Roots of Unity over Large Algebraic Fields*

Moshe Jarden

Contents

Introduction	109
1. The Haar measure of a Galois group	111
2. Jordan totient function	113
3. Lower bounds for $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)]$	115
4. The values of the function $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)]$	117
5. The divergence of $[\tilde{\mathbb{Q}}(\sigma)_n : \tilde{\mathbb{Q}}(\sigma)]$	118
6. Roots of unity over finite fields	120
7. Roots of unity over $\tilde{\mathbb{F}}_p(\sigma)$	122
8. Fields of finite type	123
9. Points of finite order on linear algebraic groups	124
References	126

Introduction

Consider a field L of characteristic $p \geqq 0$. Then for every positive integer n which is not divisible by p there exists in the separable closure of L, L_s, a primitive root of unity of order n, which is, by definition, an element ζ_n for which n is the smallest positive integer such that $\zeta_n^n = 1$. The adjunction of ζ_n to L gives rise to a Galois extension L_n of L and there is a canonical monomorphism of the Galois group $\mathcal{G}(L_n/L)$ into $(\mathbb{Z}/n\mathbb{Z})^*$ given by $\tau \mapsto i \pmod n$ where i represents the congruence class modulo n for which $\tau(\zeta) = \zeta^i$. It follows that $[L_n : L]$ divides $\varphi(n)$, where φ is the Euler totient function. If $L = \mathbb{Q}$, then $[L_n : L] = \varphi(n)$ for every n. On the other hand if L is separably closed then $[L_n : L] = 1$. If L is an intermediate field, $[L_n : L]$ can obtain any value which divides $\varphi(n)$.

We consider in this note a ground field K of finite type, (i.e. finitely generated over its prime field) and study the function $[K_s(\sigma)_n : K_s(\sigma)]$, where $(\sigma) = (\sigma_1, \ldots, \sigma_e)$ is an e-tuple of elements of $\mathcal{G}(K_s/K)$ and $K_s(\sigma)$ is its fixed field in K_s. We find that the function $[K_s(\sigma)_n : K_s(\sigma)]$ obtains some regularity if we neglect for every e, a subset of e-tuples (σ) of Haar measure 0. We find further that in the case $e = 1$ the fields $K_s(\sigma)$ are much more closed to K_s then in the case $e \geqq 2$, in the sense that for $e = 1$ $K_s(\sigma)$ contains infinitely many roots of unity, whereas in the case $e \geqq 2$ $K_s(\sigma)$ contains only finitely many. Moreover, we prove the following theorem:

Let K be a field of finite type. Let $e \geqq 1$. Then the following statements hold for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$:

A) If $e = 1$ then for every positive integer d there exist infinitely many primes l such that $[K_s(\sigma)_l : K_s(\sigma)] = d$.

B) If $e \geqq 2$ then $\lim_{\substack{n \to \infty \\ p \nmid n}} [K_s(\sigma)_n : K_s(\sigma)] = \infty$.

---

* This work was done while the author was at Heidelberg University.

The fundamental fact that sharpens the differences between the cases $e=1$ and $e=2$ is that the harmonic series Σn^{-e} diverges for $e=1$ and converges for $e>1$. Note that no difference was found between these cases with respect to other important questions. Thus, it was proved in [9, Theorem 2.5] and in 4, Theorem 9.1] that if K is not finite then for all $e \geqq l$ and for almost all $(\sigma) \in \mathscr{G}(K_s/K)^e$ $K_s(\sigma)$ has the following two properties:

(a) Every absolutely irreducible variety defined over $K_s(\sigma)$ has a $K_s(\sigma)$-rational point.

(b) For every abelian variety A defined over $K_s(\sigma)$ the rank of the abelian group $A(K_s(\sigma))$ of all $K_s(\sigma)$-rational points of A is infinity.

The reason for the distinction of the results may be that Properties (a) and (b) have geometrical nature, whereas the question of roots of unity is more arithmetical.

It is essential to prove the Theorem only for the prime field K of each characteristic. We distinguish between two cases: $p=0$ and $p>0$. In the first case $K=\mathbb{Q}$. In this case we can say more about the roots of unity of prime order.

Almost all $(\sigma) \in \mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ have the following properties:

C) For every $\theta < \dfrac{e-1}{e+1}$ and for all but finitely many primes l

$$[\tilde{Q}(\sigma)_l : \tilde{Q}(\sigma)] > (l-1)^\theta .$$

Thus, the rate of divergence of $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)]$ increases as e increases.

D) For every positive integer d there exist infinitely many primes $l \equiv 1 \pmod{d}$ such that $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = \dfrac{l-1}{d}$.

The analogue of C) for prime characteristic seems to be false since it clashes with the hypotheses that there exist infinitely many Mersenne's primes. The analogue of D) for characteristic p includes Artin's conjecture on the existence of infinitely many primes l for which p is a primitive root, so that it is very difficult to establish it.

In Section 9 we apply B) to linear algebraic groups and prove the following Theorem:

E) Let K be a field of finite type and let $e \geqq 2$. Then almost all $(\sigma) \in \mathscr{G}(K_s/K)^e$ have the following property:

For every linear algebraic group G defined over $K_s(\sigma)$ the order of the torsion $K_s(\sigma)$-rational points of G is bounded.

The author wishes to express his indebtedness to P. Roquette and W. D. Geyer for their encouragement and advise.

Notation

We use lower case latin letters to denote rational integers. The letters e, l, p will always stand for a positive integer, a prime and the characteristic of the field in question respectively. $\mathbb{F}_q$ = the field with q elements. $\mathbb{Q}$ = the field of rational numbers. $\mathbb{Z}$ = the ring of integers. $\hat{\mathbb{Z}}_l$ = the ring of l-adic integer, $\hat{\mathbb{Z}} = \prod_l \hat{\mathbb{Z}}_l$. ζ = the Riemann Zeta-function.

If K is a field then K_s and $\tilde{K}$ stand for the separable closure and the algebraic closure of K. If $M \supseteq L \supseteq K$ is a tower of Galois extensions and $A \subseteq \mathcal{G}(M/K)$ then $A|L$ is the set of all restrictions $\sigma|L$ of the elements $\sigma \in A$. If $(\sigma) \in \mathcal{G}(M/K)^e$ then $L(\sigma)$ is the fixed field of $(\sigma_1, \ldots, \sigma_e)$ in L. If $\sigma_1, \ldots, \sigma_e$ are e elements of a pro-finite group G then $\langle \sigma \rangle = \langle \sigma_1, \ldots, \sigma_e \rangle$ denotes the closed subgroup generated by $\sigma_1, \ldots, \sigma_e$.

If α is an element of a group G then $\operatorname{ord}\alpha$ is the order of α in G. If a, n are relatively prime then $\operatorname{ord}_n a$ is the order of a modulo n.

$|A|$ = the cardinality of the set A.

1. The Haar Measure of a Galois Group

Let K be a field and let M be a Galois extension of K. It is well known that the Galois group $\mathcal{G}(M/K)$ is compact with respect to its Krull topology. There is therefore a unique way to define a Haar measure μ on the Borel field of $\mathcal{G}(M/K)$ such that $\mu(\mathcal{G}(M/K)) = 1$. If L is a finite separable extension of K contained in M, then $\mu(\mathcal{G}(M/L)) = [L:K]^{-1}$, if L is an infinite extension then $\mu(\mathcal{G}(M/L)) = 0$. We complete μ by adjoining to the Borel field all the subsets of zero sets and denote the completion also by μ. More generally, for a positive integer e, we consider the product space $\mathcal{G}(M/K)^e$ and again denote by μ the appropriate completion of the power measure. It coincides with the completion of the Haar measure of $\mathcal{G}(M/K)^e$.

Our main measure theoretic device in this note is expressed in the following Lemma.

