in F$.

Proof. a) Suppose that there is such a one-to-one mapping f in $\mathfrak{M}[G,F]$ from $x \in M$ onto a well-founded set $y \in M$. Since $f \in M \to H[f] \in F$ it is sufficient to show that $H[f] \leqslant K[x]$ in order to verify that $K[x] \in F$ holds. Hence, take $\tau \in H[f]$ and $u \in x$. Then

$$(*) \qquad \tau(\langle u,f(u)\rangle) = \langle \tau(u), \tau(f(u))\rangle = \langle \tau(u), f(u)\rangle$$

since $f(u) \in y$, hence $f(u)$ well-founded, hence $\tau(f(u)) = f(u)$ by lemma 2. But $\tau \in H[f] \to \tau(f) = f$, hence $\langle u,f(u)\rangle \in f \to \tau(\langle u,f(u)\rangle) \in f$, which means by (*): $\langle \tau(u), f(u)\rangle \in f$. But f is one-to-one, hence $\tau(u) = u$. Thus $\tau \in K[x]$ and $H[f] \in F$, $H[f] \leqslant K[x]$ implies by (ii) $K[x] \in F$.

b) In order to prove the converse, suppose that for some $x \in M$ we have that $K[x] \in F$. Since $\mathfrak{M}[G,F] \triangleq \langle M,\varepsilon\rangle$ is a model of ZF^0 the axiom of pairing and union hold in it, and there are subsets s of x which can be mapped in $\mathfrak{M}$ one-to-one onto well-founded sets of $\mathfrak{M}$ (e.g. singletons). For each such map f_s, $s \subseteq x$, it holds that $K[x] \leqslant H(f_s)$. The set (in the sense of the surrounding set theory) of functions f_s, ordered by "is an extension of" is inductively ordered and has therefore by Zorn's lemma a maximal element f_0. The maximality of f_0 implies that f_0 must be defined on the whole set x (this argument takes place in the surrounding set theory ZF + (WF) + (AC)). But $f_1 \subseteq f_2 \to K[x] \leqslant H[f_2] \leqslant H[f_1]$. Hence $K[x] \leqslant H[f_0]$ and $H[f_0] \in F$. Since $Rg(f_0) \subseteq M$ and $Dom(f_0) = x \subseteq M$ we infer that $f_0 \subseteq M$. Hence, by (β), $f_0 \in M$, and lemma 4 is proved.

Corollary 5: (In ZF + (WF) + (AC)). A set x of the model $\mathfrak{M}[G,F]$ is well-orderable in $\mathfrak{M}[G,F]$ iff $K[x] \in F$.

Proof. If $K[x] \in F$, the there is by lemma 4 in $\mathfrak{M}$ a one-to-one mapping f from x onto a well-founded set y. By lemma 3, y can be well-ordered.Hence f induced a welloredering of x. If, conversely, x can be wellordered in $\mathfrak{M}$, then there is in $\mathfrak{M}$ a one-to-one mapping f from x onto an ordinal α where f and α are in $\mathfrak{M}$. But α is well-founded, hence $K[x] \in F$ by lemma 4.

C) THE INDEPENCENCE OF THE AXIOM OF CHOICE

In the set theory ZF^0 + (WF) the reflexive sets in the base $R_0(A) = A$ are all different but not too much distinguished. We shall use this fact in the construction of a ZF^0-model $\mathfrak{M}$ in which (AC) does not hold.

But in order to ensure that choice fails in $\mathfrak{M}$ we require that $\mathfrak{M}$ satisfies some symmetries. These symmetries of $\mathfrak{M}$ are determined by the group $G \leqslant \mathrm{Aut}(V,\varepsilon)$ and the filter F of subgroups of G. Further suitable choices of groups G and filters F will give ZF^0-models in which the "general" axiom of choice fails but certain fragments of (AC) are true.

<u>The Model of A.Fraenkel</u>.

We shall present the model constructed by Fraenkel [21] but with the modifications due to E.P.Specker [82] (see [82] p.197-198). We work in a set theory ZF^0 + (AC) in which there is a countable set A of reflexive sets such that the weak axiom of foundation (WF) holds with respect to A, id est $V = \bigcup_\alpha R_\alpha(A)$. The consistency relative to ZF^0 was shown in section A).

Let $\{a_0, a_1, a_2, \ldots\} = A$ be a fixed enumeration of A. A transposition of A is a one-to one mapping π from A onto A which interchanges just two elements of A and is the identical mapping for all other elements. Call a transposition π of A "kind" iff π interchanges a_{2k} with a_{2k+1}. If $B = \{\{a_{2k}, a_{2k+1}\};\ k \in \omega\}$, then $\bigcup B = A$ and every kind transposition π maps B onto itself. Now let G be the group of those permutations τ of A which are a finite product of kind transpositions. Obviously G is abelian. Let F be the set of subgroups H of G whose index in G is finite:

$$F = \{H;\ H \leqslant G \wedge [G:H] < \aleph_0\}$$

We shall show that F is a filter satisfying conditions (i), (ii), (iii) and (iv).

<u>Lemma</u> (H.Poincaré): The intersection of a finite number of subgroups of finite index has finite index.

<u>Proof</u>. Let G be any group and let H_1 and H_2 be subgroups of G of finite index. Elements a and b of G lie in the same right coset of $H_1 \cap H_2$ iff $ab^{-1} \in H_1 \cap H_2$. Thus we obtain all right cosets of $H_1 \cap H_2$ by taking all non-empty intersections of right cosets of H_1 with right cosets of H_2. Thus $[G:H_1 \cap H_2]$ is finite. - The general case follows by induction on the number of subgroups.

It is well-known that $H_1 \leqslant H_2 \leqslant G$, then $[G:H_1] = [G:H_2]\cdot[H_2:H_1]$, and $H \leqslant G,\ g \in G \rightarrow [G:H] = [G:g^{-1}Hg]$. Hence our set F is in fact a filter, satisfying conditions (i), (ii), (iii). (For the grouptheoretical background we refer the reader to "Group Theory" by W.R.

SCOTT (Prentice-Hall, Inc.New Jersey 1964)p.20).

If $a \in A$, then $[G:H[a]] = 2$ (obviously), hence for all $a \in A$ the groups $H[a]$ are in F and F satisfies condition (iv). Thus the base A of reflexive sets is a set of the ZF^0-model $\mathfrak{M}[G,F] \triangleq \langle M,\varepsilon\rangle$. Now $B \subseteq M$ and since $H[B] = G \in F$ we infer that also the countable set B is a set of $\mathfrak{M}[G,F]$.

Lemma. In $\mathfrak{M}[G,F]$ the set $B = \{\{a_{2k},a_{2k+1}\};\ k \in \omega\}$ has no choice set.

Proof. Suppose there would be in $\mathfrak{M}[G,F]$ a choice set, say C, of B, such that C contains precisely one element from each set $\{a_{2k},a_{2k+1}\}$. Then $H[C]$ would be in F. But the only permutation $\tau \in G$ which fixes C is the identity. Hence $H[C]$ would be the trival subgroup $E = \{e\}$ when e is the identical mapping on A. But E has infinite index in G, a contradiction to $H[C] \in F$. B is countable in $\mathfrak{M}$, thus:

Corollary: The weak axiom of choice (AC_2^{ω}) saying, that every countable set of unordered pairs has a choice function, is independent from the axioms of the system ZF^0 + (WF).

