THE COMPLETE EXISTENTIAL THEORY OF HURWITZ'S POSTULATES FOR ABELIAN GROUPS AND FIELDS*

BY B. A. BERNSTEIN

1. *Introduction.* Hurwitz has proposed sets of postulates for abelian groups and fields.† If F', F'', F_n denote his sets for denumerable, continuous, and finite fields respectively, G', G'', G_n the corresponding sets for abelian groups, then I have proved in another paper‡ the following theorem.

THEOREM A. *Postulate-sets F', F'', G', G'', G_n $(n > 1)$ are each completely independent; postulate-set F_n is completely independent§ when, and only when, n exceeds 2 and is a power of a prime.*

The object of this note is to investigate postulate-set F_n further, and to prove the following theorem, which, together with Theorem A establishes the *complete existential theory*§ of each of Hurwitz's six postulate-sets for abelian groups and fields.

THEOREM B. *For postulate-set F_n, when n exceeds 2 and is not a power of a prime, there exists no system having the character $(+++++++)$, but there exist systems having all the other characters; when $n = 2$ there exist no systems having the characters $(-+++-+)$ and $(-+-+-+)$, but there exist systems having all the other characters.*

2. *Hurwitz's Postulates F_n for Finite Fields.* For finite fields Hurwitz's postulates are as follows (K, $\oplus$, $\odot$ being undefined):

(A_1) If a, b, c, $a \oplus b$, $c \oplus b$, and $a \oplus (c \oplus b)$ belong to K, then $(a \oplus b) \oplus c = a \oplus (c \oplus b)$.

* Presented to the Society April 8, 1922.

† W. A. Hurwitz, *Postulate-sets for abelian groups and fields,* ANNALS OF MATHEMATICS, (2), vol. 15 (1913), p. 93.

‡ *On complete independence of Hurwitz's postulates for abelian groups and fields,* ANNALS OF MATHEMATICS, (2), vol. 24 (1922).

§ See E. H. Moore, *Introduction to a form of general analysis,* New Haven Mathematical Colloquium, Yale University Press, p. 82.

(A_2) If a and b belong to K, then there is an element x of K such that $a \oplus x = b$.

(M_1) If a, b, c, $a \odot b$, $c \odot b$, and $a \odot (c \odot b)$ belong to K, then $(a \odot b) \odot c = a \odot (c \odot b)$.

(M_2) If a and b belong to K, and $a \oplus a \neq a$, there is an element x of K such that $a \odot x = b$.

(D) If a, b, c, $a \odot b$, $a \odot c$, $b \oplus c$, $(a \odot b) \oplus (a \odot c)$ belong to K, then $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

(N_n) K contains $n > 1$ elements.*

3. *Proof of Theorem B.* The proof of Theorem B is obtained with the help of the table below.†

(1) Systems 1–32 of the table have the characters $(\pm\pm\pm\pm\pm\pm-)$ for F_n.

(2) Let 1′–32′ be the systems obtained from 1–32 by substituting (a) the class of *least positive residues modulo n* for the class of integers and (b) the *least positive residue modulo n of* $a + b$, ab, $a - b$ for $a + b$, ab, and $a - b$ respectively, except that $a^2 + (b - 1)^2$ in 16 is left unchanged. Then when $n > 2$, systems 2′–32′ will have the characters $(\pm\pm\pm\pm\pm\pm+)$ except $(+++++++)$; when $n = 2$, systems 1′–9′, 11′–20′, 22′–32′ will be systems having all the characters $(\pm\pm\pm\pm\pm\pm+)$ except $(-+++--+)$ and $(-+-+--+)$.

(3) When $n > 2$ and not a power of a prime there exists no field.

(4) When $n = 2$ there exists no system having the character $(-+++--+)$. For, since postulates (A_1) and (D) have to be contradicted, and (A_2) satisfied, $a \oplus b$ must be defined by the table

$\oplus$	0	1
0	1	0
1	1	0

Further, since postulates (M_1) and (M_2) have to be satisfied,

* Postulate-sets F' and F'' are obtained from set F_n by substituting for (N_n) respectively: (N') K is countably infinite, (N'') K has the cardinal number of the continuum. Sets G_n, G', G'' are obtained from F_n, F', F'' respectively by omitting (M_1), (M_2), and (D).

† This table may also be used conveniently in the proof of Theorem A.

$a \odot b$ must be defined by one or the other of the tables:

$\odot$	0	1
0	1	0
1	0	1

$\odot$	0	1
0	0	1
1	1	0

That is, we must have either

$$a \oplus b = b + 1 \pmod 2, \qquad a \odot b = a + b + 1 \pmod 2$$

or else

$$a \oplus b = b + 1 \pmod 2, \qquad a \odot b = a + b \pmod 2.$$

But for either case postulate (D) would be satisfied.

(5) That when $n = 2$ there is no system having the character $(-+-+-+)$ I have shown in the paper cited above.

This completes the proof of our theorem.

SYSTEMS HAVING THE CHARACTERS $(\pm\pm\pm\pm\pm\pm-)$ FOR F_n

No.	Character	K	$a \oplus b$	$a \odot b$
1	$(++++++-)$	Integers*	$a + b$	ab
2	$(+++++--)$	"	$a + b$	$a + b$
3	$(++++-+-)$	"	$a + b$	0
4	$(+++-++-)$	"	$a + b$	b
5	$(++-+++-)$	"	a	$a + b$
6	$(-+++++-)$	"	b	$a + b$
7	$(++++---)$	"	$a + b$	1
8	$(+++-+--)$	"	$a + b$	$b + 1$
9	$(+-+++--)$	"	0	$a + b$
10	$(-++++--)$	"	$a - b$	$a + b$
11	$(+++--+-)$	"	$a + b + 1$	$b + 0/a$
12	$(+-+-++-)$	"	0	0
13	$(-++-++-)$	"	$b + 1$	$a/0$
14	$(+--+++-)$	"	0	b
15	$(-+-+++-)$	"	b	b
16	$(--++++-)$	"	$b + \dfrac{0}{a^2 + (b-1)^2}$	a
17	$(++-----)$	"	$a + b$	$a + 1$
18	$(+-+----)$	"	0	1
19	$(-++----)$	"	$b + 1$	1
20	$(+--+---)$	"	0	$b + 1$
21	$(-+-+---)$	"	$a - b$	$a - b$
22	$(--+++--)$	"	$ab + a$	$a + b$
23	$(+----+-)$	"	1	$b + 0/a$
24	$(-+---+-)$	"	$b + 1$	$b + 0/a$
25	$(--+--+-)$	"	$ab + a$	0
26	$(---+++-)$	"	$a + 1$	b
27	$(+------)$	"	0	$a + 1$
28	$(-+-----)$	"	$b + 1$	$a + 1$
29	$(--+----)$	"	$a + 1$	a
30	$(-----+-)$	"	$b + 0/a$	$b + 0/a$
31	$(----+--)$	"	$ab + a$	$b + 1$
32	$(-------)$	"	$a + 1$	$a + 1$

* Positive, negative, and 0.

THE UNIVERSITY OF CALIFORNIA