Lemma 1.1 (Borel-Cantelli). *Let $\{E_i\}_{i=1}^{\infty}$ be a sequence of measurable sets in a probability space (X, μ). Put*

$$\bar{E} = \{x \in X \mid x \text{ belongs to infinitely many } E_i's\} = \bigcap_{n=1}^{\infty} \bigcup_{i=n}^{\infty} E_i ,$$

$$\underline{E} = \{x \in X \mid x \text{ belongs to almost all the } E_i's\} = \bigcup_{n=1}^{\infty} \bigcap_{i=n}^{\infty} E_i .$$

Then

a) *If the sequence $\{E_i\}_{i=1}^{\infty}$ is independent and if $\sum_{i=1}^{\infty} \mu(E_i) = \infty$ then $\mu(\bar{E}) = 1$.*

b) $\sum_{i=1}^{\infty} \mu(E_i) < \infty \Rightarrow \mu(\bar{E}) = 0$.

c) $\sum_{i=1}^{\infty} \mu(X - E_i) < \infty \Rightarrow \mu(\underline{E}) = 1$.

Proof. Assume first that the sequence $\{E_i\}$ is independent and that $\Sigma \mu(E_i) = \infty$. Then $\prod_{i=n}^{\infty} (1 - \mu(E_i)) = 0$ for every $n \geq 1$. Hence

$$\mu\left(\bigcup_{i=n}^{\infty} E_i\right) = 1 - \mu\left(\bigcap_{i=n}^{\infty} X - E_i\right) = 1 - \prod_{i=n}^{\infty} (1 - \mu(E_i)) = 1 ,$$

since the sequence $\{X - E_i\}$ is also independent. It follows that $\mu(\bar{E}) = 1$.

Assume now that $\Sigma\mu(E_i)<\infty$. Then

$$\mu(\bar{E})\leqq\mu\left(\bigcup_{i=n}^{\infty}E_i\right)\leqq\sum_{i=n}^{\infty}\mu(E_i)\quad\text{for every}\quad n\geqq 1\,.$$

The right hand side tends to 0 as $n\to\infty$. Hence $\mu(\bar{E})=0$.

The statement c) is only a reformulation of b). □

A sequence $\{K_i/K\}_{i=1}^{\infty}$ of field extensions is said to be *linearly disjoint* if K_{i+1} is linearly disjoint from $K_1\dots K_i$ for every $i\geqq 1$. As an example of such a sequence we can take any sequence of the form $\{\mathbb{Q}_l/\mathbb{Q}\,|\,l\in L\}$, where L is a set of relatively prime positive integers. We shall use this example later on. In [9, Lemma 1.9] it was proved that if all the K_i are separable over K then the condition "$\{K_i/K\}_{i=1}^{\infty}$ is linearly disjoint" is equivalent to the condition "$\{\mathcal{G}(K_s/K_i)^e\}_{i=1}^{\infty}$ is independent in the probabilistic sense". Lemma 1.1 therefore implies the following Lemma

Lemma 1.2. *Let $\{K_i/K\}_{i=1}^{\infty}$ be a sequence of separable algebraic field extensions. Put $S=\{(\sigma)\in\mathcal{G}(K_s/K)^e\,|\,(\sigma)$ belongs to infinitely many $[K_s/K_i]$'s$\}$. Then*

a) *If the sequence $\{K_i/K\}$ is linearly disjoint and*

$$\sum_{i=1}^{\infty}\frac{1}{[K_i:K]^e}=\infty\quad\textit{then}\quad\mu(S)=1\,.$$

b) $\displaystyle\sum_{i=1}^{\infty}\frac{1}{[K_i:K]^e}<\infty\Rightarrow\mu(S)=0\,.$

In the case where K_i/K are Galois extensions we can say more. First note that if L/K is a finite Galois extension and $C\subseteqq\mathcal{G}(L/K)^e$ then

$$\mu(\{(\sigma)\in\mathcal{G}(K_s/K)^e\,|\,(\sigma\,|\,L)\in C\})=\frac{|C|}{[L:K]^e}\,.$$

Next we establish the following Lemma.

Lemma 1.3. *Let $\{K_i/K\}_{i=1}^{\infty}$ be a linearly disjoint sequence of finite Galois extensions. For every $i\geqq 1$ let $\bar{A}_i$ be a subset of $\mathcal{G}(K_i/K)^e$ and let*

$$A_i=\{(\sigma)\in(K_s/K)^e\,|\,(\sigma\,|\,K_i)\in\bar{A}_i\}\,.$$

Then the sequence $\{A_i\}_{i=1}^{\infty}$ is independent in the space $\mathcal{G}(K_s/K)^e$.

Proof. We have to show that every finite subsequence of $\{A_i\}_{i=1}^{\infty}$ is independent. We do it, for example, for the first n sets.

Put $L=K_1\dots K_n$. Then

$$\mathcal{G}(L/K)^e\cong\mathcal{G}(K_1/K)^e\times\cdots\times\mathcal{G}(K_n/K)^e\,.$$

For every n-tuple of e-tuples $(\sigma_1,\dots,\sigma_n)$ in $\mathcal{G}(K_1/K)^e\times\cdots\times\mathcal{G}(K_n/K)^e$ there exists exactly one e-tuple (σ) in $\mathcal{G}(L/K)^e$ such that $(\sigma\,|\,K_i)=(\sigma_i)$, $i=1,\dots,n$.

Therefore, if we put $A'=\left(\bigcap_{i=1}^{n}A_i\right)|\,L$ then

$$|A'|=\prod_{i=1}^{n}|\bar{A}_i|\,.$$

Hence

$$\mu\left(\bigcap_{i=1}^{n} A_i\right) = \frac{|A'|}{[L:K]^e} = \prod_{i=1}^{n} \frac{|\bar{A}_i|}{[K_i:K]^e} = \prod_{i=1}^{n} \mu(A_i).$$

As a corollary of Lemmas 1.1 and 1.3 we have

Lemma 1.4. *Notations as in Lemma 1.3. Put*

$$\bar{S} = \{(\sigma) \in \mathcal{G}(K_s/K)^e \mid (\sigma) \text{ belongs to infinitely many } A_i's\}$$

$$\underline{S} = \{(\sigma) \in \mathcal{G}(K_s/K)^e \mid (\sigma) \text{ belongs to almost all the } A_i's\}.$$

Then

a) *If the sequence* $\{K_i/K\}$ *is linearly disjoint and*

$$\sum_{i=1}^{\infty} \frac{|\bar{A}_i|}{[K_i:K]^e} = \infty \quad \text{then} \quad \mu(\bar{S}) = 1.$$

b) $\sum_{i=1}^{\infty} \frac{|\bar{A}_i|}{[K_i:K]^e} < \infty \Rightarrow \mu(\bar{S}) = 0.$

c) $\sum_{i=1}^{\infty} \frac{|\mathcal{G}(K_i/K)^e - \bar{A}_i|}{[K_i:K]^e} < \infty \Rightarrow \mu(\underline{S}) = 1.$

We shall frequently use the fact that the intersection of a countable number of measurable subsets of $\mathcal{G}(K_s/K)^e$ of measure 1 is again a subset of measure 1. Thus if

$$S_1(\sigma),\ S_2(\sigma),\ S_3(\sigma), \ldots$$

is a sequence of statements on the e-tuples (σ) of $\mathcal{G}(K_s/K)^e$ then "For almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ all the statements $S_1(\sigma)$, $S_2(\sigma)$, $S_3(\sigma)$, ... hold" is equivalent to "For every $i \geqq 1$ and for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ $S_i(\sigma)$ holds".

