Les surfaces de la seconde classe ont les invariants

$$p_g = \frac{p\,(p-1)}{2}, \quad p_a = \frac{p\,(p-1)}{2} - p, \quad p^{(1)} = (4p-5)\,(p-2),$$

donc on a

$$p_g - 2\,(p_a + 2) = -\frac{(p-2)\,(p-3)}{2} - 1,$$

c'est à dire un nombre négatif.

6. Nous avons dit dans le n⁰ 1. que la limite inférieure de $p^{(1)}$ est atteinte dans le cas des courbes canoniques hyperelliptiques. Plus généralement, si la série caractéristique du système canonique est telle que tous ses groupes passant par un point de la courbe passent par $k-1$ autres points, on a l'inégalité

$$p^{(1)} \geqq k\,(p_g - 2 + \delta_k) + 1,$$

δ_k désignant encore le défaut de la série caractéristique du système canonique linéaire. Mais dans le cas général, où tous les groupes contenant un point ne contiennent pas nécéssairement d'autres points, on a d'après M. Castelnuovo *) l'inégalité

$$p^{(1)} \geqq 3\,(p_g - 2 + \delta_k). \tag{10}$$

Nous avons alors

$$3p_g - 6 \leqq 12p_a + 13 - 4\,(p_g - p_a - 3),$$

donc on a l'inégalité

$$p_g \leqq \frac{16}{7}\,p_a + \frac{31}{7}. \tag{11}$$

Remarquons que si le défaut δ_k est égal à $p_g - p_a$, on a

$$p_g \leqq \frac{19}{10}\,p_a + \frac{31}{10},$$

mais on a supposé $p_g \geqq 2\,(p_a + 2)$. Donc la série caractéristique du système canonique linéaire ne peut pas dans ce cas avoir le défaut maximum.

*) M. Castelnuovo a bien voulu nous signaler cette inégalité importante de son Mémoire: „Osservazioni intorno alla geometria sopra una superficie. Nota II". Rendiconti del Reale Istituto Lombardo Ser. II. Vol. XXIV. 1891. Qu'il nous soit permis de lui exprimer ici nos plus vifs remerciments.

G. A. MILLER.

Gauss's Lemma and some related group theory.

(Lemmat Gaussa i niektóre twierdzenia dotyczące teoryi grup).

According to Gauss's Lemma any number m, which is not divisible by the prime number p, is a quadratic residue or a quadratic non-residue of p accordnig as the series

$$m, \quad 2m, \quad \ldots., \quad \frac{p-1}{2}\,m \tag{A}$$

includes an even or an odd number of numbers whose least absolute residues (mod p) are negative. We shall give a proof of this lemma, which is explicitly based upon well known properties of abelian groups and will suggest various more general statements. The main objects of this note are to exhibit, in an elementary manner, the setting of this lemma in the theory of abelian groups and to show how readily its proof may be deduced from this theory.

Let G be any abelian group of order g, and let

$$s_1, \quad s_2, \quad \ldots.., \quad s_g$$

be the operators of G. Consider the set of operators

$$s_1^n, \quad s_2^n, \ldots.., \quad s_g^n \tag{B}$$

and let d be the highest common factor of g and n. Since d divides g it results that G involves a subgroup of order d, and that the total number of operators of G whose orders divide d constitute a group H of order h. As the order of a subgroup divides the order of the group it results that $g = kh$, $k \geqq 1$. The subgroup H is composed of all the operators of G which reduce to the identity in (B). Hence all the operators of G may be divided into g/h sets which satisfy the condition that all the operators of each set have the same n^{th} power, while any two operators belonging te two different sets have different n^{th} powers. All the operators of such a set may be obtained by multiplying any operator of the set by all the operators of H, and the distinct operators of (B) constitute a subgroup of index h under G.

A set of operators of a group will be called a complete set for the n^{th} powers if the n^{th} powers of these operators give all the different n^{th} powers of the operators of the group and if no two operators of the set have the same n^{th} power. Suppose that the operators

$$t_1, \quad t_2, \quad \dots\dots, \quad t_\lambda \qquad\qquad \lambda = g/h$$

represent a complete set for the n^{th} power of the abelian group G. One and only one such operator corresponds to each operator of the quotient group G/H, and hence such a set can be selected in h^λ different ways. A necessary and sufficient condition that a complete set for the n^{th} powers of G can be so selected that the operators of the set constitute a group is that λ and n are relatively prime.

Since there is a (1, 1) correspondence between $t_1, t_2, \dots, t_\lambda$ and the operators of G/H it results that the products

$$t_1 t_\alpha, \quad t_2 t_\alpha, \quad \dots, \quad t_\lambda t_\alpha$$

constitute a complete set for the n^{th} powers of G whenever t_α is any operator of G. That is, the products obtained by multiplying all the operators of a complete set for the n-th powers of an abelian group by any operator of the group constitute a complete set for the n^{th} powers. The h sets obtained by letting t_α represent successively all the operators of H are called complementary sets. These complementary sets involve every operator of G once and only once, and every complete set for n^{th} powers contains one and only one of the h operators $t_\lambda H$ for every value of α from 1 to λ.