A model of E.Specker.

Again we choose ZF^0 + (AC) + "there is a countable set A of reflexive sets such that $V = \bigcup_\alpha R_\alpha(A)$" as surrounding set theory. Let G be the group of those one-to-one mappings π from A onto A which move only finitely many elements of A. Define $F^* = \{K[t];$ t is a finite subset of A$\}$ and let F be the filter of subgroups of G such that F^* is a filter-basis of F. Specker shows in [82] p.198-199 that in the model $\mathfrak{M}[G,F]$ the following holds:

(1) The powerset of A is neither finite nor transfinite (i.e. contains no countable subset). The powerset of A is hence Dedekind-finite but not finite.

(2) There is no one-to-one mapping f from $A \times A$ into the powerset of A. Hence the statement $\bigwedge_m (m^2 \leqslant 2^m)$ fails in Specker's model.

D) THE INDEPENDENCE OF THE GENERALIZED CONTINUUM-HYPOTHESIS FROM THE ALEPH-HYPOTHESIS

We shall obtain the result mentioned in the heading by constructing Fraenkel's model in a set theory ZF^0 + (GCH) in which there exists a countable set A of reflexive sets such that $V = \bigcup_\alpha R_\alpha(A)$ is true. The following lemma shows that the latter theory is consistent and can thus be used to construct in it the model of Fraenkel.

Lemma. If ZF is consistent, then ZF^0 + (GCH) + "there exists a countable set A of reflexive sets such that $V = \bigcup_\alpha R_\alpha(A)$" is consistent too.

Proof. If ZF is consistent, then ZF + (GCH) is consistent by Gödel's theorem. Define a permutation F of the universe as in theorem 4 of chapter 3, section A. It was shown there (and in theorem 2), that

$$ZF + (AC) \vdash Rep(F, ZF^0) \wedge Rep(F, (AC))$$

Now let x be any set of power $\aleph_\alpha$ and let $P_F(x)$ be the power set of x in the sense of F, id est $P_F(x) = \{F(t);\ t \subseteq x\}$. Notice that x has also in the F-sense power $\aleph_\alpha$. But then x can be mapped one-to-one onto $\omega_\alpha - \omega_0 = \{\beta;\ \omega \leqslant \beta < \omega_\alpha\}$. We may assume that $x \cap (\omega \cup \{F(\gamma);\ \gamma \in \omega \wedge \gamma \neq 1\}$ is empty (otherwise map x onto such a set). Then the 1-1-mapping f from x onto $\omega_\alpha - \omega_0$ is not moved by F. By (GCH) $P(\omega_\alpha - \omega_0)$ can be mapped in a 1-1-fashion onto $\omega_{\alpha+1} - \omega_0$, hence the same holds for P(x). But in the model determined by F, $\omega_{\alpha+1}$ and $\omega_{\alpha+1} - \omega_0$ are equipotent and P(x) has in the F-sense power $\aleph_{\alpha+1}$. Thus

$$ZF + (GCH) \vdash Rep(F, (GCH)).$$

Let A be the set $\{F(x);\ F(x) \in \omega^*\} = \{x; F(x) \in \omega^*\}_F$.
This shows that ZF^0 + (GCH) + "there is a countable set A of reflexive sets" is consistent. But similar to v.Neumann's procedure we may restrict the universe of all sets to those which lie in some $R_\alpha(A)$ without violating any ZF^0-axiom nor the (GCH). The lemma is thus proved.

Now we proceed in the set theory whose consistency is assured by the lemma and define in it Fraenkel's model $\mathfrak{M}[G,F]$ as in section C). It was shown there that the set A is in $\mathfrak{M}[G,F]$ and that there is no wellordering of A in $\mathfrak{M}[G,F]$. Hence the (GCH) fails in Fraenkel's model. The technique for showing that the aleph-hypothesis (AH): $\bigwedge_\alpha (2^{\aleph_\alpha} = \aleph_{\alpha+1})$ holds in $\mathfrak{M}[G,F]$ is simply by proving that the model inherits the (AH) from the surrounding set theory.

Lemma. If the aleph-hypothesis holds in the surrounding set theory, then the aleph-hypothesis holds also in Fraenkel's model.

Proof. Let x be a set in Fraenkel's model $\mathfrak{M}[G,F] \triangleq \langle M,\varepsilon\rangle$ such that in $\mathfrak{M}$, x is wellordered and of power $\aleph_\alpha$. Then there is in $\mathfrak{M}$ a one-to-one function f from x onto the initial ordinal ω_α. But ω_α is a wellfounded set. Hence $K[x] \varepsilon F$ by lemma 4. f can be extended to a one-to-one mapping from P(x) onto $P(\omega_\alpha)$ by defining $f(y) = \{f(z); z \varepsilon y\}$ for $y \subseteq x$. But again $P(\omega_\alpha)$ is a wellfounded set. Since the aleph-hypothesis (AH) holds (in the set theory), there is a 1-1-mapping g from $P(\omega_\alpha)$ onto $\omega_{\alpha+1}$. Since both sets are in M, we obtain that $g \subseteq M$. But g is wellfounded, hence $H[g] = G \varepsilon F$ and therefore by (β) (see section B):g is in the model. Thus P(x) can be mapped one-to-one onto $\omega_{\alpha+1}$ and has therefore in $\mathfrak{M}$ power $\aleph_{\alpha+1}$, q.e.d.

Corollary. The statement (PW): "The powerset of a well-ordered set is wellorderable" holds in Fraenkel's-model, though (AC) fails in it.

Remark. H.Rubin has shown, that in full ZF the axiom of choice (AC) is equivalent to the statement (PW) (see: H.Rubin, Notices AMS, vol.7(1960)p.381, or H.+J.Rubin: Equivalents of the Ax.of choice, Amsterdam 1963,p.77-78). By our corollary (PW) → (AC) cannot be proved in ZF^0 alone: in ZF^0 the axiom of choice (AC) is independent from (PW), though both are equivalent in full ZF.

It follows from the result of H.Rubin, that in full ZF the (GCH) and the aleph-hypothesis (AH) are equivalent. Our lemma says that in ZF^0 alone the (GCH) is independent from (AH).

E) THE INDEPENDENCE OF THE AXIOM OF CHOICE (AC) FROM KUREPA'S ANTICHAIN PRINCIPLE

G.Kurepa has considered in his paper "Ueber das Auswahlaxiom", Math. Annalen 126(1953)p.381-384, the following statement

(KA) "Every partially ordered set $\langle s,\leqslant\rangle$ has a maximal antichain".

Here a subset t of s is called an antichain iff for $x,y \varepsilon t \rightarrow \neg(x \leqslant y \vee y \leqslant x)$. Kurepa has shown that in ZF^0, (KA) in conjunction with the

(O) Ordering-theorem: "Every set can be lineareIy ordered"

is equivalent to the axiom of choice: $ZF^0 \vdash (AC) \leftrightarrow [(KA) \wedge (O)]$ and has asked wether (KA) alone is equivalent to (AC) of not. We have proved (U.Felgner, Math.Zeitschr.111(1969)p.221-232) that in full ZF in fact (AC) and (KA) are equivalent (the axiom of foundation is used in the proof).In contrast to this result J.D.Halpern was able to show that in ZF^0 alone (AC) is independent from (KA). The proof is contained in Halpern's thesis (Berkeley 1962) and not yet published.