2. Jordan Totient Function

The Jordan totient function J_e is defined for every positive integer n as the number of the e-tuples $(a_1, \ldots, a_e)$ of integers between 1 and n for which $gcd(a_1, \ldots, a_e, n) = 1$. One can show that

$$J_e(n) = n^e \prod_{l \mid n} \left(1 - \frac{1}{l^e}\right) = \sum_{d \mid n} \mu(d) \left(\frac{n}{d}\right)^e$$

where μ is the Möbius function (cf. Le Veque [10, p. 89]). J_1 is the well known Euler totient function φ.

We are interested in an asymptotic formula for the sum $\sum_{m=1}^{n} J_e(m)$. We start with a preliminary asymptotic formula.

Lemma 2.1. $$\sum_{k=1}^{n} k^e = \frac{n^{e+1}}{e+1} + \frac{n^e}{2} + 0(n^{e-1}) \quad n \to \infty$$

where the 0 *depends on e.*

Proof. By Borevich and Shafarevich [2, p. 384]

$$\sum_{k=1}^{n} k^e = \frac{1}{e+1} \sum_{i=0}^{e} \binom{e+1}{i} B_i (n+1)^{e+1-i}$$

where B_i is the i-th Bernoulli's number, $B_0 = 1, B_1 = -\frac{1}{2}$,

$$= \frac{1}{e+1}\left((n+1)^{e+1} - \frac{e+1}{2}(n+1)^e + \cdots + (e+1)\,B_e(n+1)\right)$$

$$= \frac{n^{e+1}}{e+1} + \frac{n^e}{2} + 0(n^{e-1}).$$

□

Lemma 2.2. *If* $e \geqq 2$ *then*

$$\sum_{c=1}^{n} \mu(c)\left[\frac{n}{c}\right]^{e+1} = \sum_{c=1}^{n} \mu(c)\left(\frac{n}{c}\right)^{e+1} + 0(n^e) \quad n \to \infty. \tag{1}$$

$$\sum_{c=1}^{n} \mu(c)\left[\frac{n}{c}\right]^{e} = 0(n^e) \quad n \to \infty. \tag{2}$$

$$n^{e+1} \sum_{c=n+1}^{\infty} \frac{\mu(c)}{c^{e+1}} = 0(n^e) \quad n \to \infty. \tag{3}$$

Proof. 1) We can write $\left[\frac{n}{c}\right]$ in the form $\left[\frac{n}{c}\right] = \frac{n}{c} - \theta$ where $0 \leqq \theta < 1$. Then

$$\sum_{c=1}^{n} \mu(c)\left[\frac{n}{c}\right]^{e+1} = \sum_{c=1}^{n} \mu(c) \sum_{i=0}^{e+1} \binom{e+1}{i}\left(\frac{n}{c}\right)^{e+1-i}(-\theta)^i$$

$$= \sum_{c=1}^{n} \mu(c)\left(\frac{n}{c}\right)^{e+1} + \sum_{c=1}^{n} \mu(c) \sum_{i=1}^{e+1} \binom{e+1}{i}\left(\frac{n}{c}\right)^{e+1-i}(-\theta)^i.$$

Now

$$\left|\sum_{c=1}^{n} \mu(c) \sum_{i=1}^{e+1} \binom{e+1}{i}\left(\frac{n}{c}\right)^{e+1-i}(-\theta)^i\right| \leqq \sum_{i=1}^{e+1} \binom{e+1}{i} \sum_{c=1}^{n}\left(\frac{n}{c}\right)^{e+1-i}$$

$$\leqq n^e \sum_{i=1}^{e-1} \binom{e+1}{i} \sum_{c=1}^{\infty} \frac{1}{c^2} + n(e+1) \sum_{c=1}^{n} \frac{1}{c} + \sum_{c=1}^{n} 1$$

$$= 0(n^e) + 0(n \log n) + n = 0(n^e)$$

by LeVeque [10, p. 95]. The Formula (1) is therefore established.

2) $\left|\sum_{c=1}^{n} \mu(c)\left[\frac{n}{c}\right]\right| \leqq n^e \sum_{c=1}^{\infty} \frac{1}{c^2} = 0(n^e).$

3) $\left|n^{e+1} \sum_{c=n+1}^{\infty} \frac{\mu(c)}{c^{e+1}}\right| \leqq n^{e+1} \int_{n}^{\infty} \frac{d\theta}{\theta^{e+1}} = \frac{n}{e} = 0(n^e).$

□

Lemma 2.3. *If* $e \geqq 2$ *then*

$$\sum_{m=1}^{n} J_e(m) = \frac{n^{e+1}}{(e+1)\,\zeta(e+1)} + 0(n^e)\; n \to \infty.$$

Proof.

$$\sum_{m=1}^{n} J_e(m) = \sum_{m=1}^{n} \sum_{cd=m} \mu(c)\, d^e = \sum_{c=1}^{n} \mu(c) \sum_{d=1}^{\left[\frac{n}{c}\right]} d^e .$$

By Lemma 2.1

$$= \sum_{c=1}^{n} \mu(c) \left(\frac{1}{e+1} \left[\frac{n}{c}\right]^{e+1} + \frac{1}{2}\left[\frac{n}{c}\right]^{e} + 0\left(\left[\frac{n}{c}\right]^{e-1}\right)\right).$$

By Lemma 2.2

$$= \frac{n^{e+1}}{e+1} \sum_{c=1}^{n} \frac{\mu(c)}{c^{e+1}} + 0(n^e)$$

$$= \frac{n^{e+1}}{e+1} \sum_{c=1}^{\infty} \frac{\mu(c)}{c^{e+1}} - \frac{n^{e+1}}{e+1} \sum_{c=n+1}^{\infty} \frac{\mu(c)}{c^{e+1}} + 0(n^e).$$

By Lemma 2.2 and Le Veque [10, p. 120]

$$= \frac{n^{e+1}}{(e+1)\,\zeta(e+1)} + 0(n^e).$$

□

Lemma 2.4. *There exists a positive constant c such that for every positive integers e and n*

$$J_e(n) \geqq \frac{c^e n^e}{(\log \log n)^e}.$$

Proof. By Le Veque [10, p. 114]

$$J_e(n) = n^e \prod_{l \mid n} \left(1 - \frac{1}{l^e}\right) \geqq n^e \prod_{l \mid n} \left(1 - \frac{1}{l}\right)^e = \varphi(n)^e \geqq \frac{c^e n^e}{(\log \log n)^e}.$$

□

3. Lower Bounds for $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)]$

Lemma 3.1. *Let l be an odd prime, m a positive integer and D a set of divisors of $\varphi(l^m)$. Put*

$$E = \{(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e \mid [\tilde{\mathbb{Q}}(\sigma)_{l^m} : \tilde{\mathbb{Q}}(\sigma)] \in D\}.$$

Then

$$\mu(E) = \frac{1}{\varphi(l^m)^e} \sum_{d \in D} J_e(d).$$

Proof. It is certainly sufficient to prove the Lemma for the case where D consists of only one divisor d of $\varphi(l^m)$.

