Concerning Abelian-Regular Transitive Triple Systems.

By

ELIAKIM HASTINGS MOORE of Chicago.

Introduction.

A *triple system* Δ_t of t elements ($t=6m+1, 6m+3$) is invariant under a certain (largest) substitution-group G^t on its t elements. The system Δ_t is called *transitive* if its group G^t is transitive, and, in particular, *cyclic* if its group G^t contains a cyclic substitution on (all) the t elements.

Mr. Netto*) 1893 has given (i. e., §§ 4, 5) explicitly (in terms of a primitive congruence-root for a prime modulus)

1) a cyclic $\Delta_{t=6m+1=p}$ where p is any prime,

2) a cyclic $\Delta_{t=6m+3=3p}$ where p is any prime of the form $p=6k+5$.

Mr. Heffter**) 1897 brings out clearly (i. e., §§ 1, 4) the "difference-problems" underlying the problems of construction of cyclic systems Δ_t ($t=6m+1, 6m+3$). He then exhibits (i. e., §§ 2, 5)

3) cyclic $\Delta_{t=6m+1=12k+7=3p-2}$ where p is any prime of the form $p=4k+3$ with the primitive root 2,

4) a cyclic $\Delta_{t=6m+3=3p}$ where p is any prime > 3 (by a slight modification of 2)).

Mr. Heffter's interesting paper has led me to recur to the question of the construction of triple systems.

A *regular* triple system Δ_t is a transitive system whose corresponding substitution-group G^t contains a *regular****) sub-group H_t^t of order

*) Netto, *Zur Theorie der Tripelsysteme* (*Mathematische Annalen*, vol. 42, pp. 143—152, 1893).

**) Heffter, *Ueber Tripelsysteme* (*Mathem. Ann.*, vol. 49, pp. 101—112, 1897).

***) An abstract group H_t of order t with the elements $A_1, \dots, A_t$ determines the holodically isomorphic *regular* substitution group H_t^t on the t letters $l_{A_1}, \dots, l_{A_t}$ by the correspondence

$$A_j \sim a_j = \begin{pmatrix} l_{A_1} & \dots & l_{A_i} & \dots & l_{A_t} \\ l_{A_1 A_j} & \dots & l_{A_i A_j} & \dots & l_{A_t A_j} \end{pmatrix}.$$

t on the t elements; the group H_t^t is a *group of regularity* of the system Δ_t . We use the notation $\Delta_t | H_t^t$ for this *regular aspect* of the system Δ_t . In this paper we study the properties of a particular regular aspect $\Delta_t | H_t^t$ of a regular system Δ_t and not the interrelations of the various regular aspects.

Two regular aspects $\Delta_t' | H_t'^t$ and $\Delta_t'' | H_t''^t$ are *equivalent* or *abstractly identical* if they differ only in the notation of the elements. Even if the two aspects are not equivalent, the two systems may be equivalent.

If two regular aspects $\Delta_t | H_t'^t$ and $\Delta_t | H_t''^t$ of the same system Δ_t are equivalent, the two groups $H_t'^t$ and $H_t''^t$ are conjugate under the group G^t of the Δ_t .

An *Abelian-regular* triple system Δ_t is a regular system Δ_t whose group of regularity H_t^t is an Abelian or commutative group.

An abstract Abelian group H_t of order t is fully characterised by its system of *invariants**), say its *invariant-character*,

$$(1) \quad [p_1^{n_1}, \dots, p_i^{n_i}, \dots, p_d^{n_d}]_d,$$

which is a certain combination of powers of primes — the *invariants* — whose product is the order t . And conversely, every such combination (1) is the invariant-character of precisely one Abelian group H_t .

Of all abstract Abelian groups H_t of a certain order t two are of preëminent simplicity and interest:

$$(2) \quad 1) \text{ the cyclic } H_t, \quad 2) \text{ the cyclid } H_t.$$

If the invariants are by pairs relatively prime, then the group H_t is the cyclic H_t , and conversely. If the invariants are individually prime, then the group H_t is what I call the cyclid H_t , and conversely. These two groups are identical if and only if the order t is the product of unrepeatd primes; in this case there is indeed only this one Abelian group H_t .

We speak similarly of *cyclid triple systems* Δ_t , and notice at once that the cyclic systems 1), 2), 4) are also cyclid systems.

The contents of this paper I now briefly summarize.

§ 1: A triple system Δ_t with the Abelian-regular aspect $\Delta_t | H_t^t$ decomposes or separates (as to its $\frac{1}{6}t(t-1)$ triples) into m_1 configurations**) of type 1^0 Cf $t_3 = Cf_1 \begin{pmatrix} t & 3 \\ 3 & t \end{pmatrix}$ and m_2 configurations of

*) Weber, Algebra, vol. 2, p. 39 fg.

**) I use the *general matrix notation* for configurations introduced in I (*The General Tactical Configuration: Definition and Notation*) of my paper *Tactical Memoranda I—III* (*American Journal of Mathematics*, vol. 18, pp. 264—303, 1896).

In particular, a tactical configuration $Cf \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of rank 2 is an arrangement

type $2^0 Cf_2 \left(\begin{smallmatrix} t & 1 \\ 3 & \frac{1}{3}t \end{smallmatrix} \right)$ likewise regular with respect to the group H_t^t ,

where $m_1 t + m_2 \frac{1}{3}t = \frac{1}{6}t(t-1)$, that is, $3m_1 + m_2 = \frac{1}{2}(t-1)$. Thus, $(m_1, m_2) = (m, 0)$ if $t = 6m + 1$, and $(m_1, m_2) = (m - m', 1 + 3m')$ if $t = 6m + 3$, where m' is an integer such that $0 \leq m' \leq m$.