We shall work in a set theory ZF^0 + (AC) in which there is an infinite set A of reflexive sets such that $V = \bigcup_\alpha R_\alpha(A)$.

Let G be a group of permutations of A. If H is a subgroup of G consisting of those elements of G which leave a finite subset E of A pointwise fixed, then we say that H has finite support and E is called a support ("Träger") of H.

Definition of Halpern's model. Let G be the group of all permutations of $A = R_0(A)$ (a permutation is a surjective one-to-one mapping). Let F be the set of all such subgroups H of G which contain a finite-support subgroup. F is a filter of subgroups of G satisfying conditions (i),...,(iv). Define $\mathfrak{M} \triangleq \mathfrak{M}[G,F]$ as in section B. It follows that $\mathfrak{M}$ satisfies the axioms of ZF^0 and that $A = R_0(A)$ is a set of $\mathfrak{M}$ such that (WF), the weak axiom of foundation, holds in $\mathfrak{M}$ with respect to A as base.

Remark. Since G is the group of all permutations of A, the supports of the finite support-subgroups of G are uniquely determined (If G would not be the full group of permutations the supports would not be unique). If H is a finite support subgroup of G we let supp(H) be the support of H.

Lemma 1. If H_1, H_2 are finite support-subgroups of G, then $grp\{H_1,H_2\}$ is also a finite support-subgroup of G and $supp(grp\{H_1,H_1\}) = supp(H_1) \cap supp(H_2)$.

Proof. $grp\{H_1,H_2\}$ is the subgroup of G generated by H_1 and H_2, id est: the smallest subgroup of G containing H_1 and H_2. Define

$$H_3 = \{\tau \in G;\ \tau \text{ leaves } supp(H_1) \cap supp(H_2) \text{ pointwise fixed}\}$$

Clearly $grp\{H_1,H_2\} \leqslant H_3$. In order to prove the converse consider $\tau \in H_3$. Define $a = supp(H_1)$, $b = supp(H_2)$ and let

$$a - (a \cap b) = \{a_1,\ldots,a_k\}$$

Let $c_1,\ldots,c_k$ be distinct elements not in $a \cup \tau^{-1}(b) \cup b$. Let σ_1 be the permutation of $A = R_0(A)$ which permutes a_i with c_i $(1 \leq i \leq k)$ and is constant otherwise. Then $\sigma_1 \in H_2$. Let

$$b - (a \cap b) = \{b_1, \ldots, b_m\}$$

Notice that $\sigma_1\tau^{-1}(b_i) \notin a$ and $b_i \notin a$ (by definition) Let σ_2 be the permutation of A which maps b_i onto $\sigma_1\tau^{-1}(b_i)$ and is constant for the other elements of A. Hence

$$\sigma_2(b_i) = \sigma_1\tau^{-1}(b_i) \text{ and } \sigma_2 \in H_1.$$

Finally define $\sigma_3 = \tau\sigma_1^{-1}\sigma_2$. Then

$$\sigma_3(b_i) = \tau\sigma_1^{-1}\sigma_2(b_i) = \tau\sigma_1^{-1}\sigma_1\tau^{-1}(b_i) = b_i$$

for $1 \leq i \leq m$. Further, since τ, σ_1 and σ_2 leave $a \cap b$ pointwise fixed, σ_3 also leaves $a \cap b$ pointwise fixed. Thus σ_3 leaves b pointwise fixed and we get $\sigma_3 \in H_2$. But $\sigma_3 = \tau\sigma_1^{-1}\sigma_2 \rightarrow \tau = \sigma_3\sigma_2^{-1}\sigma_1$, thus $\tau \in grp\{H_1, H_2\}$ q.e.d.

Lemma 2. If $H[x] = \{\tau \in G;\ \tau^*(x) = x\}$ includes a finite-support subgroup, then $H[x]$ contains a finite-support subgroup which includes all other finite-support subgroups which are contained in $H[x]$.

Proof. Remember that τ^* is the unique extension of τ to an automorphism of the universe V (see section B). Let I be the intersection over the set of supports of the finite-support subgroups included in $H[x]$. Since each support is finite, hence I is finite and can be represented as an intersection of only finitely many of supports. The group generated by the union of subgroups corresponding to these finitely many supports has support I (this follows from lemma 1 and an ordinary induction), is contained in $H[x]$ and is largest in the sense stated, q.e.d.

Remark and Definition. If x is in the model $\mathfrak{M}[G,F]$, then $H[x] \in F$. But by definition of the filter F, there is a finite support-subgroup H^* contained in $H[x]$. Thus, by lemma 2, $H[x]$ includes a largest finite-support subgroup. This subgroup is uniquely determined and depends only on $H[x]$ (if x is in $\mathfrak{M}[G,F]$), and we denote this finite-support subgroup of $H[x]$ by $H_0[x]$. Further we write $F(x) = supp(H_0[x])$.

We shall prove that Kurepa's Antichain Principle (KA) holds in $\mathfrak{M}[G,F]$. Since every "abstract" partial ordering $\leq$ on a set s can be represented by the inclusion relation $\subseteq$, we may restrict ourself to the discussion of sets t, where $\subseteq$ is the partial ordering on t (namely, for $x \in s$ define $[x] = \{y \in s;\ y \leqslant x\}$ and $t = \{[x];\ x \in s\}$, then $\langle s,\leqslant\rangle$ and $\langle t,\subseteq\rangle$ are isomorphic).

Lemma 3: (KA) holds in Halpern's model $\mathfrak{M}[G,F]$.

Proof. Let t be a set of $\mathfrak{M} \triangleq \mathfrak{M}[G,F]$, and define

$Z = \{y;\ y \subseteq t \wedge y \in \mathfrak{M} \wedge F(y) \subseteq F(t) \wedge y \text{ is an anti-chain}\}$.

Z is a subset of the model $\mathfrak{M}$ but not necessarily $Z \in \mathfrak{M}$. We want to prove that Z has maximal elements.

If T is a subset of Z, totally ordered by $\subseteq$, then $\bigcup T$ is again an antichain. Further $H[\bigcup T] \geqslant \bigcap\{H[y];\ y \in T\}$ and always: $y \in Z \rightarrow H_0[t] \leqslant H_0[y] \leqslant H[y]$ where $H_0[t] \in F$. Thus $H[\bigcup T] \in F$. Since $T \subseteq Z \subseteq \mathfrak{M}$, hence $\bigcup T \subseteq \mathfrak{M}$ by the transitivity of $\mathfrak{M}$ and therefore $\bigcup T \in \mathfrak{M}$ (see (α) and (β) in section B). Finally: $H_0[t] \leqslant H[\bigcup T] \rightarrow H_0[t] \leqslant H_0[\bigcup T]$, thus (by lemma 1): $F(\bigcup T) \subseteq F(t)$. This shows that $\bigcup T \in Z$. Since Z is inductively ordered by $\subseteq$ there is in Z by Zorn's lemma a maximal element, say y_0, in Z (notice that $Z \neq \emptyset$, since $F(\emptyset) = \emptyset \subseteq F(t)$, hence $\emptyset \in Z$). We want to show that y_0 is maximal among all antichains of $\langle t,\subseteq\rangle$ in $\mathfrak{M}$.