The continued product of the operators in every possible complete set for the n^{th} powers of G corresponds to the same operator in G/H since the continued product of all the operators of an abelian group is its operator of order two if the abelian group has only one such operator, and this continued product is the identity in all other cases[1]. In fact the operators in exactly

$h^{\lambda-1}$ of the complete sets for n-th powers of G have the same continued product. Since

$$t_1 t_\alpha . t_2 t_\alpha . \dots . t_\lambda t_\alpha = t_1 t_2 \dots . t_\lambda . t_\alpha^\lambda$$

it results that the complete set for the n-th powers which is obtained by multiplying each operator of such a set by t_α has the same continued product as the original set whenever $t_\alpha^\lambda = 1$, and only then.

Before going further with these general developments it may be convenient to apply some of these results in a proof of Gauss's Lemma. In this special case we consider the cyclic group G of order $p-1$ which is generated by the numbers

$$1, \quad 2, \dots, \quad p-1,$$

when they are combined by multiplication (mod. p). If we let $n=2$ it follows that $d=2$ and $h=2$. The subgroup H is composed of 1 and $p-1=-1$, and the operators of G/H are the quadratic residues of p. These operators are the squares of any one of the $2^{\frac{p-1}{2}}$ complete sets for squares of G. Two such complementary sets are evidently as follows:

$$1, \qquad 2, \dots, \qquad \frac{p-1}{2},$$

$$-1, \quad -2, \dots, \quad -\frac{p-1}{2}.$$

The products obtained by multiplying (mod p) all the operators of a set by any one α of the numbers $1, 2, \dots, p-1$ must be either in the set or in its complement. As the continued product of the numbers in the new set is equal to the continued product of the numbers in the original set multiplied by α^{p-1}, it results that this continued product is the same for both of the sets, when α is a quadratic residue of p and only then. As the numbers of a set and its complement differ only with respect to sign, these continued product will also be the same or different as an even or an odd number of the given products are in the complementary set. This completes a proof of the theorem: If all the numbers in any given complete set for squares (mod p) of the numbers $1, 2, \dots, p-1$ are multiplied by any one α of the latter set, then α is a quadratic residue or a quadratic non-residue of p as an even or an odd number of these products are found in the set which is complementary to the given set for squares.

[1] Zsigmondy, Monatshefte für Mathematik und Physik, vol. (1896), p. 219.

If we select for the complete set for squares the numbers $1, 2, \dots, \frac{p-1}{2}$ the preceding theorem furnishes a proof of Gauss's Lemma. If we select for this set the numbers $\frac{p+1}{2}, \dots, p-2, p-1$, and if we let $\alpha=2$, the given products are composed of the odd numbers in the series $1, 2, \dots, p-1$. Hence 2 is a quadratic residue or a quadratic non-residue of p according as the number of odd numbers which are less than $p/2$ is even or odd; that is, according as p is of the form $8n \pm 1$ or of the form $8n \pm 3$.

The quadratic character of α as regards a prime modulus may also be determined as follows: Since an operator and its inverse are of the same order and have the same properties as regards powers, it results that 2 and $\frac{p+1}{2}$ have the same quadratic character (mod p). If we multiply $\frac{p+1}{2}$ by the even numbers of the set

$$1,\ 2, \dots, \frac{p-1}{2},$$

we evidently obtain numbers of this set (mod p), while we obtain only numbers of the complementary set if we multiply $\frac{p+1}{2}$ by the odd numbers of the given set. In fact

$$(2k-1)\frac{p+1}{2} = kp + k - \frac{p}{2} - \frac{1}{2} = \frac{p}{2} + k - \frac{1}{2} \pmod{p}.$$

As $2k-1 \leqq \frac{p-1}{2}$, it results that $(2k-1)\frac{p+1}{2}$ is in the set which is complementary to $1, 2, \dots, \frac{p-1}{2}$ and hence $\frac{p+1}{2}$ is a quadratic residue or a quadratic non-residue of p as $\left[\frac{p+1}{4}\right]$ is even or odd.

A necessary and sufficient condition that an operator of a cyclic group is a non-square is that its order is divisible by the highest power of 2 which divides the order of the cyclic group. Hence it results that the index of 2 (mod p) is divisible by 4 whenever p is of the form $8n-3$, and this index is always divisible by 2 when p is of the form $8n+3$. In particular: 2 is a primitive root of all primes of the form $4q+1$, q being any odd prime; and it is also a primitive root of all primes of the form $2q+1$ whenever q is of the form $4n+1$. When q is of the form $4n-1$ it is clear that -2 is a primitive root of every prime of the form $2q+1$, since 2 is a quadratic residue and -1 is a quadratic non-residue of each of these primes. Hence the known theorem: 2 is a primitive root of all primes which are of the form $4q+1$, q being an odd prime, and also of all primes of the form $2q+1$ when q is an odd prime of the form $4n+1$; when q is an odd prime of the form $4n-1$ and $2q+1$ is a prime, then -2 is a primitive root of this prime.

If a prime is of the form $6q+1$ and the number of odd integers $\leqq 3q$ is odd, then 2 is a non-residue of $6q+1$ and hence it belongs either to exponent $2q$ or to exponent $6q$. In the latter case (2) is a primitive root and in the former case $2^h \equiv -1 \pmod{6q+1}$. Hence it results that when $6q+1$ is a prime of the form $8n+3$ it has 2 for a primitive root unless $2^p \equiv -1$ (mod $6q+1$). In a similar manner we see that when $6q+1$ is a prime of the form $8n-1$ it has -2 for a primitive root unless $2^p \equiv 1$ (mod $q+1$).