Denoting by $A_1, \dots, A_t$ the t elements of the abstract group H_t and by 1 the identity-element, we find that a regular configuration $Cf_1 | H_t^t$ or $Cf_2 | H_t^t$ depends upon a *sextette* $\Sigma_1 | H_t$ or $\Sigma_2 | H_t$

$$(3) \quad \Sigma | H_t = \begin{bmatrix} A_1 & A_2 & A_3 \\ A_1^{-1} & A_2^{-1} & A_3^{-1} \end{bmatrix} \quad \left(\begin{array}{l} A_1 A_2 A_3 = 1 \\ A_i \neq 1, i = 1, 2, 3 \end{array} \right)$$

of six or two distinct elements respectively; in the latter case

$$A_1 = A_2 = A_3.$$

Conversely, a sextette $\Sigma_1 | H_t$ or $\Sigma_2 | H_t$ determines two $Cf_1 | H_t^t$ or one $Cf_2 | H_t^t$ respectively. The two $Cf_1 | H_t^t$ are equivalent.

The regular $\Delta_t | H_t^t$ depends upon a *separation* $\Sigma_{m_1, m_2} | H_t$ of the $t - 1$ elements $A_i (A_i \neq 1)$ of the H_t into m_1 sextettes $\Sigma_1 | H_t$ and m_2 sextettes $\Sigma_2 | H_t$.

Conversely, such a *sextette-separation* $\Sigma_{m_1, m_2} | H_t$ determines $2m_1 \Delta_t | H_t^t$,

The determinations are in every case absolutely explicit in terms of the data.

§ 2: Absolutely explicit exhibition (*without* the use of primitive congruence-roots) of

- (I) a sextette-separation $\Sigma_{m, 1} | H_{t=6m+3}$
 where H_t is any Abelian group of order $t = 6m + 3$ having one invariant*) 3,

and so (by § 1) of

- (I') 2^m Abelian-regular triple systems $\Delta_{t=6m+3} | H_t^t$.

§ 3: Modification of the phrasings of § 1 by the introduction of the *Galois field notions*, which are so useful in tactical investigations**).

§ 4: Explicit exhibition (in terms of primitive roots of Galois fields and of primitive roots of prime-power moduli) of (in general***) more than one)

of a elements into d c -ads in such a way that every element enters exactly b c -ads (of course the relation $ab = cd$ holds).

*) This a restriction only if t is divisible by 9. For every $t = 6m + 3$ there is at least one such H_t .

**) See, for instance, my paper, *Tactical Memoranda I-III*, cited above.

***) I exhibit *only one* separation (II) *if and only if* t is a prime of the form $6k + 1$ or the square of a prime of the form $6k + 5$. In the former case this separation is the one underlying Mr. Netto's system 1).

(II) sextette-separation $\Sigma_{m,0} | H_{t=6m+1}$

where t is any integer of the form $6m+1$ in which every prime factor p of the form $p=6k+5$ enters an even number of times, and where H_t is any Abelian group of order t in whose invariant-character every such prime enters always with the exponent 1,

and so (by § 1), for every such separation, of

(II') 2^m Abelian-regular triple systems $\Delta_{t=6m+1} | H_t'$.

These constructions (I', II') are effected (§§ 2, 4) by flexible methods. It is quite likely that apart from a few exceptional cases I have exhibited for the t 's in question representatives of a number λ_t of classes of Δ_t , where λ_t is greater than 1 and increases rapidly with t and with the complexity of t 's prime-factor composition. But in order to prove this it would be necessary to scrutinize the systems Δ_t much more closely and on the basis of essential properties of the systems Δ_t (independent of the accident of method of construction) to sort them into distinct sorts*).

In my paper**) of 1893 I showed how to construct by an elementary reduction-method for every t of the form $6m+1$ or $6m+3$ and greater than 13 at least two distinct sorts of classes of triple systems Δ_t .

I expected in a later paper to "consider certain triple systems whose groups are interesting" (l. c., p. 272). Indeed of the results of the present paper I worked out at that time the general theory of the cyclic Δ_t in the ordinary cyclic notation — of the unipartite character $\{t\}_1$ (§ 1) — (very much***) as now presented by Mr. Heffter), and then (as a generalization of the cyclic-cyclid case $t=p=6m+1$) passed to the general theory of the cyclid $\Delta_{t=p^n=6m+1}$ in the Galois field phrasing of the unipartite characteristic $\{[p^n]\}_1$ (§ 3), and had immediately (as a generalization of Mr. Netto's cyclic-cyclid $\Delta_{t=p=6m+1}$ (1)) the cyclid $\Delta_{t=p^n=6m+1} | H_t' \{[p^n]\}_1$ (§ 4).

Mr. Heffter exhibits his cyclic $\Delta_{t=6m+3=3p}$ ($p>3$) 4) in the ordinary cyclic notation of the unipartite character $\{3p\}_1$. I discover that the exhibition in the phrasing of the bipartite character $\{3, p\}_2$ is much more elegant (§ 2) and am led to the present analysis of the general Abelian-regular transitive triple systems in the phrasings of the f -partite characters (§ 1) and the $(g+h)$ -partite characteristics (§ 3).

*) Cf. *Mathem. Annalen*, vol. 43, p. 272.

**) *Concerning Triple Systems* (*Mathem. Annalen*, vol. 43, pp. 271–285, 1893).

***) Only more fully, viz., by the introduction of the 6-adic sextettes $\Sigma | \text{cyclic } H_t$ (§ 2) and the corresponding separation $\Sigma_{m_1, m_2} | \text{cyclic } H_t$. The 6-idic sextettes $\sigma | \text{cyclic } H_t$ and the corresponding separation $\sigma_{m_1, m_2} | \text{cyclic } H_t$ are given in the difference-problem phrasing by Mr. Heffter.

