conics. The author states for example that every plane quintic can be regarded as conjugate to a line in an involution determined by a net of cubics, having a suitable number of fundamental points.

11. By the aid of parametric representation of the points on a non-singular plane cubic, Professor Emch discusses the collinearity of the 27 points of contact of tangents to the cubic from its 9 inflexions. He finds 81 lines containing each 3 such points, and 81 other lines connecting 2 contact points with an inflexion.

12. Professor Halsted gave a brief outline of "intrinsic spherics", or spherical trigonometry independent of the parallel postulate, and advocated from a pedagogical standpoint the introduction of the sphere as two-dimensional figure into elementary geometry, instead of the use of the three-dimensional globe.

13. The problem of determining all algebraic minimal surfaces was solved analytically by Weierstrass in 1866 (see his collected works, volume 3, pages 39–52). Darboux, in his Théorie générale des surfaces, part 1, No. 221, has shown that such surfaces can always be generated by the translation of an algebraic curve. This shows that the function $F(s)$ used in the formulas of Weierstrass must be algebraic. Professor Hancock proposes as a problem next to be attacked the question of determining all those minimal surfaces which are not themselves algebraic, but contain a sheaf of algebraic curves.

H. S. WHITE.

EVANSTON, ILL.,
March, 1905.

ON THE USE OF HYPERCOMPLEX NUMBERS IN CERTAIN PROBLEMS OF THE MODULAR GROUP.

BY DR. J. W. YOUNG.

(Read before the American Mathematical Society, September 17, 1904.)

THE following discussion connects two subjects which have hitherto been considered apart, and indicates a method of attacking certain modular group problems which seems susceptible of further elaboration.

By the modular group Γ, I mean the totality of substitutions $v(z) = (\alpha z + \beta)/(\gamma z + \delta)$, where α, β, γ, δ are integers satisfying the relation $\alpha\delta - \beta\gamma = 1$. It is an old problem to define *arithmetically* the subgroups of Γ; except for the cyclic and so-called congruence subgroups it is as yet an unsolved problem.* In what follows I indicate a method of attack on such problems which seems not to have been employed hitherto. By applying this method in a special case I am led to the definition of the cyclic subgroups of Γ and of congruence groups corresponding to cyclic quotient groups, the latter in an explicit form not before given.

The method referred to is as follows: Let E be a commutative hypercomplex number system with a modulus and let a, b, c, d be numbers of E such that $ad - bc$ is neither zero nor a divisor of zero. Then the substitution $w(z) = (az + b)/(cz + d)$ has a unique inverse, $w^{-1}(z) = (dz - b)/(-cz + a)$.

If then for v we place the totality of substitutions of Γ, the totality $w^{-1}vw$ will form a group simply isomorphic with Γ, whose coefficients are numbers of E. This may be called a hypercomplex representation of Γ, and it seems not unreasonable to suppose that a suitably chosen representation of this kind may bring to light relations very difficult to obtain with the ordinary representation.

To illustrate the method, I propose to apply it in a simple case, in which it leads in a direct and natural manner to the explicit arithmetic definitions of certain congruence subgroups.

Let E be the two-unit system, whose units, e_1, e_2 combine as follows:

$$e_1^2 = e_1,\ e_1e_2 = e_2e_1 = e_2,\ e_2^2 = 0.$$

Also let w be

$$w(z) = \frac{(e_1 + \frac{1}{2}ae_2)z + be_2}{ce_2z + e_1 - \frac{1}{2}ae_2},$$

whose determinant is e_1; a, b, c being any real numbers. If we place

* By "arithmetic" definition is here meant one by means of an explicit arithmetic condition on the coefficients. Subgroups, neither cyclic nor of the congruence character, have been defined by conditions on the quotients in the continued fraction representation of the substitutions by Fricke, *Math. Ann.*, vol. 30 (1880), p. 345, and the author, *Trans. Am. Math. Soc.*, vol. 5 (1904), p. 88.

$$v(z) = \frac{az+\beta}{\gamma z+\delta}, \quad w^{-1}vw = v' = \frac{a'z+\beta'}{\gamma' z+\delta'},$$

we obtain after a short calculation

$$\alpha' = \alpha e_1 + [c\beta - b\gamma]e_2 \qquad \beta' = \beta e_1 - [a\beta - b(\alpha-\delta)]e_2$$

$$\gamma' = \gamma e_1 + [a\gamma - c(\alpha-\delta)]e_2 \qquad \delta' = \delta e_1 - [c\beta - b\gamma]e_2.$$

Now it is clear that the totality of substitutions v', in which the coefficients of e_2 are all zero, form a subgroup. In this way we find that the conditions

$$\text{(A)} \quad a\beta - b(\alpha-\delta) = 0, \quad a\gamma - c(\alpha-\delta) = 0, \quad c\beta - b\gamma = 0,$$

(of which the last is a result of the other two, if $a \neq 0$) define a subgroup of Γ, for any set a, b, c. It is easy to show that *the subgroup defined by* (A) *is always cyclic, and any complete* * *cyclic subgroup of* Γ *can be defined in this way by a proper choice of* a, b, c. It hardly seems worth while to give the details of the proof.

Again, if a, b, c, n are integers, it is evident that the totality of substitutions for which

$$\text{(B)} \quad a\beta - b(\alpha-\delta) \equiv 0, \quad a\gamma - c(\alpha-\delta) \equiv 0, \quad c\beta - b\gamma \equiv 0$$

form a subgroup. Suppose all the substitutions of Γ to be reduced mod n, and denote the resulting group of finite order $\mu(n)$ by $G_{\mu(n)}$. In case n is a prime p, it is easy to show that, for the different values of a, b, c, (B) gives the totality of cyclic subgroups of $G_{\frac{1}{2}p(p^2-1)}$.