Suppose y_0 is not a maximal antichain of $\langle t,\subseteq\rangle$ in $\mathfrak{M}$. Then there is an element $y \in t - y_0$ such that $y_0 \cup \{y\}$ is an antichain.

Let $\qquad y_1 = y_0 \cup \{\tau^*(y);\ \tau \in H_0[t]\}$.

Then $H_0[t] \leqslant H[y_0]$ implies $H_0[t] \leqslant H[y_1]$. Since $H_0[t] \in F$ therefore $H[y_1] \in F$. Since $y_0 \subseteq y_1 \subseteq t \subseteq \mathfrak{M}$ therefore $y_1 \in \mathfrak{M}$ (by (β) in sect. B). On the other hand $H_0[t] \leqslant H[y_1]$ implies $F(y_1) \subseteq F(t)$. y_1 cannot be an antichain, since otherwise $y_1 \in Z$ contradicting the maximality of y_0. Hence y_1 must have two comparable elements. We have two cases:

Case 1: There are $z \in y_0$ and $\tau \in H_0[t]$ such that $z \subseteq \tau^*(y)$ or $\tau^*(y) \subseteq z$.

Case 2: There are $\tau_1, \tau_2 \in H_0[t]$ such that $\tau_2^*(y) \neq \tau^*(y)$ and $\tau_1^*(y) \subseteq \tau_2^*(y)$.

If case 1 holds, we have $(\tau^{-1})^*(z) \subseteq y$ or $y \subseteq (\tau^{-1})^*(z)$. But $\tau \in H_0[t] \leqslant H_0[y_0] \leqslant H[y_0]$ and $z \in y_0$ implies $(\tau^{-1})^*(z) \in y$. This contradicts the fact that $y_0 \cup \{y\}$ is an anti-chain.

If case 2 holds, put $\tau = \tau_1^{-1}\tau_2$. Since $H_0[t]$ is a group: $\tau \in H_0[t]$ and we obtain the existence of $\tau \in H_0[t]$ such that $y \neq \tau^*(y)$ and $y \subseteq \tau^*(y)$. We want to find a $m_0 \in \omega$ such that $\tau^{m_0 *}(y) = y$. Hence it is natural to look at:

$$D_1 = \{w \in F(y);\ \bigvee_n (0 < n \wedge \tau^n(w) = w)\}$$

$$D_2 = \{z \in A = R_0(A);\ \bigvee_w \bigvee_n [w \in D_1 \wedge \tau^n(w) = z]\}.$$

τ^n means n-times iterated application of τ. Since $F(y)$ is finite, D_1 is finite too. Further D_2 is finite since $w \in D_1$ implies that after a finite number of successive iterations of τ one comes back to w. Thus D_2 is finite since D_1 is finite and every element w of D_1 has only finitely many images under successive iteration of τ. Also, D_2 is closed under τ. Thus D_2 together with $\tau \restriction D_2$ is a permutation group. Since τ is a one-to-one mapping on D_2, the finite cycles $S_z = \{z, \tau(z), \tau^2(z), \ldots\}$ are either equal of disjoint and form orbits of the permutation group $\langle D_2, \tau \restriction D_2 \rangle = \mathfrak{G}$. The group $\mathfrak{G}$ is hence the direct sum of these cyclic groups. Let n_0 be the order of $\mathfrak{G}$.

If $z \in F(y) - D_1$, then $\tau^n(z)$ is never in D_2 (and there is a finite numver n_z such that $m > n_z$ implies $\tau^m(z) \notin F(y)$ (since $F(y)$ is finite and $\tau^n(z) \neq z$ for all $n > 0$). Let m_0 be the first multiple of n_0 strictly greater than $\mathrm{Max}\{n_z;\ z \in F(y) - D_1\}$. Then

$$\tau^{m_0}(w) = w \text{ if } w \in D_2$$

since $m_0 = k \cdot n_0$ for some $k \in \omega$ and the cardinality of the orbits of $\mathfrak{G}$ devide the order of $\mathfrak{G}$. Further by definition of m_0: $z \in F(y) - D_1 \rightarrow n_z < m_0$, hence $\tau^{m_0}(z) \notin F(y)$. Thus if $z \in F(y) \cap \{\tau^{m_0}(w);\ w \in F(y)\}$ then $\tau^{m_0}(z) = z$.

We define a permutation σ of $A = R_0(A)$ which maps $X = F(y)$ onto $Y = \{\tau^{m_0}(z);\ z \in F(y)\}$ by $\sigma(x) = \tau^{m_0}(x)$ for $x \in X$, $\sigma(u) = x$ for $u = \tau^{m_0}(x) \in Y$ and $\sigma(v) = v$ otherwise. σ is well-defined since on $X \cap Y$ we have that σ is the identity as was just proved above.

From $\sigma(z) = \tau^{m_0}(z)$ for $z \in F(y)$ we obtain

(1) $\sigma^*(y) = (\tau^{m_0})^*(y)$

since $\sigma \restriction F(y) = \tau^{m_0} \restriction F(y)$, hence $\sigma^{-1}\tau^{m_0} \in H_0[y] \leqslant H[y]$, thus $(\sigma^{-1}\tau^{m_0})^*(y) = y$, id est $\sigma^*(y) = \tau^{m_0 *}(y)$.

Since also $\sigma\tau^{m_0}$ is the identity on $F(y)$ we obtain in a quite similar way from $\sigma(\tau^{m_0}(z)) = z$ for $z \in F(y)$:

(2) $\sigma^*(\tau^{m_0})^*(y) = y$.

By hypothesis $y \subseteq \tau^*(y)$, and since τ^* is an automorphism, we have

(3) $\quad y \subseteq \tau^*(y) \subseteq (\tau^2)^*(y) \subseteq \ldots \subseteq (\tau^{m_0})^*(y)$.

Thus by (1): $y \subseteq \sigma^*(y)$. But (3) also yields $\sigma^*(y) \subseteq \sigma^*(\tau^{m_0})^*(y)$. Applying (2), we have $\sigma^*(y) \subseteq y$. Thus $y = \sigma^*(y)$. From (1) we deduce $y = (\tau^{m_0})^*(y)$. Finally, from (3), we arrive at the contradiction $y = \tau^*(y)$ and lemma 3 is proved.

Let (AC_2) be the axiom of choice for families (= sets) whose elements are couples (= unordered pairs). Instead of proving that the (unrestricted) axiom of choice (AC) does not hold in Halpern's model $\mathfrak{M}$, we shall show that already (AC_2) fails in $\mathfrak{M}$.

Lemma 4: The weak axiom of choice (AC_2) does not hold in Halpern's model $\mathfrak{M}[G,F]$.