[Addition of May 4, 1897. In a paper *Concerning Regular Triple Systems* to appear in the autumn in the *Bulletin of the American Mathematical Society* I show how the general regular triple system $\Delta_t | H_t$ depends upon a 6-idic sextette-separation $\sigma_{m_1, m_2} | H_t$ and then (as a generalization of I § 2 of this paper) exhibit explicitly a separation $\sigma_{m, 1} | H_{t=6m+3}$, where H_t is any group of order $t = 6m + 3$ having a self-conjugate element A_0 of period 3 and a sub-group K_{2m+1} not containing A_0].

§ 1.

Abelian-regular triple systems $\Delta_t | H_t$ and the corresponding sextette-separations $\Sigma_{m_1, m_2} | H_t$.

An abstract Abelian group H_t may be taken as given by a certain *base*

$$(1) \quad \{A_1, \dots, A_i, \dots, A_f\}$$

where the basal elements A_i are abstract *generators* of the group H_t which obey the *generational relations*

$$(2) \quad A_i^{a_i} = 1, \quad A_i A_j = A_j A_i \quad (i, j = 1, \dots, f)$$

where the a_i are positive integers, the *basal periods*. The order t is the product of the periods:

$$(3) \quad t = \prod_{i=1, f} a_i.$$

Such a basal exhibition of H_t depends entirely upon the *f-partite basal-character*

$$(4) \quad \{a_1, \dots, a_i, \dots, a_f\}_f.$$

Conversely, every character $\{a_1, \dots, a_i, \dots, a_f\}_f$ (4) defines an Abelian group $H_t (t = a_1 \dots a_i \dots a_f)$ with basal exhibition

$$H_t \{a_1, \dots, a_i, \dots, a_f\}_f.$$

Obviously two characters having the same periods a_i arranged however in different orders on the faces of the characters define the same abstract group; two such characters are not (essentially) distinct.

The group H_t has one *invariant-character* (Intr. (1))

$$(5) \quad [p_1^{n_1}, \dots, p_i^{n_i}, \dots, p_a^{n_a}]_a.$$

Every basal-character $\{a_1, \dots, a_i, \dots, a_f\}_f$ of this H_t serves to define the invariant-character as follows. The invariant-character of a cyclic group $G_a \{a\}_1$ is the combination of powers of distinct primes whose product is a . The invariant-character of $H_t \{a_1, \dots, a_i, \dots, a_f\}_f$ is the combination of the invariants of the basal cyclic groups

$$G_{a_i} \{a_i\}_1 \quad (i = 1, \dots, f).$$

The various basal-characters of a group $H_t[p_1^{n_1}, \dots, p_i^{n_i}, \dots, p_d^{n_d}]_d$ are easily obtained from the invariant-character. For every group H_t of order t a power of a prime there is (essentially) only one basal-character, but for every group H_t of other orders t there are various (essentially) distinct basal-characters.

The groups $H_t\{p_1^{n_1}, \dots, p_d^{n_d}\}_d$ and $H_t[p_1^{n_1}, \dots, p_d^{n_d}]_d$ are identical.

We are in this § 1 dealing with an abstract Abelian group H_t , its corresponding regular substitution-group H_t^t , and an Abelian-regular triple system $\Delta_t | H_t^t$.

If for the moment we denote the t elements of H_t by $A_i (i=1, \dots, t)$, then the regular H_t^t is a substitution-group on the t letters A_i holodrically isomorphic to the H_t by the correspondence

$$(6) \quad A_j \sim \begin{pmatrix} A_1 & \dots & A_i & \dots & A_t \\ A_1 A_j & \dots & A_i A_j & \dots & A_t A_j \end{pmatrix}.$$

Of the Abelian group $H_t\{a_1, \dots, a_i, \dots, a_f\}_f$ the $t=a_1 \dots a_i \dots a_f$ elements are

$$(7) \quad A_E = A_{a_1, \dots, e_i, \dots, e_f} = A_1^{a_1} \dots A_i^{e_i} \dots A_f^{e_f} \\ (e_i = 0, 1, \dots, a_i - 1; i = 1, 2, \dots, f)$$

where E denotes the f -partite mark with integral elements e_i

$$(8) \quad E = \{e_1, \dots, e_i, \dots, e_f\}.$$

The t marks E with the character $\{a_1, \dots, a_i, \dots, a_f\}_f$ form a system closed under the addition and subtraction*) — inner, in Grassmann's sense —

$$(9) \quad E' = \{\dots, e'_i, \dots\}, \quad E'' = \{\dots, e''_i, \dots\}, \quad E = \{\dots, e_i, \dots\} \\ E' \pm E'' = E, \quad e'_i \pm e''_i \equiv e_i \pmod{a_i} \quad (i = 1, \dots, f).$$

The additive-group $H_t^* \{a_1, \dots, a_i, \dots, a_f\}_f$ of the t marks E and the group $H_t \{a_1, \dots, a_i, \dots, a_f\}_f$ of the t elements A_E are holodrically isomorphic:

$$(10) \quad A_{E'} A_{E''} = A_{E' + E''}.$$

We introduce as the t letters of the H_t^t the t letters l_E or the t marks E ; then H_t^t contains the t substitutions

$$(11) \quad A_E = \left(\dots, \frac{l_E}{l_{E' + E}}, \dots \right) = \left(\dots, \frac{E'}{E' + E}, \dots \right).$$

*) We write further, e being any integer,

$$0 = \{0, \dots, 0, \dots, 0\}, \quad eE = Ee = \{ee_1, \dots, ee_i, \dots, ee_f\}.$$

The triple system $\Delta_t | H_t^t \{a_1, \dots, a_i, \dots, a_f\}_f$ in the t marks $E\{\dots, a_i, \dots\}_f$ is invariant under the t substitution A_E (11), where

$$t = a_1 \dots a_i \dots a_f = 6m + 1 \quad \text{or} \quad 6m + 3.$$

In this case then the periods a_i are all odd.