Indeed, for every $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ we have

$$[\tilde{\mathbb{Q}}(\sigma)_{l^m} : \tilde{\mathbb{Q}}(\sigma)] = [\mathbb{Q}_{l^m} : \mathbb{Q}_{l^m}(\sigma)] = |\langle \sigma \mid \mathbb{Q}_{l^m} \rangle| \tag{1}$$

since

$$\mathbb{Q}_{l^m}(\sigma) = \mathbb{Q}_{l^m} \cap \tilde{\mathbb{Q}}(\sigma) \quad \text{and} \quad \tilde{\mathbb{Q}}(\sigma)_{l^m} = \mathbb{Q}_{l^m}\, \tilde{\mathbb{Q}}(\sigma).$$

Also

$$\mathcal{G}(\mathbb{Q}_{l^m}/\mathbb{Q}) \cong \mathbb{Z}/\varphi(l^m)\,\mathbb{Z} \tag{2}$$

since l is an odd prime. For every $a \in \mathbb{Z}$ we denote by $\bar{a}$ its congruence class modulo $\varphi(l^m)$. Put

$$\bar{E} = \{(\bar{a}_1, \ldots, \bar{a}_e) \in (\mathbb{Z}/\varphi(l^m)\mathbb{Z})^e \mid |\langle \bar{a}_1, \ldots, \bar{a}_e \rangle| = d\}.$$

Then, by (1) and (2)

$$\mu(E) = \frac{|\bar{E}|}{\varphi(l^m)^e}. \tag{3}$$

Now, $\langle \bar{a}_1, \ldots, \bar{a}_e \rangle = \langle gcd(a_1, \ldots, a_e, \varphi(l^m)) \rangle$. Hence

$$|\langle \bar{a}_1, \ldots, \bar{a}_e \rangle| = \frac{\varphi(l^m)}{gcd(a_1, \ldots, a_e, \varphi(l^m))}.$$

It follows that $|\bar{E}|$ is equal to the number of the e-tuples $(a_1, \ldots, a_e)$ of integers between 1 and $\varphi(l^m)$ which satisfy $gcd(a_1, \ldots, a_e, \varphi(l^m)) = \frac{\varphi(l^m)}{d}$. This number is equal to the number of the e-tuples $(b_1, \ldots, b_e)$ of integers between 1 and d for which $gcd(b_1, \ldots, b_e, d) = 1$, i.e. to $J_e(d)$. Our Lemma follows from (3). □

Since $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)]$ divides $l-1$ it is interesting to compare it with powers of $l-1$ of exponents $0 < \theta < 1$. This is done to some extent in the following theorem.

Theorem 3.2. *Let e be a positive integer. Then for almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ and for every $\theta < \frac{e-1}{e+1}$ there exists an $l_0 = l_0(\sigma, \theta)$ such that for every prime $l \geqq l_0$*

$$[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] > (l-1)^\theta. \tag{1}$$

Proof. Consider an increasing sequence $\{\theta_n\}_{n=1}^{\infty}$ of real numbers which converges to $\frac{e-1}{e+1}$. Obviously it suffices to prove that for every n and for almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ there exists an l_0 such that for every prime $l \geqq l_0$ (1) is satisfied with θ replaced by θ_n. We therefore choose a fixed $\theta < \frac{e-1}{e+1}$ and prove that for almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ there exists an l_0 such that for every $l \geqq l_0$ (1) holds. The case $e = 1$ is trivial. We therefore assume that $e \geqq 2$.

For every prime l we denote by $A(l)$ the set of all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ for which (1) holds and by $B(l)$ its complement in $\mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$. Let A be the set of all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ for which (1) holds for almost all l. By Lemma 3.1

$$\mu(B(l)) = \frac{1}{(l-1)^e} \sum_{\substack{d \mid l-1 \\ d \leqq (l-1)^e}} J_e(d).$$

Hence, by Lemma 2.3

$$\mu(B(l)) \leqq \frac{1}{(l-1)^e} \sum_{d \leqq (l-1)^\theta} J_e(d) \leqq c(l-1)^{\theta(e+1)-e}$$

for some constant c. Hence

$$\sum_l \mu(B(l)) \leqq c \sum_l \frac{1}{(l-1)^{e-\theta(l+1)}} < \infty$$

since $e - \theta(e+1) > 1$. Hence, by Lemma 1.4 $\mu(A) = 1$. □

Problem 1. Is it possible to prove Theorem 3.2 for every $\theta < 1$?

4. The Values of the Function $[\mathbb{Q}(\sigma)_l : \mathbb{Q}(\sigma)]$

The next Theorem gives a second answer to the question how close can $[\mathbb{Q}(\sigma)_l : \mathbb{Q}(\sigma)]$ be to $l-1$ for a (σ) which is selected at random.

Theorem 4.1. *Let e be a positive integer. Then for almost every $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ we have: For every positive integer there exist infinitely many primes l such that*

$$(*) \qquad d \mid l-1 \quad \text{and} \quad [\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = \frac{l-1}{d}.$$

Proof. Since there are only countably many d's, it suffices to consider a fixed d and to prove that for almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ there exist infinitely many primes l for which $(*)$ holds.

Indeed, for every prime $l \equiv 1 \pmod{d}$ let

$$A(l) = \left\{(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e \mid [\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = \frac{l-1}{d}\right\}.$$

By Lemma 3.1 and Lemma 2.4

$$\mu(A(l)) = (l-1)^{-e} J_e\left(\frac{l-1}{d}\right) \geqq c_1 (l-1)^{-e} \frac{\left(\frac{l-1}{d}\right)^e}{\left(\log\log \frac{l-1}{d}\right)^e} \geqq \frac{c_2}{l}$$

for some positive constants c_1, c_2. Hence, by Dirichlet's theorem (cf. LeVeque [11, p. 217])

$$\sum_{l \equiv 1 \pmod{d}} \mu(A(l)) = \infty .$$

The sequence $\{\mathbb{Q}_l/\mathbb{Q} \mid l \text{ is prime}\}$ is linearly disjoint. Hence, by Lemma 1.4 almost all $(\sigma) \in \mathcal{G}(\mathbb{Q}/\mathbb{Q})^e$ belong to infinitely many $A(l)$'s. □

Theorem 4.1 shows that there does not exist a $\theta < 1$ such that

$$\limsup_l (l-1)^{-\theta} [\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = 1$$

for almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$. This removes a possible negative solution to Problem 1.

If $e \geqq 2$ then Theorem 3.2 implies that

$$\lim_{l \to \infty} [\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = \infty$$

for almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$. In particular, there are only finitely many roots of unity of prime order in those $\tilde{\mathbb{Q}}(\sigma)$. This statement is no more true if $e = 1$. Moreover, we have

Lemma 4.2. *For almost all $\sigma \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$ we have: For every positive integer d there exist infinitely many primes l such that $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = d$.*

Proof. Again it suffices to consider a fixed d and to prove that there exist infinitely many primes l such that $[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = d$.

Indeed, for every odd prime $l \equiv 1 \pmod{d}$ we put

$$B(l) = \{\sigma \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q}) | [\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] = d\}$$

$$= \{\sigma \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q}) | [\mathbb{Q}_l : \mathbb{Q}_l(\sigma)] = d\} .$$

Then $\mu(B(l)) = \dfrac{J_e(d)}{l-1}$, by Lemma 3.1, hence $\Sigma \mu(B(l)) = \infty$. Moreover, the $B(l)$'s are independent, by Lemma 1.3, hence, by Lemma 1.4, almost every $\sigma \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$ belongs to infinitely many $B(l)$'s. □

5. The Divergence of $[\mathbb{Q}(\sigma)_n : \mathbb{Q}(\sigma)]$

We have already proved that if $e \geqq 2$ then the sequence $\{[\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] | l$ is a prime$\}$ diverges to infinity for almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$. Our aim now is to strengthen this result by replacing l by n and letting n to run over all positive integers. We begin with a Lemma which serves as a complement to Lemma 3.1.