Proof: Let $Y = \{z;\ \bigvee_u \bigvee_v (u,v \in A = R_0(A) \wedge u \neq v \wedge z = \{\langle u,v\rangle, \langle v,u\rangle\})\}$. $A = R_0(A)$ is a set of $\mathfrak{M}$ as was noticed previously. Thus $Y \subseteq \mathfrak{M}$. But Y is closed under G, thus $H[Y] = G \in F$. Hence, by (β) of section B, Y is a set of the model $\mathfrak{M}$. Also $z \in Y$ implies $\overline{\overline{z}} = 2$ and distinct elements of Y are disjoint. Suppose there would be a choice set C for Y in $\mathfrak{M}$, id est $\bigwedge_w [w \in Y \rightarrow w \cap C$ has cardinality $1]$ and $C \in \mathfrak{M}$. It follows $H[C] \in F$ and $F[C]$ is a finite subset of the infinite set $R_0(A)$. Pick elements $u,v \in R_0(A) - F(C)$ such that $u \neq v$. Let τ be the permutation of $R_0(A)$ which interchanges u and v and is the identity otherwise. Then $\tau \in H_0[C] \leqslant H[C]$, hence $\tau^*(C) = C$, and $y = \{\langle u,v\rangle, \langle v,u\rangle\} \in Y$. Suppose $\langle u,v\rangle \in C$, then $\tau^*(\langle u,v\rangle) = \langle v,u\rangle \in \tau^*(C)$, hence $\langle v,u\rangle \in C$: a contradiction. If $\langle v,u\rangle \in C$ then one concludes similarly that $\langle u,v\rangle \in C$, again contradicting the assumption on C. Thus Y has no choice set in $\mathfrak{M}$, q.e.d.

This finishes the proof, that in Halpern's model $\mathfrak{M}[G,F]$ all axioms of ZF^0, Kurepa's Antichain Principle (KA) and $\neg(AC_2)$ are true. As a

Corollary (J.D.HALPERN): The axiom of choice (AC) does not follow from Kurepa's Antichain-Principle (KA) in ZF^0.

Remark. Since (AC_2) fails in Halpern's model $\mathfrak{M}$, the ordering principle (O) fails in $\mathfrak{M}$ too, since $ZF^0 \vdash (O) \rightarrow (AC_2)$. Further $ZF^0 \vdash$ (BPI) $\rightarrow$ (O) (via compactness-theorem of the lower predicate calculus, e.g.) where (BPI) is the Boolean Prime Ideal theorem "Every Boolean algebra has a prime ideal". Stone (Trans.AMS vol.40(1936) p.37-111) has shown in ZF^0 that (BPI) is equivalent to the "Representation Theorem for Boolean Algebras": "Every Boolean Algebra $\langle B, \sqcup, \sqcap, \neg\rangle$ is isomorphic to a set-algebra $\langle C, \cup, \cap, -\rangle$".

The statement

(SPI): "Every infinite set algebra has a non-principle prime ideal"

follows from the (BPI). Tarski has asked, whether (SPI) $\to$ (BPI) is provable. Halpern has shown, that in ZF^0 this implication is not provable. Halpern shows that in the model above the (SPI) holds while the (BPI) fails in it.

Lemma 5 (U.Felgner, M.Z. 111(1969)): Kurepa's Antichain Principle (KA) implies in ZF^0 the statement (LW) which says that every linearely ordered set can be well-ordered.

Proof. Let $\langle s, \leqslant \rangle$ be a linearly ordered set. The powerset P(s) of s is a set of chains. By a theorem of Zermelo (Math.Ann.65(1908)p. 261-281, theorem 28) there is a set K whose elements are pairwise disjoint, such that there is a one-to-one mapping f from $P(s) - \{\emptyset\}$ onto K with the property that for $\emptyset \neq t \in P(s)$, $f(t) \in K$ is isomorphic to t. Thus P(s) is represented isomorphically by K, but K is a set of pairwise disjoint chains. A maximal antichain C of $\bigcup K$ is a choice function which selects from each chain just one element. Thus we get a choice function g defined on $P(s) - \{\emptyset\}$. By Zermelo's well-ordering theorem (Math.Ann.59(1904)p.514-516, or 65(1908)p.107-128) the set s can be wellordered, q.e.d.

Thus (LW) holds in Halpern's model $\mathfrak{M}$ too. Since $ZF^0 \vdash$ (LW) $\to$ (PW), we have strengthened our result in chapter D: in ZF^0 the (AC) is independent from (LW). Further, Felgner proved that (LW) $\longrightarrow$ (KA) is not a theorem of ZF^0.

F) THE UNDEFINABILITY OF CARDINALITY IN ZF^0

One says that the sets x and y are equipotent (or equinumerous), in symbols $x \approx y$, iff there is a one-to-one function mapping x on y. The notion of the cardinal number $\overline{\overline{x}}$ of x is obtained from equipotency by abstraction. In the presence of the axiom of choice (AC) the term $\overline{\overline{x}}$ can be defined to be the least ordinal α equipotent with x. If we do not have (AC) but the axiom of foundation, we are still able to define adequately $\overline{\overline{x}}$ à la Frege-Russell-Scott:

$$\overline{\overline{x}} = \{y;\ y \approx x \wedge \bigwedge_z (z \approx x \to \rho(y) \leqslant \rho(z))\}$$

where ρ is the Mirimanoff-rank function (see chapt.I,sect.E). Here $\overline{\overline{x}}$ consists of sets y of lowest rank equinumerous with x (see D.Scott: Definitions by abstraction in axiomatic set theory, Bull.AMS 61(1955) p.442, and

[74] Dana SCOTT: The notion of rank in set-theory; Summaries Summer Institute for Symbolic Logic, Cornell Univ.1957, p.267-269).

We remark, that even in the absence of both the axioms of choice and regularity but in the presence of either the weak axiom of foundation in the form "there is a set A such that $V = \bigcup_\alpha R_\alpha(A)$" or the axiom (U.Fg.,Archiv d.Math.20): "the universe V can be covered by a well-ordered sequence of sets s_α, α an ordinal". We shall show that in ZF^0 without any additional covering axiom (like foundation, etc.) there is no adequate definition of the term $\overline{\overline{x}}$. This result was obtained first by Azriel Lévy

[50] A.LÉVY: The Definability of Cardinal Numbers; in: "Foundations of Mathematics", Gödel-Festschrift, Springer-Verlag Berlin 1969,p.15-38.

Also R.J.Gauntt has obtained this result (independently):

[22] R.J.GAUNTT: Undefinability of Cardinality; Proceedings of the U.C.L.A.-set Theory Institute 1967. To appear in 1970.

In the presentation of the proof we shall follow mainly R.J.Gauntt but in few details A.Lévy.

When one considers the question of whether one can define in ZF^0 the cardinality operation $\overline{\overline{x}}$, the following possibilities turn up:

(a) $\overline{\overline{x}}$ is definable in a set theory ST: there is a term t(x) of ST with the only free variable x such that

$$ST \vdash \bigwedge_x \bigwedge_y [t(x) = t(y) \leftrightarrow x \approx y]$$

(b) $\overline{\overline{x}}$ is relatively definable in a set theory ST: there is a term t(x, z) of ST with the only free variables z and x such that

$$ST \vdash \bigvee_z \bigwedge_x \bigwedge_y [t(x,z) = t(y,z) \leftrightarrow x \approx y].$$

Obviously (a) entails (b) (Lévy [50] considers further possibilities). If we take ZF^0 + foundation (id est ZF) or ZF^0 + (AC) as set theory ST, then (a) holds. We shall prove a strong undefinability result, namely,that even (b) does not hold for the set theory ZF^0.