Hence the Δ_t contains with the triple $[E_1 E_2 E_3]$ the t triples (not necessarily all distinct)

$$(12) \quad [E_1 + E \quad E_2 + E \quad E_3 + E] \quad (E \text{ any}).$$

Writing the triple or 3-ad $[E_1 E_2 E_3]$, having regard to the order of the marks, as a 3-id $\{E_1 E_2 E_3\}$, we see that the corresponding sextette of differences

$$(13) \quad \begin{Bmatrix} E_2 - E_3 & E_3 - E_1 & E_1 - E_2 \\ E_3 - E_2 & E_1 - E_3 & E_2 - E_1 \end{Bmatrix}$$

is an invariant, and indeed a *characteristic invariant* for the 3-idic triples $\{E_1 + E \quad E_2 + E \quad E_3 + E\}$ of this set (12).

Such a difference-sextette has always the form

$$(14) \quad \sigma | H_t^* = \begin{Bmatrix} D_1 & D_2 & D_3 \\ -D_1 & -D_2 & -D_3 \end{Bmatrix}$$

where*)

$$(15) \quad D_1 + D_2 + D_3 = 0, \quad D_i \neq 0, \quad D_i \neq -D_j \quad (i, j = 1, 2, 3),$$

$$(16) \quad D_1, D_2, D_3$$

are either (1⁰) no two equal or (2⁰) all equal.

According as the sextette $\sigma | H_t^*$ is $\sigma_1 | H_t^*$ or $\sigma_2 | H_t^*$, of the type 1⁰ or 2⁰, it contains six or two distinct marks, and the corresponding set of triples (12) contains t or $\frac{1}{3}t$ triples, and is indeed a

(tactical) *configuration* $Cf_1 \begin{pmatrix} t & 3 \\ 3 & t \end{pmatrix}$ or $Cf_2 \begin{pmatrix} t & 1 \\ 3 & \frac{1}{3}t \end{pmatrix}$ regular with

respect to the group H_t^t of substitutions A_E (11). The type 2⁰ occurs only if t has the form $t = 6m + 3$.

The triple system $\Delta_t | H_t^t$ is the composition of m_1 configurations of type 1⁰ $Cf_1 | H_t^t$ and m_2 configurations of type 2⁰ $Cf_2 | H_t^t$ with distinct triples. Here $tm_1 + \frac{1}{3}tm_2 = \frac{1}{6}t(t-1)$, $3m_1 + m_2 = \frac{1}{2}(t-1) = 3m$ or $3m + 1$. Hence we have

) The periods a_i are all odd. Every triple has three distinct marks. Two triples having two marks in common have also the third of each in common. The sextette $\sigma | H_t^$ (14) in which $D_1 + D_2 + D_3 = 0$ belongs to the 3-idic triples

$$\{0, -D_3, D_2\}, \quad \{D_3, 0, -D_1\}, \quad \{-D_2, D_1, 0\}.$$

From these remarks one draws the conclusions (15), (16) of the text.

$$(17) \quad t = \begin{cases} 6m+1 \\ 6m+3 \end{cases}, \quad (m_1, m_2) = \begin{cases} (m, 0) \\ (m-m', 1+3m') \end{cases} \quad 0 \leq m' \leq m.$$

Corresponding to and characteristic of this *configuration-separation* $Cf_{m_1, m_2} | H_t^t$ of the triple system is a *sextette-separation* $\sigma_{m_1, m_2} | H_t^*$ of the $t-1$ marks E ($E \neq 0$) into m_1 sextettes $\sigma_1 | H_t^*$ and m_2 sextettes $\sigma_2 | H_t^*$ (Repetitions of marks occur only within the individual sextettes $\sigma_2 | H_t^*$).

Conversely, with respect to any Abelian group

$$H_t \{a_1, \dots, a_i, \dots, a_f\}_f$$

of order $t = a_1 \dots a_i \dots a_f = 6m+1, 6m+3$ any such sextette-separation $\sigma_{m_1, m_2} | H_t^*$ of the $t-1$ marks E ($E \neq 0$) serves uniquely to define an Abelian-regular triple system $\Delta_t | H_t^t$.

A 6-adic sextette $\Sigma_1 | H_t^*$ of type 1^0 (15), (16)

$$(18) \quad \Sigma_1 | H_t^* = \begin{bmatrix} D_1 & D_2 & D_3 \\ -D_1 & -D_2 & -D_3 \end{bmatrix}$$

may be written in $12 = 2 \cdot 3!$ ways as a 6-idic sextette $\sigma_1 | H_t^*$ (14). Of these the six derived from the two

$$(19) \quad \left\{ \begin{array}{ccc} D_1 & D_2 & D_3 \\ -D_1 & -D_2 & -D_3 \end{array} \right\} \quad \left\{ \begin{array}{ccc} -D_1 & -D_3 & -D_2 \\ D_1 & D_3 & D_2 \end{array} \right\}$$

by cyclical permutations of their columns determine the same configuration $Cf_1 | H_t^t$; they arise from the six 3-idic triples $\{E_1 E_2 E_3\}$ corresponding to one 3-adic triple $[E_1 E_2 E_3]$. We say that these six 6-idic sextettes are *essentially* the same. The remaining six similarly determine another configuration $Cf_1 | H_t^t$.

The two configurations depend respectively upon the two say *opposite* (essentially distinct) 6-idic sextettes $\sigma_1 | H_t^*$

$$(20) \quad \left\{ \begin{array}{ccc} D_1 & D_2 & D_3 \\ -D_1 & -D_2 & -D_3 \end{array} \right\} \quad \left\{ \begin{array}{ccc} -D_1 & -D_2 & -D_3 \\ D_1 & D_2 & D_3 \end{array} \right\}$$

which correspond to the 6-adic sextette (18).