Lemma 5.1. *Let e be a positive integer, $0 < \theta < 1$ and $\eta = e - \theta(e+1)$. Put*

$$A(2, m) = \{(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e | [\tilde{\mathbb{Q}}(\sigma)_{2^m} : \tilde{\mathbb{Q}}(\sigma)] \leqq \varphi(2^m)^\theta\} .$$

Then

$$\mu(A(2, m)) = 0\left(\frac{1}{2^{\eta m}}\right) \quad m \to \infty .$$

Proof. We can assume, without loss of generality, that $m \geqq 2$. For every $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ we have

$$[\tilde{\mathbb{Q}}(\sigma)_{2^m} : \tilde{\mathbb{Q}}(\sigma)] = [\tilde{\mathbb{Q}}_{2^m} : \tilde{\mathbb{Q}}_{2^m}(\sigma)] = |\langle \sigma | \tilde{\mathbb{Q}}_{2^m} \rangle| . \tag{1}$$

Further

$$\mathcal{G}(\mathbb{Q}_{2^m}/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{m-2}\mathbb{Z} . \tag{2}$$

For every pair (a, b) of integers denote by $(\bar{a}, \bar{b})$ the pair in which $\bar{a}$ is the congruence class of a modulo 2 and $\bar{b}$ is the congruence class of b modulo 2^{m-2}. Let $B(m)$ be the set of all e-tuples

$$((\bar{a}_1, \bar{b}_1), \ldots, (\bar{a}_e, \bar{b}_e)) \tag{3}$$

in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{m-2}\mathbb{Z}$ which generate a subgroup of order $\leqq 2^{(m-1)}$. (1) and (2) imply that it suffices to prove that

$$|B(m)| = 0(2^{m\theta(e+1)}) \quad m \to \infty .$$

Indeed, there exists an $a \in \{0, 1\}$ such that

$$\langle (\bar{a}_1, \bar{b}_1), \ldots, (\bar{a}_e, \bar{b}_e) \rangle \supseteq \langle (\bar{a}, \overline{gcd(b_1, \ldots, b_e, 2^{m-2})}) \rangle ,$$

hence

$$|\langle (\bar{a}_1, \bar{b}_1), \ldots, (\bar{a}_e, \bar{b}_e) \rangle| \geqq \frac{2^{m-2}}{gcd(b_1, \ldots, b_e, 2^{m-2})} .$$

On the other side

$$\langle (\bar{a}_1, \bar{b}_1), \ldots, (\bar{a}_e, \bar{b}_e) \rangle \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \langle \bar{b}_1, \ldots, \bar{b}_e \rangle ,$$

hence

$$|\langle(\bar{a}_1, \bar{b}_1), \ldots, (\bar{a}_e, \bar{b}_e)\rangle| \leqq \frac{2 \cdot 2^{m-2}}{gcd(b_1, \ldots, b_e, 2^{m-2})}.$$

It follows that if $0 \leqq k \leqq m-1$ is such that

$$(\langle(\bar{a}_1, \bar{b}_1), \ldots, (\bar{a}_e, \bar{b}_e)\rangle| = 2^k),$$

then

$$gcd(b_1, \ldots, b_e, 2^{m-2}) = 2^{m-2-k+\varepsilon} \tag{4}$$

where $\varepsilon \in \{0, 1\}$, and if $k=0$ then $\varepsilon = 0$. For every $0 \leqq k \leqq m-2$ denote by $C(k)$ the set of all e-tuples (3) which satisfy $gcd(b_1, \ldots, b_e, 2^{m-2}) = 2^{m-2-k}$. We have by (4) that

$$B(m) \subseteqq \bigcup_{k=0}^{[(m-1)\theta]} C(k). \tag{5}$$

Clearly

$$|C(k)| = 2^e J_e(2^k).$$

Hence, by (5)

$$|B(m)| \leqq 2^e \sum_{k=0}^{[(m-1)\theta]} J_e(2^k) = 2^{e+e[(m-1)\theta]} = 0(2^{m\theta(e+1)}).$$

□

Lemma 5.2. *Let* $e \geqq 2$, $\theta < \dfrac{e-1}{e+1}$ *and* $\eta = e - \theta(e+1)$. *For every* $m \geqq 1$ *set*

$$A(m) = \{(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e \mid \exists \text{ a prime } l : [\tilde{\mathbb{Q}}(\sigma)_{l^m} : \tilde{\mathbb{Q}}(\sigma)] \leqq \varphi(l^m)^\theta\}.$$

Then

$$\mu(A(m)) = 0\left(\frac{1}{2^{\eta m}}\right) \quad m \to \infty.$$

Proof. For every prime l put

$$A(l, m) = \{(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e \mid [\tilde{\mathbb{Q}}(\sigma)_{l^m} : \tilde{\mathbb{Q}}(\sigma)] \leqq \varphi(l^m)^\theta\}.$$

For $l \geqq 3$ we have by Lemmas 3.1 and 2.3 that

$$\begin{aligned}
\mu(A(l, m)) &\leqq \frac{1}{\varphi(l^m)^e} \sum_{d \leqq \varphi(l^m)^\theta} J_e(d) \\
&\leqq \frac{1}{l^{(m-1)e}(l-1)^e}\left[\frac{l^{(m-1)\theta(e+1)}(l-1)^{\theta(e+1)}}{(e+1)\zeta(e+1)} + c l^{(m-1)\theta e}(l-1)^{\theta e}\right] \\
&\leqq \frac{c_2}{l^{(m-1)\eta}}
\end{aligned}$$

where c_1, c_2 are positive constants which does not depend on l and m. Now $A(m) = \bigcup_l A(l, m)$, hence, by Lemma 5.1

$$\begin{aligned}
\mu(A(m)) &\leqq \mu(A(2, m)) + \sum_{l \neq 2} \mu(A(l, m)) \\
&\leqq \mu(A(2, m)) + c_2 \sum_{k=3}^{\infty} \frac{1}{k^{(m-1)\eta}} \\
&\leqq \mu(A(2, m)) + c_2 \int_2^{\infty} \frac{dx}{x^{(m-1)\eta}} = 0\left(\frac{1}{2^{m\eta}}\right).
\end{aligned}$$

□

Lemma 5.3. *Let $e \geqq 2$. Then for almost all $(\sigma) \in \mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$*

$$\lim_{n \to \infty} [\tilde{\mathbb{Q}}(\sigma)_n : \tilde{\mathbb{Q}}(\sigma)] = \infty . \tag{1}$$

Proof. Choose a fixed $0 < \theta < \dfrac{e-1}{e+1}$. For every $k \geqq 1$ put, in the notations of Lemma 5.2, $B(k) = \bigcup_{m=k}^{\infty} A(m)$. Then $\{B(k)\}_{k=1}^{\infty}$ is a decreasing sequence of measurable sets and if we put $B = \bigcap_{k=1}^{\infty} B(k)$ then $\mu(B) = 0$. Let

$$S = \{(\sigma) \in \mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e \mid \exists\, l_0 \, \forall\, l \geqq l_0 : [\tilde{\mathbb{Q}}(\sigma)_l : \tilde{\mathbb{Q}}(\sigma)] > (l-1)^{\theta}\} .$$

By Theorem 3.2 $\mu(S) = 1$. Hence, if we put

$$T = S \cap (\mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e - B)$$

then

$$\mu(T) = 1 .$$

We prove that (1) holds for every $(\sigma) \in T$.