Theorem (Lévy,Gauntt): If ZF^0 is consistent, then so is ZF^0 plus the schema

$$(*) \quad \neg \bigvee_x \bigwedge_a \bigvee\!\!\!{}^1_y [\phi(y,a,x) \wedge \bigwedge_b (a \approx b \leftrightarrow \phi(y,b,x))].$$

Proof. If ZF^0 is consistent, then also the theory (called ZF^∇) ZF^0 + "there is a proper class A of reflexive sets equinumerous with On (the class of all ordinals), such that for every x there exists $y \in x$ with either $y \cap x = \emptyset$ or $y \in A$" is consistent (see the results of Chapt.III, sect.A). Hence there is a function G (a classterm) mapping On one-to-one onto A. We will now construct within this universe a Fraenkel-Mostowski-Specker model $\mathfrak{M}$ of ZF^0 plus the schema (*). - In the sequel the elements of A are called atoms.

Each ordinal α can be written (in a unique way) as $\beta + n$ where β is a limit ordinal and $n \in \omega$ (this follows from Cantor's normal-form theorem). Define $\alpha \equiv 0$ iff $n \equiv 0$ (congruence modulo 2) for $\alpha = \beta + n \wedge \mathrm{Lim}(\beta) \wedge n \in \omega$, and define $\alpha \equiv 1$ iff $n \equiv 1$ modulo 2 for $\alpha = \beta + n \wedge \mathrm{Lim}(\beta) \wedge n \in \omega$. The ordinals congruent o are thus $0,2,4,\ldots,\omega,\omega+2,\omega+4,\ldots$ and the ordinals congruent 1 are $1,3,5,\ldots,$ $\omega+1,\omega+3,\ldots$ For each ordinal α, $\{G(\alpha),G(\alpha+1)\}$ is a pair of atoms and if $\alpha \equiv o$ then $\bigwedge_\beta[\beta \equiv o \wedge \alpha \neq \beta \rightarrow \{G(\alpha),G(\alpha+1)\} \cap \{G(\beta),G(\beta+1) = \emptyset]$.

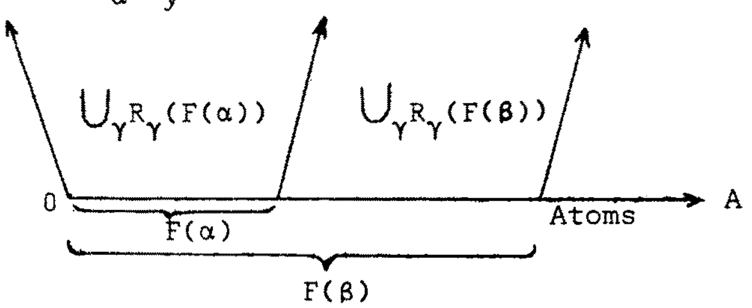
Definition. $F(\alpha) = \{G(\beta);\ (\beta \equiv 0 \wedge \beta < \alpha) \vee (\beta \equiv 1 \wedge \beta \leq \alpha)\}$.

The following definition is due to D.Mirimanoff (L'Ens.Math.vol.17 (1917)p.33 and p.211).

Definition. $\mathrm{Ker}(x) = C(x) \cap A$ = the set of atoms in the transitive closure of x.

(read: the kernel of x; Mirimanoff used the term "noyaux").
We now restrict the universe to elements of sets built up from $F(\alpha)$'s, i.e. $V = \bigcup_\alpha(\bigcup_\gamma R_\gamma(F(\alpha)))$. That is, the restricted universe consists of all x for which $\bigvee_\alpha \bigvee_y (x \in y \wedge \mathrm{Ker}(y) \subseteq F(\alpha))$.

e.g. for $\alpha < \beta$:



Notice that each $F(\alpha)$ is s set and $\bigcup_\alpha F(\alpha) = A$, where A is a proper class. For each permutation f on $F(\alpha)$, define $f(x)$ over the entire (restricted) universe as follows:

$f(x) = x$ for atoms x not in $F(\alpha)$,
$f(x) = \{f(y);\ y \in x\}$ for sets x.

This definition is welldefined since if x is in the restricted universe, then $x \subseteq R_\gamma(F(\beta))$ for some ordinals β and γ [for the definition of $R_\gamma(a)$ see p.53]. By induction hypothesis it is assumed that f is defined for all $y \in R_\delta(F(\beta))$ for $\delta \leqslant \gamma$ and all β.

Definition. A permutation f on $F(\alpha)$ is called semi-admissible iff it preserves pairs, id est, for all $\beta < \alpha$ such that $\beta \equiv 0$ there exists $\gamma < \alpha$ such that $\gamma \equiv 0$ and

$$f(\{G(\beta),G(\beta+1)\}) = \{G(\gamma),G(\gamma+1)\}.$$

Definition. A permutation f on $F(\alpha)$ is called admissible iff it fixes pairs, id est: for all $\beta < \alpha$ such that $\beta \equiv 0$ it holds that

$$f(\{G(\beta),G(\beta+1)\}) = \{G(\beta),G(\beta+1)\}.$$

Definition. x is symmetric $\leftrightarrow$ there is a finite set $\underline{a}$ of atoms such that each admissible permutation τ which leaves $\underline{a}$ pointwise fixed, fixes x (not necessarily pointwise!).

Definition. Sets of the model $\mathfrak{M}$ are those sets x which are hereditarily symmetric (id est: x and every element y of the transitive closure of x is symmetric).

Digression. Notice the similarity of the model $\mathfrak{M}$ just defined with Fraenkel's model in section C. The admissible permutations of $F(\omega)$ are called there "nice". But there is one important difference. In the definition of a symmetric set x we avoided the use of the notion of a finite support subgroup $K[\underline{a}]$ and in the definition of the model $\mathfrak{M}$ we avoided the use of a filter of subgroups. This is done since the permutations are already proper classes. Hence the groups $K[\underline{a}]$ would be totalities of proper classes and the filter F a collection of those totalities. It is possible to formulate a type theoretic extension of ZF-set theory in which sets can be collected to classes (à la v.Neumann-Bernays-Gödel) and in which classes can be collected to totalities, totalities to systems etc (in which the predicates "set", "class", "totality" "system",... are primitiv) using an idea of I.L. Novak-Gàl (Fund. Math. 37(1951)p.87-110). In such a set theory one can talk about the groups $K[\underline{a}]$, the filter F, etc. But since in the discussion above reference is made only with respect to one single class of permutations f of the <u>sets</u> $F(\alpha)$ we could restrict ourself to mention only permutations of certain type. The use of the notions "subgroup", "filter" would make only linguistical differences. Further remark that a permutation of the class A of atoms moves only elements which are in some $F(\alpha)$. Hence the "essential" part of a permutation on A is a set. This explaines that in the definition of a symmetric set we have quantified only over sets (thus class-variables to range over permutations on A are not needed). The formulae: "x is symmetric" and "x is hereditarily symmetric" are thus ZF-formulae. Thus $\mathfrak{M} = \{x;\ x \text{ is hereditarily symmetric}\}$ is a class-term of ZF.

The following lemmata are easily proved. The proofs are similar to those of section B.

<u>Lemma 1</u>. (In ZF^{∇}): If f is semi-admissible and g is admissible, then $f^{-1}gf$ is admissible.