A 6-adic sextette $\Sigma_2 | H_t^*$ of type 2^0 (15), (16) determines only one configuration $Cf_2 | H_t^t$.

Thus, a $\Delta_t | H_t^t$ with the configuration-separation $Cf_{m_1, m_2} | H_t^t$ determines essentially only one 6-idic sextette-separation $\sigma_{m_1, m_2} | H_t^*$ and one 6-adic sextette-separation $\Sigma_{m_1, m_2} | H_t^*$ of the $t-1$ marks E ($E \neq 0$).

Conversely, a separation $\sigma_{m_1, m_2} | H_t^*$ determines one

$$\Delta_t | H_t^t = Cf_{m_1, m_2} | H_t^t,$$

while a separation $\Sigma_{m_1, m_2} | H_t^*$ determines 2^{m_1} essentially distinct separations $\sigma_{m_1, m_2} | H_t^*$ and so 2^{m_1} $\Delta_t | H_t^t = Cf_{m_1, m_2} | H_t^t$. These 2^{m_1} aspects $\Delta_t | H_t^t$ are distinct in the t marks E . They represent however

at most 2^{m_1-1} classes of aspects $\Delta_i | H_i^t$, for the substitution replacing every mark E by its opposite mark $-E$ interchanges the 2^{m_1} aspects by pairs.

It is clear that the phrasings $\sigma_1 | H_i^*$, $\sigma_2 | H_i^*$, $\sigma_{m_1, m_2} | H_i^*$, $\Sigma_1 | H_i^*$, $\Sigma_2 | H_i^*$, $\Sigma_{m_1, m_2} | H_i^*$ in terms of the additive-group H_i^* of the marks E are equivalent to the corresponding phrasings $\sigma_1 | H_i, \dots, \Sigma_{m_1, m_2} | H_i$ in terms of the holodrically isomorphic group H_i of the t elements A_E . The H_i -phrasings, being the more fundamental, were used in the summary in the introduction. The H_i^* -phrasings however are better adapted for specific applications.

§ 2.

Explicit exhibition of a sextette-separation

$$\Sigma_{m,1} | H_{t=6m+3}$$

where H_t is any Abelian group of order $t = 6m + 3$ having one invariant 3.

The Abelian group H_t has the invariant-basal-character

$$(1) \quad \{p_1^{n_1} = 3, p_2^{n_2}, \dots, p_i^{n_i}, \dots, p_d^{n_d}\}_d.$$

We separate this into the two supplementary characters

$$(2) \quad \{p_1^{n_1} = 3\}_1, \quad \{p_2^{n_2}, \dots, p_d^{n_d}\}_{d-1},$$

and write similarly for the corresponding marks

$$(3) \quad E = \{e_1, e_2, \dots, e_d\} = \{e_1; C\}; \quad \{e_1\} = \{+1\}, \{-1\}, \{0\}; \\ C = \{e_2, \dots, e_d\}.$$

There are $t = 6m + 3 = 3u$ d -partite marks E ; there are $u = 2m + 1$ $(d-1)$ -partite marks C .

For this system of $t-1$ marks E ($E \neq 0$) we proceed to exhibit a 6-adic sextette-separation $\Sigma_{m,1} | H_i^*$ consisting of m sextettes $\Sigma_1 | H_i^*$ and one sextette $\Sigma_2 | H_i^*$.

The single sextette $\Sigma_2 | H_i^*$ is

$$(4) \quad \Sigma_2 = \begin{bmatrix} B & B & B \\ -B & -B & -B \end{bmatrix} \quad B = \{1, 0, \dots, 0\} = \{1; 0\}.$$

The remaining $t-3 = 6m = 3(u-1)$ marks E ($E \neq 0, B, -B$) have the form

$$E = \{e; C\} = \{1; C\}, \{-1; C\}, \{0; C\} \quad (C \neq 0).$$

The $u-1 = 2m$ marks C ($C \neq 0$) separate uniquely into m pairs of opposite marks, $+C, -C$; $C \neq -C$, since every period $p_i^{n_i}$ ($i=2, \dots, d$) is odd.

To every such pair of opposite marks corresponds a sextette $\Sigma_i | H_i^*$

$$(5) \quad \Sigma_1^{(C)} = \Sigma_1^{(-C)} = \left[\begin{array}{ccc} \{ 1; +C \} & \{ -1; +C \} & \{ 0; -2C \} \\ \{ -1; -C \} & \{ 1; -C \} & \{ 0; +2C \} \end{array} \right].$$

We have exhibited a 6-adic sextette-separation $\Sigma_{m,1} | H_{t=6m+3}^*$ of remarkable simplicity.

It determines 2^m essentially distinct 6-idic sextette-separations $\sigma_{m,1} | H_{t=6m+3}^*$.

Every separation $\sigma_{m,1} | H_{t=6m+3}^*$ yields (§ 1) an Abelian-regular triple system $\Delta_{t=6m+3} | H_t'$ with the configuration-separation $Cf_{m,1} | H_t'$.

§ 3.

Galois Field phrasing of § 1. The characteristics

$$\{ [p_1^{n_1}], \dots, [p_g^{n_g}]; p_1'^{n_1'}, \dots, p_h'^{n_h'} \}_{g+h}$$

of an Abelian group.

Preparatory to specific applications in § 4 of the theorems of § 1 we here modify the phrasings of § 1 by the introduction of the Galois field notions*).