Indeed, let $(\sigma) \in T$ and set $M = \tilde{\mathbb{Q}}(\sigma)$. Let $s > 0$. Then there exists an l_0 such that for every prime $l \geqq l_0$ $[M_l : M] > (l-1)^{\theta}$ and hence there exists an $l_1 \geqq l_0$ such that for every prime $l \geqq l_1$

$$[M_l : M] > s . \tag{2}$$

Further there exists a k_0 such that for every $k \geqq k_0$ $2^{(k-1)\theta} > s$. Also $(\sigma) \notin B$ hence there exists a $k_1 \geqq k_0$ such that $(\sigma) \notin B(k_1)$. This implies that for every $k \geqq k$ and every prime l

$$[M_{l^k} : M] > l^{(k-1)\theta}(l-1)^{\theta} \geqq 2^{(k-1)\theta} > s . \tag{3}$$

Now, there exists an n_0 such that for every $n > n_0$ either n has a prime divisor $l \geqq l_1$ or n is divisible by a prime power l^k with $k \geqq k_1$. In the first case we have by (2)

$$[M_n : M] \geqq [M_l : M] > s$$

and in the second case we have by (3) that

$$[M_n : M] \geqq [M_{l^k} : M] > s . \qquad \square$$

6. Roots of Unity over Finite Fields

While the behaviour of the roots of unity over $\mathbb{Q}$ is known in great detail, very little is known about it over finite fields. It happens that this behaviour is strongly connected with number theoretic questions, some of which are the subject of well known conjectures. In this section we gather some simple facts on the roots of unity over finite fields which will help us to establish analogy to the theory which has been developed in the previous sections over $\mathbb{Q}$. The key Lemma is the following

Lemma 6.1. *Let F be a field of q elements and let $n \geqq 1$ be relatively prime to q. Then $[F_n : F] = \operatorname{ord}_n q$.*

Proof. Put $[F_n : F] = r$ and $\mathrm{ord}_n q = s$. Then $\mathcal{G}(F_n/F) = \{\tau_1, \ldots, \tau_r\}$ where τ_i is defined by

$$\tau_i(x) = x^{q^i} \quad x \in F_n, \quad i = 1, \ldots, r.$$

In particular if ζ is a primitive n-th root of 1 then the elements $\zeta^q, \zeta^{q^2}, \zeta^{q^3}, \ldots, \zeta^{q^r}$ are distinct, since $F_n = F(\zeta)$. It follows that the numbers $q, q^2, \ldots, q^r$ are distinct modulo n, hence $r \geqq s$.

Conversely, $\xi \mapsto \xi^{q^i}$ defines an element $\tau_i \in \mathcal{G}(F_n/F)$ for every i. This gives us s distinct elements of $\mathcal{G}(F_n/F)$, hence $s \leqq r$. □

It follows from Lemma 6.1 that we have to focus our attention on $\mathrm{ord}_n q$ as a function of n. First note that it diverges to ∞.

Indeed, we have the stronger statement

Lemma 6.2. *If $a, n \geqq 2$ are two relatively prime integers then*

$$\mathrm{ord}_n a \geqq \frac{\log(n+1)}{\log a}.$$

Proof.

$$\mathrm{ord}_n a = r \Rightarrow n \mid a^r - 1 \Rightarrow n \leqq a^r - 1$$

$$\Rightarrow r \geqq \frac{\log(n+1)}{\log a}.$$

□

If a is not divided by the prime l then $\mathrm{ord}_l a$ divides $l-1$. One can therefore consider $\dfrac{l-1}{\mathrm{ord}_l a}$ and ask for its properties. One of them is given by the following

Lemma 6.3. *For every $a > 1$ the function $\Psi(l) = \dfrac{l-1}{\mathrm{ord}_l a}$, whose arguments are the primes l which do not divide a, is unbounded.*

Proof. Assume that $\Psi(l)$ is bounded. Then $\Psi(l)$ obtains only a finite number of values $k_1, \ldots, k_s$. There exists now an n_0 such that for every $n > n_0$ $a^n - 1$ has a primitive divisor, i.e. a prime divisor l which does not divide $a^m - 1$ for $m < n$ (cf. Carmichael [3, Theorem XXIII]).

Put $n = n_0(k_1+1)(k_2+1)\ldots(k_s+1)+1$. Then $n > n_0$ and $nk_i + 1 = (n_0(k_1+1)\cdot(k_2+1)\cdots(k_s+1)+1)k_i + 1 \equiv k_i + 1 \equiv 0 \pmod{k_i+1}$ for $i = 1, \ldots, s$. Since $1 < k_i + 1 < nk_i + 1$, $nk_i + 1$ is composite.

Let l be a primitive prime divisor of $a^n - 1$. Then $n = \mathrm{ord}_l a$ and hence there exists an $1 \leqq i \leqq s$ such that $l = nk_i + 1$, which is a contradiction. □

Remark. The proof of Lemma 6.3 is roughly the same as that of the analogous theorem in Fibonacci sequences proved by Dov Jarden in [8, p. 5].

By combining Lemmas 6.1, 6.2, and 6.3 we obtain the following

Lemma 6.4. *Let F be a field with q elements.*

a) *If n is prime to q then $[F_n : F] \geqq \dfrac{\log(n+1)}{\log q}$.*

b) *The function $\dfrac{l-1}{[F_l : F]}$ is unbounded.*

7. Roots of Unity over $\tilde{\mathbb{F}}_p(\sigma)$

We consider now the field $\mathbb{F}_p$ as a ground field and study the behaviour of the roots of unity over $\tilde{\mathbb{F}}_p(\sigma)$ for a $(\sigma) \in \mathcal{G}(\tilde{\mathbb{F}}_p/F_p)^e$ selected at random. We distinguish between two cases: $e=1$ and $e \geqq 2$.

We beginn by the analogue of Lemma 4.2:

Lemma 7.1. *Almost all $\sigma \in \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F})$ have the following properties:*

a) *$\tilde{\mathbb{F}}_p(\sigma)$ is an infinite field.*

b) *$\tilde{\mathbb{F}}_p(\sigma)$ has exactly one extension of each degree d, i.e. $\langle\sigma\rangle \cong \hat{\mathbb{Z}}$.*

c) *For every positive integer d there exist infinitely many primes l such that $[\tilde{\mathbb{F}}_p(\sigma)_l : \tilde{\mathbb{F}}_p(\sigma)] = d$.*

Proof. For every r $\mathbb{F}_{p^r}$ is a Galois extension of $\mathbb{F}_p$ of degree r. Hence $\{\mathbb{F}_{p^r}/\mathbb{F}_p \mid r$ is a prime$\}$ is a linearly disjoint sequence of extensions. Moreover

$$\sum_{r \text{ prime}} \frac{1}{[\mathbb{F}_{p^r} : \mathbb{F}_p]} = \Sigma \frac{l}{r} = \infty ,$$

hence, by Lemma 1.4, $\mathbb{F}_p(\sigma)$ contains infinitely many $\mathbb{F}_{p^r}$ with r prime, and in particular $\tilde{\mathbb{F}}_p(\sigma)$ is an infinite field for almost all $\sigma \in \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)$.

Put now $\mathbb{F}_p^{(r)} = \bigcup_{m=1}^{\infty} \mathbb{F}_{p^{r^m}}$, for every prime r. Then $\mathbb{F}_p^{(r)}$ is an infinite extension of $\mathbb{F}_p$ and $\mathcal{G}(\mathbb{F}_p^{(r)}/\mathbb{F}_p) \cong \hat{\mathbb{Z}}_r$.

Hence $\mu(\mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p^{(r)})) = 0$. Put $S = \bigcup_r \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p^{(r)})$. Then $\mu(S) = 0$. We prove that $\langle\sigma\rangle \cong \hat{\mathbb{Z}}$ for every $\sigma \in \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p) - S$.

Indeed, consider such a σ. Let r be a prime. Then $\mathbb{F}_p^{(r)} \not\subseteq \tilde{\mathbb{F}}_p(\sigma)$. Hence $\mathcal{G}(\mathbb{F}_p^{(r)} \cdot \tilde{\mathbb{F}}_p(\sigma)/\tilde{\mathbb{F}}_p(\sigma))$ is isomorphic to a non trivial closed subgroup of $\hat{\mathbb{Z}}_r$, hence to $\hat{\mathbb{Z}}_r$ itself (cf. Ribes [12, p. 57]). If follows that $\langle\sigma\rangle = \mathcal{G}(\tilde{\mathbb{F}}_p/\tilde{\mathbb{F}}_p(\sigma)) \cong \hat{\mathbb{Z}}$, i.e. $\tilde{\mathbb{F}}_p(\sigma)$ has exactly one extension of each degree d.

