HIGHER IRREDUCIBLE CONGRUENCES.

BY DR. LEONARD E. DICKSON.

1. Comprising the theory of congruences irreducible modulo p (p=prime), we may establish a theory of quantics belonging to and irreducible in the Galois Field* of order p^n. The existence-proofs of an irreducible congruence modulo p for every degree due to Galois†, Serret‡ and Jordan§ may each be readily generalized to prove that for every m, n and p (=prime) there exists a quantic of degree m belonging to and irreducible in the $GF[p^n]$, or to give a notation, an $IQ[m, p^n]$.

As we may define the $GF[p^{nm}]$ either by an $IQ[m, p^n]$ or by an $IQ[mn, p]$, a theory of the former quantics can often be of practical value in setting up and working in the $GF[p^{nm}]$. In certain investigations (like many due to Jordan), where it seems preferable to use the concrete form of the $GF[p^{nm}]$ (viz., use the quantics built on a Galois imaginary), it may often be simpler, especially if generalizing, to use a defining $IQ[m, p^n]$, keeping the reference $GF[p^n]$ in its abstract form. The quantics then occurring will be of degree $\leqq m-1$ instead of degree $\leqq mn-1$.

The first part of the theory given here runs parallel with the beautiful developments of Serret, Cours D'Algèbre Supérieure, Section III, Chapter III (§360 being a marked exception; compare §16 below), so I content myself with enunciating the more important generalized theorems. As it is quite otherwise with Chapter IV, I give in detail the corresponding developments. The concluding pages in Serret, 199–211 would require a method of attack entirely different (even if capable of generalization).

2. THEOREM. If $F(\xi)$, belonging to and irreducible in the $GF[p^n]$, divides the product $\varphi(\xi) \cdot \chi(\xi)$, it divides one factor at least.

Corollary. The decomposition of a quantic into irreducible factors in the $GF[p^n]$ can be effected in a single way.

3. THEOREM. $F(\xi)$, an $IQ[m, p^n]$, divides the function

* I use the abstract form of the theory due to Galois. See MOORE, Proceedings of the Congress of Mathematics of 1893, at Chicago; also, BOREL et DRACH, Théorie des Nombres et Algèbre supérieure, 1895.

† GALOIS, "Sur la théorie des nombres," *Bulletin des Sciences mathématiques* de M. Férussac, 1830; reprinted in *Journal de mathématiques pures et appliquées*, 1846.

‡ Cours d'Algèbre supérieure, vol. 2, pp. 122–211.

§ Traité des Substitutions, § 21.