A Galois field $GF[p^n]$ of order p^n , of rank n , and of modulus p (a prime), is a system of p^n marks μ which may be combined by the four fundamental operations of algebra — addition, subtraction, multiplication and division —, these operations being subject to the ordinary operational identities of algebra, and the result of every such operation being an uniquely determined mark of the field. *The operations are purely tactical.*

There is one and only one Galois field $GF[p^n]$ for every order p^n , p a prime, n a positive integer. For $n = 1$, the $GF[p^n = p]$ consists (to speak concretely) of the classes of integers (modulo p).

The $GF[p^n]$ qua additive-group $AG[p^n]$ is an Abelian group with the invariant-basal character $\{p, \dots, p\}_n$, that is, it is the cyclid group of order p^n .

*) Galois, *Sur la théorie des nombres* (*Bulletin des Sciences Mathématiques* de M. Ferussac, vol. 13, p. 428, 1830; reprinted, *Journal de Mathématiques pures et appliquées*, vol. 11, pp. 398—407, 1846).

Serret, *Algèbre supérieure*, fifth edition, vol. 2, pp. 122—189.

Jordan, *Traité des substitutions*, pp. 14—18.

Moore, *A doubly infinite system of simple groups* (*Mathematical Papers read at the... Congress... Chicago 1893*, pp. 208—242, 1896; in abstract, *Bulletin of the New York Mathematical Society*, vol. 3, Dec., 1893. § 3 is an abstract formulation of the Galois field theory).

Its every mark μ satisfies the generalized Fermat equation

$$x^{p^n} - x = 0.$$

The $GF[p^n]$ has primitive roots ϱ ; every mark μ ($\mu \neq 0$) is a power of a primitive root ϱ , while ϱ itself is a primitive root of the equation $x^{p^n-1} = 1$. The multiplicative-group $MG[p^n]$ of the $p^n - 1$ marks μ ($\mu \neq 0$) of the $GF[p^n]$ is the cyclic group of order $p^n - 1$.

In § 1 we have introduced the basal character $\{a_1, \dots, a_f\}_f$ as fundamental for the Abelian group $H_f\{a_1, \dots, a_f\}_f$ and the system of t f -partite marks E , $E = \{e_1, \dots, e_f\}$. These marks E formed a closed system under inner addition and subtraction (§ 1, (9)). They have not been otherwise combined.

In case certain n of the periods a_i — say $a_1, \dots, a_n$ — are each p a prime, we may effect a 1 — 1 correspondence invariant under addition and subtraction between the p^n n -partite marks $E' = \{e_1, \dots, e_n\}$ with the character $\{p, \dots, p\}_n$ and the p^n marks ε of the $GF[p^n]$. We write the character $\{p, \dots, p\}_n$ more briefly $\{[p^n]\}$.

After suitable change of order and grouping of the periods a_i of the character $\{a_1, \dots, a_f\}_f$ we may replace it by the more general*) character, call it *characteristic*,

$$(1) \quad \{[p_1^{n_1}], \dots, [p_g^{n_g}]; b_1, \dots, b_h\}_{g+h} \quad \left(f = h + \sum_{i=1, g} n_i\right)$$

where the $p_1, \dots, p_g$ are primes (not necessarily distinct), and the

$$t = \prod_{i=1, f} a_i = \prod_{i=1, g} p_i^{n_i} \cdot \prod_{i=1, h} b_i$$

f -partite marks $E = \{e_1, \dots, e_f\}$ by the t $(g+h)$ -partite marks

$$(2) \quad E = \{\varepsilon_1, \dots, \varepsilon_g; e_1, \dots, e_h\}$$

where ε_i is a mark of the $GF[p_i^{n_i}]$ ($i = 1, \dots, g$) and e_i is an integer taken modulo b_i ($i = 1, \dots, h$).

Every character is a characteristic (without Galois-elements). In a characteristic it makes no (essential) difference if a prime period-element $b = p$ be written as a Galois-element $[p^n] = [p]$. Thus, the most general *cyclid characteristic* may be written (without period-elements) in the form

$$(3) \quad \{[p_1^{n_1}], \dots, [p_g^{n_g}]\}_g.$$

There is for a given order t (essentially) only one cyclid characteristic if and only if t is the product of unrepeatd prime factors.

*) Since the change of order and grouping may in general be effected in several essentially distinct ways.

The (inner) multiplication of two marks E of the same characteristic is defined after the analogy of § 1 (9)*. (This multiplication depends on the characteristic and not merely on the character.)

A mark E such that the equation $EE' = 0$ has a solution $E' \neq 0$ is called a *divisor of zero*. Such a mark E has as one of its elements ε_i the mark $\varepsilon_i = 0$ of the $GF[p_i^{n_i}]$ or as one of its elements e_i an integer e_i not relatively prime to the period b_i .

There are

$$(4) \quad \varphi \{ [p_1^{n_1}], \dots, [p_g^{n_g}]; b_1, \dots, b_h \}_{g+h} = \prod_{i=1, g} \varphi [p_i^{n_i}] \cdot \prod_{i=1, h} \varphi (b_i)$$

marks E of characteristic $\{ ; \}_{g+h}$ which are not divisors of zero. Here $\varphi[a] = a - 1$ and $\varphi(b)$ denotes as usual the number of positive integers less than and relatively prime to the positive integer b . The corresponding *multiplicative group* $MG \{ ; \}_{g+h}$ is an Abelian group of order $\varphi \{ ; \}_{g+h}$. For the general cyclid characteristic $\{ [p_1^{n_1}], \dots, [p_g^{n_g}] \}_g$ (3), this Abelian $MG \{ ; \}_g$ has the character $\{ p_1^{n_1} - 1, \dots, p_g^{n_g} - 1 \}_g$. For the particular cyclic character $\{ p^n \}_1$, this Abelian $MG \{ p^n \}_1$ has the order $\varphi(p^n) = p^{n-1}(p-1)$ and is cyclic** if p is any odd prime.

§ 4.