<u>Lemma 2</u>. (In ZF^{∇}): $x \in \mathfrak{M} \leftrightarrow (x \subseteq \mathfrak{M} \wedge x \text{ is symmetric})$.

<u>Lemma 3</u>. (In ZF^{∇}): No two disjoint infinite sets of atoms are equinumerous in $\mathfrak{M}$.

<u>Proof</u>. Suppose the lemma is false. Then there are such infinite sets x and y and a one-to-one function g, mapping x onto y, in $\mathfrak{M}$. Since x,y and g are symmetric, there are finite sets a,b,c of Atoms such that every admissible permutation π leaving a (resp. b,c) pointwise fixed, fixes x (resp. y,g). If $G(\alpha) \in x - a$ for $\alpha \equiv 0$, then $G(\alpha+1) \in x$. Now pick $\alpha \equiv 0$ such that $G(\alpha) \in x - (a \cup b \cup c)$. Since g maps x onto y, $g(G(\alpha)) = G(\beta) \in y$ and $g(G(\alpha+1)) = G(\gamma) \in y$. Thus $\langle G(\alpha),G(\beta)\rangle \in g$ and $\langle G(\alpha+1),G(\gamma)\rangle \in g$. Take an admissible permutation π which interchanges the atoms $G(\alpha)$ and $G(\alpha+1)$ but is the identity otherwise. Since x and y are disjoint, π acts as the identical mapping on y. Thus $\pi(\langle G(\alpha),G(\beta)\rangle) = \langle \pi(G(\alpha)),G(\beta)\rangle = \langle G(\alpha+1),G(\beta)\rangle \in \pi(g) = g$ since π leaves c pointwise fixed. Hence $g(G(\alpha+1)) = G(\beta)$, a contradiction, g would not be one-to-one, q.e.d.

<u>Lemma 4</u>. (In ZF^{∇}): Any permutation on $F(\alpha)$, which moves only finitely many atoms, is in $\mathfrak{M}$.

<u>Proof</u>. Let a be the finite set of atoms moved by the permutation π. Then every admissible permutation τ which leaves a pointwise fixed maps π onto itself.

Lemma 5. (In ZF^{∇}): For each x and semi-admissible permutation π, $x \in \mathfrak{M} \leftrightarrow \pi(x) \in \mathfrak{M}$.

Proof. Use lemma 1 and lemma 2 and proceed as in the proof of lemma 1 of chapt. III, section B, page 55-56.

Lemma 6. For each ZF-formula $\Phi(x_1, \ldots, x_n)$ with n free variables, the following are theorems of ZF^{∇}:

(i) π semi-admissible $\rightarrow [\Phi(x_1, \ldots, x_n) \leftrightarrow \Phi(\pi(x_1), \ldots, \pi(x_n))]$

(ii) π semi-admissible $\rightarrow [\mathrm{Rel}(\mathfrak{M}, \Phi(x_1, \ldots, x_n)) \leftrightarrow \mathrm{Rel}(\mathfrak{M}, \Phi(\pi(x_1), \ldots, \pi(x_n)))]$.

Here $\mathrm{Rel}(\mathfrak{M}, \Phi)$ is the formula obtained from Φ by restricting all quantifiers to the class $\mathfrak{M}$ (see chapt. I, page 14). The proof is by induction on the length of Φ, using lemma 5.

Lemma 7. (In ZF^{∇}): $\mathfrak{M}$ is (with respect to ε) a model of ZF^{0}.

The proof is like the one of Specker's theorem (in section B, p.54) using lemmata 2, 5 and 6. Do not take the "hyper-classes" of all one-to-one mappings from A onto A, but take only the groups of admissible permutations on the sets $F(\alpha)$. These groups are sets! For every set x in the restricted universe only an initial segment $F(\alpha)$ of the class A of atoms is essential (definite).

Lemma 8. For each ZF-formula $\Phi(x_1, x_2, x_3)$ with three free variables, the following is provable in ZF^{∇}:

$$\mathrm{Rel}(\mathfrak{M}, \neg \bigvee_x \bigwedge_a \bigvee^{1}_y [\Phi(y,a,x) \wedge \bigwedge_b (a \approx b \leftrightarrow \Phi(y,b,x))]).$$

Proof. Suppose that the lemma is false. Then there is a ZF-formula $\Phi(x_1, x_2, x_3)$ and a set x in $\mathfrak{M}$ as required above. Since x is in $\mathfrak{M}$, hence in the restricted universe, there is an ordinal α such that $\mathrm{Ker}(x) \subseteq F(\alpha)$, where $\alpha \equiv 0$ can be choosen. Define

$$D_1 = F(\alpha+\omega) - F(\alpha).$$

Cleary, $D_1 \in \mathfrak{M}$. Suppose y is the (unique) cardinal of D_1, where $y \in \mathfrak{M}$, id est $\mathrm{Rel}(\mathfrak{M}, \Phi(y, D_1, x))$.

Case 1. $\mathrm{Ker}(y) \subseteq F(\alpha)$.

Case 2. $\mathrm{Ker}(y) \not\subseteq F(\alpha)$.

If case 1 holds, define $D_2 = F(\alpha+\omega.2) - F(\alpha+\omega)$, where $\omega.2 = \omega+\omega$. Then $D_2 \in \mathfrak{M}$. There is a semi-admissible permutation π of the atoms:

$$\pi(G(\alpha+n)) = G(\alpha+\omega+n)$$
$$\pi(G(\alpha+\omega+n)) = G(\alpha+n)$$
$$\pi(G(\beta)) = G(\beta) \text{ for } \beta < \alpha \text{ or } \alpha+\omega.2 \leqslant \beta.$$

Thus π fixes each element of $F(\alpha)$ and takes D_1 onto D_2. Hence $\pi(D_1) = D_2$, $\pi(D_2) = D_1$, $\pi(x) = x$ and $\pi(y) = y$. Then

$$\mathrm{Rel}(\mathfrak{M},\Phi(y,D_1,x)) \leftrightarrow \mathrm{Rel}(\mathfrak{M},\Phi(\pi(y), \pi(D_1), \pi(x))) \leftrightarrow$$
$$\mathrm{Rel}(\mathfrak{M},\Phi(y,D_2,x))$$

Hence y is also the cardinal of D_2. Thus $\mathrm{Rel}(\mathfrak{M},D_1 \approx D_2)$ violating lemma 3.

If case 2 holds, there is an ordinal $\beta \geqslant \alpha$ such that $G(\beta) \in \mathrm{Ker}(y) \wedge G(\beta) \notin F(\alpha)$. Pick an ordinal $\gamma, \gamma \equiv \beta$, $\gamma > \beta$, and define a permutation τ on $D_1 \cup F(\gamma+1)$ which interchanges $G(\beta)$ and $G(\gamma)$ and interchanges $G(\beta+1)$ with $G(\gamma+1)$ iff $\beta \equiv 0$, and interchanges $G(\beta-1)$ with $G(\gamma-1)$ iff $\beta \equiv 1$. Since $\alpha \equiv 0$, hence $G(\delta) \in F(\alpha) \rightarrow \delta < \alpha$, τ fixes all elements of $F(\alpha)$. Thus $\tau(x) = x$. τ moves $\mathrm{Ker}(y)$ and hence $\tau(y) \neq y$. Clearly τ is semi-admissible. Hence by lemma 6:

$$\mathrm{Rel}(\mathfrak{M},\Phi(y,D_1,x)) \leftrightarrow \mathrm{Rel}(\mathfrak{M},\Phi(\tau(y),\tau(D_1),x)).$$

Thus $\tau(y)$ is the cardinal of $\tau(D_1)$. Since y is the cardinal of D_1 and $\tau(y) \neq y$, D_1 and $\tau(D_1)$ have different cardinality and are therefore not equinumerous in $\mathfrak{M}$. But by lemma 4, τ is a set of $\mathfrak{M}$ and is a one-to-one function in the sense of $\mathfrak{M}$. Thus D_1 and $\tau(D_1)$ would be equinumerous in $\mathfrak{M}$, a contradiction. Lemma 8 is thus proved.