The method of proof will be made manifest by considering in detail the cases in which $a \equiv 0 \bmod p$. We find then †

(i) If $b \not\equiv 0$, B may be written

$$\alpha \equiv \delta, \quad \gamma \equiv \lambda\beta$$

where $b\lambda \equiv c$. The relation $\alpha\delta - \beta\gamma \equiv 1$, now becomes

$$\alpha^2 - \lambda\beta^2 \equiv 1.$$

Every solution of this congruence gives a substitution of the subgroup of $G_{\frac{1}{2}p(p^2-1)}$ in question; the number of incongruent

* By "complete" I mean not contained in any other cyclic subgroup.
† All congruences that follow are to be taken mod p.

solutions gives twice the order of the subgroup. Jordan * has given the number of solutions as follows: When $\lambda \not\equiv 0$, if λ is a quadratic residue of p, there are just $p-1$ solutions; if λ is a quadratic non-residue of p, there are just $p+1$ solutions. When $\lambda \equiv 0$, there are evidently just $2p$ solutions. For the different values λ, mod p, we obtain then

$$1 \text{ subgroup of order } p,$$
$$\tfrac{1}{2}(p-1) \text{ subgroups of order } \tfrac{1}{2}(p-1),$$
$$\tfrac{1}{2}(p-1) \text{ subgroups of order } \tfrac{1}{2}(p+1).$$

(ii) If $b \equiv 0$, $c \not\equiv 0$ we evidently obtain a single subgroup of order p.

The cases in which $a \not\equiv 0$ are treated similarly. By the transformation $\alpha = \tau + \nu$, $\delta = \tau - \nu$, the determination of the order and the number of the corresponding subgroups is made to depend on the same type of congruence as before. We find here $(a \not\equiv 0)$

$$p-1 \text{ subgroups of order } p,$$
$$\tfrac{1}{2}(p^2+1) \text{ subgroups of order } \tfrac{1}{2}(p-1),$$
$$\tfrac{1}{2}(p-1)^2 \text{ subgroups of order } \tfrac{1}{2}(p+1).$$

All the subgroups thus far obtained are clearly different, and by collecting results we have in all

$$p+1 \text{ subgroups of order } p,$$
$$\tfrac{1}{2}(p^2+1) + \tfrac{1}{2}(p-1) = \tfrac{1}{2}p(p+1) \text{ subgroups of order } \tfrac{1}{2}(p-1),$$
$$\tfrac{1}{2}(p-1)^2 + \tfrac{1}{2}(p-1) = \tfrac{1}{2}p(p-1) \text{ subgroups of order } \tfrac{1}{2}(p+1).$$

This by a well-known theorem† is the total number of subgroups of these orders contained in $G_{\frac{1}{2}p(p^2-1)}$, and they are all cyclic. The results may be stated as follows:

The three pairs of congruences

$$\left.\begin{matrix}\alpha \equiv \delta \\ \gamma \equiv \lambda\beta\end{matrix}\right\}, \quad \left.\begin{matrix}\alpha \equiv \delta \\ \beta \equiv 0\end{matrix}\right\}, \quad \left.\begin{matrix}\beta \equiv \mu(\alpha-\delta) \\ \gamma \equiv \nu(\alpha-\delta)\end{matrix}\right\}, \text{ mod } p \ [\lambda, \mu, \nu \text{ integers}]$$

* Traité des substitutions, p. 156.

† Klein-Fricke, Elliptische Modulfunctionen, vol. I, p. 434.

define three mutually exclusive sets of subgroups, and these three together constitute the totality of the cyclic subgroups of $G_{\frac{1}{2}p(p^2-1)}$. *Their number is seen to be* $p^2 + p + 1$. *The order of the subgroup is* p *when* $\lambda \equiv 0$, *when* $4\mu\nu + 1 \equiv 0$, *and in the second pair; the order is* $\frac{1}{2}(p-1)$ *when* λ *or* $4\mu\nu + 1$ *is a quadratic residue of* p; *the order is* $\frac{1}{2}(p+1)$ *when* λ *or* $4\mu\nu + 1$ *is a non-residue of* p.

This explicit form of definition seems to be new, and on account of its simplicity may be of interest.

NORTHWESTERN UNIVERSITY,
September, 1904.

EXTENSION OF A THEOREM DUE TO SYLOW.

BY PROFESSOR G. A. MILLER.

(Read before Section A of the American Association for the Advancement of Science, Philadelphia, December 29, 1904.)

EVERY group G of order p^m, p being any prime number, contains at least p invariant operators. This fundamental theorem, due to Sylow,* is included in the following: *Every non-abelian group of order* p^m *contains at least* p *invariant commutator operators, and its commutator quotient group* † *is always non-cyclic.* In this connection it seems desirable to prove the following closely related theorems: It is possible to construct a non-abelian group having any arbitrary abelian group as a commutator quotient group. Every non-cyclic abelian group of order p^α is the commutator quotient group of some non-abelian group of order p^m.

The first part of the theorem in italics may be proved as follows: Let H represent the subgroup of G which is composed of its p^β invariant operators and let H_1 represent an invariant subgroup of order $p^{\beta+1}$ which includes H.‡ Any operator s of G which is not commutative with all the operators of H_1 transforms H_1 into a simple isomorphism with itself such that each of the operators of H corresponds to itself. Since H_1 is

* Sylow, *Math. Annalen*, vol. 5 (1872), p. 584.

† It seems convenient to speak of the quotient group corresponding to the commutator subgroup as the commutator quotient group.

‡ Every invariant subgroup of a group of order p^m is included in a larger invariant subgroup of arbitrary order less than p^m.