Explicit exhibition***) for every characteristic

$$\{ [p_1^{n_1}], \dots, [p_g^{n_g}]; p_1'^{n_1'}, \dots, p_h'^{n_h'} \}_{g+h}$$

of order t , where $p_i^{n_i} = 6m_i + 1$ and $p_j' = 6m_j' + 1$ ($i=1, \dots, g; j=1, \dots, h$),
of sextette-separations $\Sigma_{m,0} | H_{t=6m+1} \{ ; \}_{g+h}$.

For every order $t = 6m + 1$ in which every prime factor p of the form $p = 6k + 5$ enters an even number of times and for every Abelian group H_t of that order in whose invariant-character (Intr. (1)) these primes enter always with exponent 1 there is at least one characteristic $\{ ; \}_{g+h}$ of the form in question. There is (essentially) only one such characteristic if and only if t contains its every prime of the form $6k + 5$ exactly twice and in the invariant-character of H_t every prime of the form $6k + 1$ enters at most once with the exponent 1.

*) We write

$1 = \{1, \dots, 1; 1, \dots, 1\}, \quad -1 = \{-1, \dots, -1; -1, \dots, -1\}.$

**) Dirichlet-Dedekind, *Zahlentheorie*, fourth edition, § 128.

***)) In terms of primitive roots of Galois fields and of primitive congruence-roots of prime-power moduli.

For the marks of such a characteristic $\{; \}_{g+h}$ we proceed to effect a sextette-separation $\Sigma_{m,0} | H_{t=6m+1} \{; \}_{g+h}$.

The case: $g = 1, h = 0$: $\{[p^n]\}_1$ ($t=p^n=6m+1$).

If $n = 1$, the cyclid group $H_t\{[p^n]\}_1 = H_t\{p\}_1$ is cyclic, and we have Mr. Netto's cyclic $\Delta_{t=p=6m+1}$ (Intr. (1)) as a basis of generalization. In fact, the generalization is — from our present Galois field standpoint — immediate.

The characteristic $\{[p^n]\}_1$ has as its corresponding multiplicative-group $MG\{[p^n]\}_1$ (§ 3) the cyclic group $G_{t-1=p^n-1=6m}$ of order $\varphi[p^n]=6m$. This contains a sub-group G_6 of order 6. With respect to this G_6 the $6m$ elements of the G_{6m} separate into m sextettes.

Correspondingly, the $t-1=6m$ marks $E=\delta$ ($\delta \neq 0$) of the $GF[p^n=t]$ separate into m sextettes. This is our desired sextette-separation $\Sigma_{m,0} |$ cyclid $H_{t=p^n=6m+1} \{[p^n]\}_1$. The fundamental sextette of type 1^0 (§ 1, (15), (16)) is

$$(1) \quad \Sigma_1 | H_t^* = \begin{bmatrix} \tau^2 & \tau^4 & \tau^6 = +1 \\ \tau^5 = -\tau^2 & \tau = -\tau^4 & \tau^3 = -1 \end{bmatrix},$$

where ϱ is a primitive root of the $GF[p^n]$ and $\tau = \varrho^m$, so that $\varrho, \tau, \tau^2, \tau^3$ are primitive roots of the respective equations $x^{6m}-1=0$, $x^6-1=0$, $x^3-1=0$, $x^2-1=0$, and $\tau^2 + \tau^4 + \tau^6 = 0$ since the roots of the equation $x^3-1=0$ are τ^2, τ^4 and τ^6 . The remaining sextettes have the form

$$(2) \quad \Sigma_1^{(\delta)} | H_t^* = \begin{bmatrix} \delta \tau^2 & \delta \tau^4 & \delta \tau^6 \\ \delta \tau^5 & \delta \tau & \delta \tau^3 \end{bmatrix} \quad (\delta \neq 0).$$

The case: $g = 0, h = 1$: $\{p^n\}_1$ ($p=6m'+1, t=p^n=6m+1$).

The cyclic character $\{p^n\}_1$ has for its multiplicative-group $MG\{p^n\}_1$ (§ 3) the cyclic group $G_{\varphi(p^n)=p^n-1(p-1)=6m'p^{n-1}}$. This contains a sub-group G_6 of order 6. With respect to this G_6 the $6m'p^{n-1}$ elements of the $G_{6m'p^{n-1}}$ separate into $m'p^{n-1}$ sextettes.

Correspondingly, the $\varphi(p^n)=6m'p^{n-1}$ marks $\{e\}$ not divisors of zero of the character $\{p^n\}_1$ separate into $m'p^{n-1}$ sextettes of type 1^0 (§ 1, (15), (16)). The fundamental sextette has the form (1) where now $\tau = \varrho^{m'p^{n-1}}$ where ϱ is a primitive root (mod. p^n); this sextette

has the type 1^0 since*) $\tau^3 \equiv -1$ and $\tau^2 + \tau^4 + \tau^6 \equiv 0 \pmod{p^n}$. The remaining sextettes obtained by multiplication obviously have the type 1^0 .

The $p^n - 1$ marks e ($e \neq 0$) of the cyclic character $\{p^n\}_1$ separate into n sets according to the greatest common divisor $[e, p^n]$ of e and p^n .

We have just separated the set $[e, p^n] = 1$ into sextettes of type 1^0 .

If we similarly separate the set $[e, p^{n'}] = 1$ of the character $\{p^{n'}\}_1$ into sextette of type 1^0 ($n' < n$), and then multiply by $p^{n-n'}$, we shall have a sextette-separation of the set $[e, p^n] = p^{n-n'}$.

The n sextette-separations so obtained for the sets

$$[e, p^n] = p^{n-n'} \quad (n' = 1, \dots, n)$$

taken together constitute the sextette-separation $\Sigma_{m,0} | H_i^* =_{p^n} 6m+1$.