Suppose now that σ has both Properties (a) and (b). We show that it has also Property (c). Put $M = \tilde{\mathbb{F}}_p(\sigma)$ and let N be an extension of M of degree d. Let α be an element of N which generates it over M. We can write M as an increasing union of finite fields K_i, since M is an infinite field. For every i large enough let $[K_i(\alpha) : \mathbb{F}_p] = n_i$. Let l_i be a primitive prime factor of $p^{n_i} - 1$, which exists by Carmichael Theorem mentioned on the proof of Lemma 6.3. Then $n_i = \operatorname{ord}_{l_i} p$ and hence, by Lemma 6.1 $[\mathbb{F}_{p,l_i} : \mathbb{F}_p] = n_i$, hence $K_i(\alpha) = \mathbb{F}_{p,l_i}$. It follows that $n = \mathbb{F}_{p,l_i} \cdot M = M_{l_i}$. Since $[N : M] = d$ and all the l_i are distinct we have that $[M_l : M] = d$ for infinitely many primes l. □

For $e \geqq 2$ we have the following analogue of Lemma 5.3.

Lemma 7.2. *If $e \geqq 2$ then almost all $(\sigma) \in \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F})^e$ have the following properties:*

a) *$\tilde{\mathbb{F}}_p(\sigma)$ is a finite field,*

b) $\lim_{\substack{n \to \infty \\ p+n}} [\tilde{\mathbb{F}}_p(\sigma)_n : \mathbb{F}_p(\sigma)] = \infty$.

Proof. We have

$$\sum_{n=1}^{\infty} \frac{1}{[\mathbb{F}_{p^n} : \mathbb{F}_p]^e} \leqq \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty .$$

Hence, by Lemma 1.4 $\tilde{\mathbb{F}}_p(\sigma)$ contains only a finite number of the fields $\mathbb{F}_{p^n}$, i.e. $\tilde{\mathbb{F}}_p(\sigma)$ is a finite field, for almost all $(\sigma)\in\mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)^e$.

Property (b) follows from Property (a) and Lemma 6.4 (a). □

We would like also to prove the analogue of Theorem 4.1 and in particular that for almost all $(\sigma)\in\mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)^e$ there exist infinitely many primes l such that $[\tilde{\mathbb{F}}_p(\sigma)_l:\tilde{\mathbb{F}}_p(\sigma)]=l-1$. For $e=2$ and for a $(\sigma)\in\mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)^2$ selected at random $\tilde{\mathbb{F}}_p(\sigma)$ is a finite field with, say q elements. Our desired analogue would then imply that $\mathrm{ord}_l q=l-1$, i.e. that q is a primitive root modulo l, for infinitely many primes l. This is however a well known and unsettled conjecture of Artin (cf. Goldstein [5, p. 343]). Theorem 4.1 appears therefore as an analogue of Artin's Conjecture.

We must be satisfied with the following weakened analogue of Theorem 4.1:

Theorem 7.3. *For every* $(\sigma)\in\mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)^e$ *the function*

$$\frac{l-1}{[\tilde{\mathbb{F}}_p(\sigma)_l:\tilde{\mathbb{F}}_p(\sigma)]} \quad l \text{ is a prime}$$

is unbounded.

Proof. Put $K=\tilde{\mathbb{F}}_p(\sigma)$. Then, by Lemma 6.1,

$$\frac{l-1}{[K_l:K]}\geqq\frac{l-1}{[\mathbb{F}_{p,l}:\mathbb{F}_p]}=\frac{l-1}{\mathrm{ord}_l p}.$$

The right hand side is not bounded, by Lemma 6.3, hence also $\dfrac{l-1}{[K_l:K]}$ is not bounded. □

On the other hand it is difficult to believe that the analogue of Theorem 3.2 is valid, since this would imply as before that for some q and $\theta>0$ $\mathrm{ord}_l q\geqq(l-1)^\theta$ for every large prime l. However, it is strongly believed that there are infinitely many Mersenne primes $l=2^r-1$ and in general one can conjecture that $\mathrm{ord}_l q\leqq c\log(l+1)$ for some constant c and for infinitely many primes l.

8. Fields of Finite Type

A field K is said to be of *finite type* if K is finitely generated over its prime field. We are going to show that if K is a field of finite type and F is its prime field then all the results proved in the previous sections for F are also valid for K. We do it in two steps.

Step 1. Let K be a purely transcendental extension of a field F. Then K is linearly disjoint from F_s over F and the restriction map $\sigma\mapsto\sigma|F_s$ is a continuous epimorphism of $\mathcal{G}(K_s/K)$ onto $\mathcal{G}(F_s/F)$ with a compact kernel. It follows that if $\bar{A}$ is a subset of $\mathcal{G}(F_s/F)^e$ of measure 1 then its lifting $A=\{(\sigma)\in\mathcal{G}(K_s/K)^e\,|\,(\sigma|F_s)\in\bar{A}\}$ is of measure 1 in $\mathcal{G}(F_s/F)^e$ (cf. Halmos [7, p. 279]). Moreover, $[F_s(\sigma)_n:F_s(\sigma)]=[K_s(\sigma)_n:K_s(\sigma)]$ for every $(\sigma)\in\mathcal{G}(K_s/K)^e$. Hence, every property of these numbers which holds for almost all $(\sigma)\in\mathcal{G}(F_s/F)^e$ holds for almost all $(\sigma)\in\mathcal{G}(K_s/K)^e$.

Step 2. Let L be a finite separable extension of a field K. Then $K_s=L_s$ and every subset of $\mathcal{G}(L_s/L)^e$ of a positive measure has also a positive measure in

$\mathcal{G}(K_s/K)^e$. It follows that every statement about fields which holds for the $K_s(\sigma)$ for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ holds also for the $L_s(\sigma)$ for almost all $(\sigma) \in \mathcal{G}(L_s/L)^e$.

Since every field of finite type can be obtained from its prime field by a purely transcendental extension followed by a finite separable extension our goal is achieved.

Thus Theorems 3.2 and 4.1, Lemmas 4.2 and 5.3 remain valid if we replace $\mathbb{Q}$ by any field K of characteristic 0 and of finite type; Lemmas 7.1 and 7.2 and Theorem 7.3 (b) remain valid if we replace $\mathbb{F}_p$ by any field K of characteristic p and $\tilde{\mathbb{F}}_p$ by K_s. By combining Lemmas 4.2 and 7.1 and this remark we get the following theorem:

Theorem 8.1. *Let K be a field of finite type. Then for almost all $\sigma \in \mathcal{G}(K_s/K)$ and for every positive integer d there exist infinitely many primes l such that $[K_s(\sigma)_l : K_s(\sigma)] = d$. In particular it follows, for $d = 1$, that $K_s(\sigma)$ contains infinitely many roots of unity of a prime order.*

By combining Lemmas 5.3 and 7.2 and the above remark we obtain the following theorem:

Theorem 8.2. *Let $e \geqq 2$ and let K be a field of finite type with* $\mathrm{char}(K) = p \geqq 0$. Then for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$

$$\lim_{\substack{n \to \infty \\ p+n}} [K_s(\sigma)_n : K_s(\sigma)] = \infty .$$

In particular, $K_s(\sigma)$ contains only a finite number of roots of unity.

9. Points of Finite Order on Linear Algebraic Groups

In this section we generalize Theorem 8.2 to linear groups which are, by definition, affine algebraic group varieties. The generalization depends on the following Lemmas:

Lemma 9.1. *Let C be a triangular matrix of the form*

$$C = \begin{pmatrix} 1 & \gamma_1 & & * \\ & \ddots & \ddots & \\ & & 1 & \gamma_{k-1} \\ 0 & & & 1 \end{pmatrix}$$

with entries in a field of characteristic $p \geqq 0$. If $C^d = I$ is the unit matrix for some positive integer d which is not divisable by p, then $C = I$.