The theorem of Lévy-Gauntt follows directly from lemmata 7 and 8.

G) A FINAL WORD

The main idea behind Gödel's construction of the model $\langle L,\varepsilon \rangle$ of ZF + (AC) was to make all sets of the model definable (or nameable) by means of a certain complexe language. The natural (inductively defined) wellordering of the language induced a wellordering of the model-class L. The main idea behind the construction of ZF^0-models $\mathfrak{M}$ in which choice fails is to guarantee that $\mathfrak{M}$ contains infinitely many sets of "indiscernible" sets. Then there is no reason why a function f defined on a infinite set of sets of mutually indiscernible elements should choose from each set just the one and not the other element. This was made precise by introducing the groups G of permutations on some infinite set $A = R_0(A)$ of "atoms" (reflexive sets) and the filter F of subgroups of G.

The symmetries of the model $\mathfrak{M}$ are determined by F. If x is in $\mathfrak{M}$ and. $x = \{\tau(y);\ \tau \in G\}$ for every $y \in x$, then x is a set of indiscernibles in $\mathfrak{M}$. In Fraenkel's model (see this chapter, section C) the sets $\{a_{2k}, a_{2k+1}\}$ are e.g. sets of indiscernibles. The set B of these sets of indiscernibles is the set-theoretical counterpart to Russell's sequence of pairs of (mutually indiscernible) socks.

The "classical" way for obtaining those families of sets of indiscernibles was to take an infinite sequence of "urelements" or "reflexive sets" and to take a certain nice permutation group which acts on them. The choice of the right permutation group and the right filter of subgroups is the alpha and omega in all applications of the Fraenkel-Mostowski-Specker method. The filter F defines on the group G a topology. If in the surrounding set theory the axiom of choice holds and the weak axiom of foundation such that the atoms form a set, then the corresponding model $\mathfrak{M}[G,F]$ satisfies the (AC) iff the topology is discrete (it is supposed that the filter F satisfies conditions (i),...,(iv)), and then the model coincides with the whole universe of sets. Thus, in order to get non-trivial applications of the FMS-method, the filter F has to contain never the trivial subgroup {1} of G.

In the next chapter we shall describe Cohen's forcing method. This method applies to full ZF-set theory and yields not only independence results "below" the (AC) but also the independence of V = L from the (GCH), the independence of (GCH) from (AC) and lots of further results. Again it is possible to introduce in Cohen-models indiscernible sets by destroying the (AC). We remark that it is even possible to construct ZF models in which V = L holds and which contain indiscernibles, but then one has to assume the existence of large cardinals κ satisfying the partition relation $\kappa \longrightarrow (\omega)_2^{<\omega}$, see J.Silver's paper: A large cardinal in the constructible universe, Fund.Math.69(1970)p.93-100.

Additions to chapter III

1) The part $K[x] \varepsilon F$ then there is a one-to-one mapping from x onto some well-founded set, of lemma 4 in section B, p.57-58, can be trivially proved as follows.

   If $K[x] \varepsilon F$ then x is wellorderable in $\mathfrak{M}[G,F]$; namely let w be any wellordering of x, then $w \subseteq \mathfrak{M}[G,F]$. But obviously $K[x] \leqslant H[w]$, thus $w \varepsilon \mathfrak{M}[G,F]$. Thus x is wellorderable in $\mathfrak{M}$ and there are 1-1-mappings from x onto some ordinals in $\mathfrak{M}$. But ordinals are well-founded sets, Q.E.D.

2) The corollary on p.62 which says that (PW) holds in Fraenkel's model $\mathfrak{M}$ can be stregthened by asserting that even (LW) holds in $\mathfrak{M}$ while (AC) fails. Proof. Let $\langle s,\leqslant \rangle$ be a linearily ordered set in $\mathfrak{M}$. Define $R = \{\langle a,b \rangle ; a,b \varepsilon s \wedge a \leqslant b\}$; thus $H[R] \varepsilon F$ and $H[R] \leqslant H[s]$. We claim that for each $y \varepsilon s$ it holds that $H[R] \leqslant H[y]$. Suppose not, then there are $y \varepsilon s$ and a $\tau \varepsilon H[R]$ such that $\tau(y) \neq y$. But $\tau(y) \varepsilon s$ and R is a linear ordering on s, thus either $\langle y,\tau(y) \rangle \varepsilon R$ or $\langle \tau(y),y \rangle \varepsilon R$. If $\langle y,\tau(y) \rangle \varepsilon R$, then $\tau(\langle y,\tau(y) \rangle) = \langle \tau(y),\tau^2(y) \rangle = \langle \tau(y),y \rangle \varepsilon \tau(R) = R$, since $\tau^2 = 1$. But $\langle y,\tau(y) \rangle \varepsilon R \wedge \langle \tau(y),y \rangle \varepsilon R$ yields $y = \tau(y)$, a contradiction! The same argument applies to the case $\langle \tau(y),y \rangle \varepsilon R$. Thus every $\tau \varepsilon H[R]$ leaves s pointwise fixed. Thus, if w is any wellordering relation on s, then $H[R] \leqslant H[w]$ and it follows that $w \varepsilon \mathfrak{M}$, q.e.d.

3) It holds that $ZF^0 \vdash (AC) \rightarrow (LW) \rightarrow (PW)$, while $ZF \vdash (AC) \leftrightarrow (LW) \leftrightarrow (PW)$. We have shown under 2) that $(LW) \rightarrow (AC)$ is not provable in ZF^0. Using the model of Mostowski [64] one shows that $(PW) \rightarrow (LW)$ is not provable in ZF^0. Let us indicate that obviously Kinna-Wagners principle of choice of proper, non-empty subsets cannot hold in Mostowski's model, since (PW) holds in it and otherwise (AC) would be true in it (see Mostowski: Colloqu.Math.6(1958)p.207-208). Let us note further that J.D.Halpern has shown that in Mostowski's model the Boolean prime ideal theorem (BPI) holds (Fund.Math.55(1964) p.57-66.

4) Finally we refer to some important papers in which the FMS-method is applied: E.Mendelson [61], [62], and:

   A.Mostowski: On the Principle of Dependent choices; Fund.Math.35 (1948)p.127-130: [68].

   H.Läuchli: Auswahlaxiom in der Algebra; Comment.Math.Helvetica 37 (1962/63)p.1-18.

   H.Läuchli: The Independence of the Ordering principle from a restricted axiom of choice; Fund.Math.54(1964)p.31-43.