The general case: $g = \text{any}$, $h = \text{any}$:

$$\{[p_1^{n_1}], \dots, [p_g^{n_g}]; p_1'^{n_1'}, \dots, p_h'^{n_h'}\}_{g+h}.$$

We consider first the marks

$$(3) \quad D = \{\delta_1, \dots, \delta_g; d_1, \dots, d_h\}$$

not divisors of zero.

The mark

$$(4) \quad Q = \{\tau_1, \dots, \tau_g; \tau_1', \dots, \tau_h'\}$$

where τ_i, τ_j' have the significations of the τ, τ of the two special cases just considered ($i = 1, \dots, g; j = 1, \dots, h$) is a root of the equation $x^6 - 1 = 0$. The six marks Q^k ($k = 1, \dots, 6$) are distinct and form a system closed under multiplication and division. Further, $Q^3 = -1$ and $Q^2 + Q^4 + Q^6 = 0$. Hence the sextette

$$(5) \quad \Sigma_1 | H_i^* = \begin{bmatrix} Q^2 & Q^4 & Q^6 \\ Q^5 & Q^1 & Q^3 \end{bmatrix}$$

is a sextette of type 1^0 (§ 1, (15), (16)). This $\Sigma_1 | H_i^*$ forms the

*) The second congruence requires proof.

The three roots of $x^3 - 1 \equiv 0 \pmod{p^n}$ are $l (= \tau^2)$, l^2 , and $l^3 (\equiv 1)$. We are to prove that $l + l^2 + l^3 \equiv l^2 + l + 1 \equiv 0 \pmod{p^n}$.

$$l^3 - 1 = (l-1)(l^2 + l + 1) \equiv 0 \pmod{p^n}.$$

Let n' be the highest power of p contained as a factor in $l-1$; $\therefore n' < n$. Then $l-1 \equiv 0 \pmod{p^{n'}}$ and $l^2 + l + 1 \equiv 0 \pmod{p^{n''}}$ where $n'' = n - n' > 0$. Hence $3l \equiv 0 \pmod{p^{n'''}}$ where n''' is the smaller of n'' and $2n'$. But, since $p = 6m+1 > 3$, $n''' = 0$. But $n'' > 0$. Hence $2n' = 0$ and $n' = n$. Hence indeed $l^2 + l + 1 \equiv 0 \pmod{p^n}$.

basis for a separation of the marks D (3) into sextettes of type 1⁰ of the form

$$(6) \quad \Sigma_1^{(D)} | H_t^* = \begin{bmatrix} D Q^2 & D Q^4 & D Q^6 \\ D Q^5 & D Q & D Q^3 \end{bmatrix}.$$

This appears at once by consideration of the corresponding multiplicative-group $MG \{ ; \}_{g+h}$.

Now we consider the $t-1$ marks E ($E \neq 0$)

$$(7) \quad E = \{ \varepsilon_1, \dots, \varepsilon_g; e_1, \dots, e_h \}.$$

We divide the marks ε_i of the $GF[p_i^{n_i}]$ into two sets according as ε_i is or is not the mark 0 ($i=1, \dots, g$) and the integers e_j of the character $\{p_j^{n_j}\}_1$ into n_j+1 sets according to the value of

$$[e_j, p_j^{n_j}] = p_j^{n_j - n_j''} \quad (n_j'' = 0, 1, \dots, n_j) \quad (j=1, \dots, h).$$

On the basis of these separations we effect a separation of the marks E into sets.

We consider a certain set of marks E having g' non-zero elements ε_i and h' non-zero elements e_j . These marks may be set in 1-1 correspondence with the marks D' not divisors of zero of the characteristic

$$(8) \quad \{ [q_1^{s_1}], \dots, [q_{g'}^{s_{g'}}]; q_1^{s_1''}, \dots, q_{h'}^{s_{h'}''} \}_{g'+h'} \quad (g'+h' \geq 1)$$

where $q_1^{s_1}, \dots, q_{g'}^{s_{g'}}$ denote certain g' of the $p_1^{n_1}, \dots, p_{g'}^{n_{g'}}$ and $q_1^{s_1''}, \dots, q_{h'}^{s_{h'}''}$ denote certain h' of the $p_1^{n_1}, \dots, p_{h'}^{n_{h'}}$ immediately determined by the set of marks E . This correspondence is invariant under addition and subtraction. The marks D' may be separated into sextettes of type 1⁰, as were the marks D (3). Whence, by the correspondence we have a sextette-separation of the set of marks E .

We have by these sextette-separations of the marks E of the various sets obtained a sextette-separation of the $t-1$ marks E ($E \neq 0$):

$$\Sigma_{m,0} | H_{t=6m+1}^*.$$

There are in all 2^{g+h} marks Q (corresponding to the various determinations of the τ_i, τ_j ($i=1, \dots, g, j=1, \dots, h$)) and 2^{g+h-1} fundamental sextettes $\Sigma_1 | H_t^*$ (5), and so 2^{g+h-1} such sextette-separations for the marks D (3). There are similarly 2^{g+h-1} sextette-separations of the marks E connected with (8).

Since there is no dependence between the partial separations

making up the complete separation $\Sigma_{m,0} | H_{t=6m+1}^*$ the number of such complete determinations exhibited here for every characteristic

$$\{[p_1^{n_1}], \dots, [p_g^{n_g}]; p_1'^{n_1'}, \dots, p_h'^{n_h'}\}$$

of the kind indicated in the caption of this § 4 increases very rapidly with the complexity of ℓ 's prime-factor composition.

Every separation $\Sigma_{m,0} | H_{t=6m+1}^*$ yields 2^m separations $\sigma_{m,0} | H_t^*$ and so $2^m \Delta_t | H_t^t$ each with the configuration-separation $Cf_{m,0} | H_t^t$.

The University of Chicago, April 10, 1897.