Proof. It is easy to see that

$$C^d = \begin{pmatrix} 1 & d\gamma_1 & & * \\ & \ddots & \ddots & \\ & & 1 & d\gamma_{k-1} \\ 0 & & & 1 \end{pmatrix}$$

hence $d\gamma_1 = \cdots = d\gamma_{k-1} = 0$. It follows that $\gamma_1 = \cdots = \gamma_{k-1} = 0$ since $p+d$. In the same way one proceeds to show that all diagonals of C above the principal diagonal consist of zeros. □

Lemma 9.2. *Let*

$$B = \begin{pmatrix} \xi_l & & * \\ & \ddots & \\ 0 & & \xi_k \end{pmatrix}$$

be a triangular matrix of order n with entries in a field of characteristic p. Then $\xi_l^n = \cdots = \xi_k^n = 1$. *If p does not divide n, then there exists an* $l \leqq i \leqq k$ *such that* $\operatorname{ord} \xi_i \geqq \sqrt[k]{n}$.

Proof. $B^n = I$.

Hence $\xi_1^n = \cdots = \xi_k^n = 1$. Put $n_j = \operatorname{ord} \xi_j$, $j = 1, \ldots, k$. Then $n_j | n$. Assume that $n_j < \sqrt[k]{n}$ for $j = 1, \ldots, k$. Then $m = lcm(n_1, \ldots, n_k) \leqq n_1 \ldots k_k < n$ and $m | n$. Put $C = B^m$. Then C satisfies the assumptions of Lemma 9.1 with $d = \dfrac{m}{n}$. Hence $C = I$. It follows that $n | m$ which is false. □

Lemma 9.3. *Let L be a field of characteristic* $p > 0$ *and let A be a* $k \times k$ *matrix of order n with entries in L. Then the maximal power of p which divides n is* $\leqq p^{k-1}$.

Proof. Put $n = p^m n'$ where n' is prime to p. Replacing A by $A' = A^{n'}$ we can assume that $\operatorname{ord} A = p^m$ and we have to prove that $A^{p^{k-1}} = I$. Again we know that there is a triangular matrix A'' with entries in $\tilde{L}$ which is similar to A (cf. Halmos [6, p. 107]). A'' has the same order as A, so we can assume, without loss of generality, that A has the form

$$A = \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_k \end{pmatrix}$$

By assumption $A^{p^m} = I$. Hence $a_1^{p^m} = \cdots = a_k^{p^m} = 1$, hence $a_1 = \cdots = a_k = 1$. Now, if we raise A to the p^{k-1}th power, we see, as in the proof of Lemma 9.1, that all the diagonals of A above the principal diagonal vanish, since $\operatorname{char}(L) = p$. It follows that $A^{p^{k-1}} = I$.

Lemma 9.4. *Let L be a field of characteristic* $p \geqq 0$ *with the property* $\lim_{\substack{n \to \infty \\ p+n}} [L_n : L] = \infty$. *Let G be a linear algebraic group defined over L. Then for every m there exists an* n_0 *such that for every point P of G*

$$n_0 < \operatorname{ord} P < \infty \implies [L(P) : L] > m .$$

In particular, the order of the torsion L-rational points of G is bounded.

Proof. Every linear algebraic group G defined over L is L-isomorphic to a Zariski L-closed subgroup of the general linear group $\mathbb{GL}_k$ for some positive

integer k (cf. Borel [1, p. 101]). It is therefore sufficient to prove our lemma for the $\mathbb{GL}_k$'s.

Let m be a positive integer. Then there exists a t_0 such that

$$t > t_0 \Rightarrow [L_t : L] > km . \tag{1}$$

Put $n_0 = p^{k-1} t_0^k$ if $p > 0$ and $n_0 = t_0^k$ if $p = 0$. Let A be a matrix of a finite order n and suppose that $n > n_0$. Put $M = L(A)$. We have to prove that $[M : L] > m$. Define n' as follows: If $p > 0$ put $n = p^l n'$ where n' is relatively prime to p. Then $l \leqq k-1$, by Lemma 9.3. If $p = 0$ put $n' = n$. In every case we have $n' > t_0^k$.

Assume that $[M : L] \leqq m$. Let B be a triangular matrix with entries in L which is similar to A. Put $B' = B^{p^l}$ if $p > 0$ and $B' = B$ if $p = 0$. Then B' has the form

$$B' = \begin{pmatrix} \xi_1 & & * \\ & \ddots & \\ 0 & & \xi_k \end{pmatrix}$$

and its order is n'. Hence, by Lemma 9.2, $\xi_1^{n'} = \cdots = \xi_k^{n'} = 1$ and there exists an $1 \leqq i \leqq k$ such that $t = \operatorname{ord} \xi_i \geqq \sqrt[k]{n'} > t_0$. It follows by (1) that

$$[L_t : L] > km . \tag{2}$$

The characteristic polynomial of B is $f(X) = (X - \xi_1) \cdots (X - \xi_k)$. It is also the characteristic polynomial of A' which is defined to be A^{p^l} if $p > 0$ and as A if $p = 0$. Hence f has coefficients in M. It follows that $[M(\xi_i) : M] \leqq k$. Hence $[L_t : L] \leqq km$ since $L_t = L(\xi_i) \subseteq M(\xi_i)$. This contradicts (2). □

Finally, by combining Theorem 8.2 and Lemma 9.4 we get the following theorem:

Theorem 9.5. *Let $e \geqq 2$ and let K be a field of finite type with $\operatorname{char}(K) = p \geqq 0$. Then almost all $(\sigma) \in \mathscr{G}(K_s/K)^e$ have the following property:*

For every linear algebraic group G defined over L and for every m there exists an n_0 such that for every point P of G

$$n_0 < \operatorname{ord} P < \infty \Rightarrow [K_s(\sigma)(P) : K_s(\sigma)] > m .$$

In particular the order of the $K_s(\sigma)$ torsion L-rational points of G is bounded.

We note that we cannot extend Theorem 8.1 to linear algebraic groups too, since, there exist linear algebraic groups like the additive group of the field in characteristic 0 which have no torsion points at all.

References

1. Borel, A.: Linear algebraic groups. New York: Benjamin 1969
2. Borevich, Z.I., Shafarevich, I.R.: Number theory. New York: Academic Press 1966
3. Carmichael, R.D.: On the numerical factors of the arithmetic forms $\alpha^n - \beta^n$. Annals of Mathematics, **15**, 30—70 (1913—1914)
4. Frey, G., Jarden, M.: Approximation theory and the rank of abelian varieties over large algebraic fields. Proc. London Math. Soc. (1973)
5. Goldstein, L.J.: Density questions in algebraic number theory. American Mathematical Monthly **78**, 342—351 (1971)
6. Halmos, P.R.: Finite dimensional vector spaces. Princeton: D. Van Nostrand Company 1958

7. Halmos, P. R.: Measure theory. Princeton: D. Van Nostrand Company 1950
8. Jarden, D.: Recurring sequences. Riveon Lematematika, Jerusalem (1966)
9. Jarden, M.: Elementary statements over large algebraic fields. Transactions of the A.M.S. **64**, 67—91 (1972)
10. Le Veque, W. J.: Topics in number theory, Vol. I. Reading: Addison-Wesley 1956
11. Le Veque, W. J.: Topics in number theory, Vol. II. Reading: Addison-Wesley 1956
12. Ribes, L.: Introduction to profinite groups and Galois cohomology. Queens University, Kingston 1970

M. Jarden
Department of Mathematical Sciences
Tel-Aviv University
Ramat-Aviv, Tel-Aviv, Israel

(Received April 9, 1974)