

**THE ELEMENTARY THEORY OF FINITE FIELDS\***

by

Moshe Jarden, Tel Aviv University

April 1994

March 2004

---

\* Notes of a course given at Tel Aviv University, Spring 1994 and Spring 2004.

## Introduction

TRANSFER THEOREM: *Let  $\theta$  be an elementary statement about fields. Set*

$$A(\theta) = \{p \in P(\mathbb{Q}) \mid \theta \text{ is true in } \mathbb{F}_p\}$$

$$S(\theta) = \{\sigma \in \text{Gal}(\mathbb{Q}) \mid \theta \text{ is true in } \tilde{\mathbb{Q}}(\sigma)\}$$

*Then  $A(\theta)$  has a Dirichlet density  $\delta(A(\theta))$ ,  $S(\theta)$  is Haar measurable and  $\delta(A(\theta)) = \mu(S(\theta))$ . Moreover,  $\delta(A(\theta))$  is a rational number which is positive exactly if  $A(\theta)$  is infinite.*

An **elementary statement** is a statement which is equivalent to a first order sentence in the language of rings (examples follow).

$\mathbb{Q}$  = the field of rational numbers;

$P(\mathbb{Q})$  = the set of rational primes;

$\tilde{\mathbb{Q}}$  = the field of all algebraic numbers;

$\text{Gal}(\mathbb{Q})$  = the absolute Galois group of  $\mathbb{Q}$ , i.e.,  $\text{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q})$ ; if  $\sigma \in \text{Gal}(\mathbb{Q})$ , then

$$\tilde{\mathbb{Q}}(\sigma) = \{x \in \tilde{\mathbb{Q}} \mid \sigma x = x\}.$$

The **Dirichlet density** of a subset  $A \subseteq P(\mathbb{Q})$  is (if the limit exists)

$$\delta(A) = \lim_{s \rightarrow 1^+} \frac{\sum_{p \in A} \frac{1}{p^s}}{\sum_{p \in P(\mathbb{Q})} \frac{1}{p^s}}.$$

In particular  $\delta(P(\mathbb{Q})) = 1$  and the density of each finite set is zero. However, there exist infinite set of primes of density zero.

The **Haar measure**  $\mu$  of  $\text{Gal}(\mathbb{Q})$  is the unique one defined with respect to the Krull topology of  $\text{Gal}(\mathbb{Q})$  such that  $\mu(\text{Gal}(\mathbb{Q})) = 1$ .

The proof of the transfer theorem involves ingredients from several areas: Algebraic number theory, the theory of profinite groups, measure theory, algebraic geometry, and model theory.

Credit: Ax [Ax] 1967, Jarden [Ja1] 1969, Fried [FrS] 1974.

References: Field Arithmetic [FrJ].

*Example 1:*  $\theta$  is the sentence  $\exists X: X^2 = -1$ .

$$\begin{aligned} \mathbb{F}_p \models \theta &\iff \text{there exists } x \in \mathbb{F}_p: x^2 = -1 \\ &\iff \text{there exists } x \in \mathbb{Z}: x^2 \equiv -1 \pmod{p} \\ &\iff p = 2 \text{ or } \left(\frac{-1}{p}\right) = 1 \quad (\text{Legendre symbol}) \\ &\iff p = 2 \text{ or } p \equiv 1 \pmod{4} \end{aligned}$$

By Dirichlet's theorem on primes in arithmetic progressions  $\delta(A(\theta)) = \frac{1}{2}$ .

$$\begin{aligned} \tilde{\mathbb{Q}}(\sigma) \models \theta &\iff \text{there exists } x \in \tilde{\mathbb{Q}}(\sigma): x^2 = -1 \\ &\iff \sqrt{-1} \in \tilde{\mathbb{Q}}(\sigma) \\ &\iff \text{res}_{\mathbb{Q}(\sqrt{-1})}\sigma = 1 \end{aligned}$$

As  $\text{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$  has two elements,  $\mu(A(\theta)) = \frac{1}{2}$ . ■

*Example 2:*  $f \in \mathbb{Z}[X]$  is a monic polynomial of degree 10:  $f(X) = X^{10} + \sum_{i=0}^9 a_i X^i$ .  $\theta$  is the statement ' $f$  factors into the product of a monic polynomial  $g$  of degree 4 and a monic polynomial  $h$  of degree 6'. Put  $a_{10} = b_4 = c_6 = 1$ . For each field  $K$  we have:

$$\begin{aligned} K \models \theta &\iff \exists g, h \in K[X]: g \text{ monic of degree 4 and } h \text{ monic of degree 6 and } f = gh \\ &\iff \exists b_0, b_1, b_2, b_3 \in K \exists c_0, c_1, c_2, c_3, c_4, c_5 \in K: \sum_{i=0}^{10} a_i X^i = \sum_{j=0}^4 b_j X^j \sum_{k=0}^6 c_k X^k \\ &\iff \exists b_0, b_1, b_2, b_3 \in K \exists c_0, c_1, c_2, c_3, c_4, c_5 \in K: \bigwedge_{i=0}^9 [a_i = \sum_{j+k=i} b_j c_k] \end{aligned}$$

Thus  $\theta$  is an elementary statement.

If  $L$  is the splitting field of  $f(X)$  over  $\mathbb{Q}$ , then  $[L : \mathbb{Q}] \leq 10!$ . If  $\sigma \in \text{Gal}(\mathbb{Q})$  and  $\text{res}_L \sigma = 1$ , then  $\tilde{\mathbb{Q}}(\sigma) \models \theta$ . Hence,  $\delta(A(\theta)) = \mu(A(\theta)) \geq \frac{1}{10!}$ . In particular, there are infinitely many primes  $p$  such that  $\mathbb{F}_p \models \theta$ . ■

*Example 3:*  $f \in \mathbb{Z}[X]$  is a monic irreducible polynomial of degree  $n > 1$ ,  $\theta$  is the statement ' $f(X)$  has no root', i.e., ' $\neg \exists X: f(X) = 0$ '. Let  $f(X) = \prod_{i=1}^n (X - x_i)$  and  $L = \mathbb{Q}(x_1, \dots, x_n)$ . Then  $\mathbb{Q}(x_1), \dots, \mathbb{Q}(x_n)$  are conjugate to each other. Hence,  $\text{Gal}(L/\mathbb{Q}(x_1)), \dots, \text{Gal}(L/\mathbb{Q}(x_n))$  are proper subgroups of  $\text{Gal}(L/\mathbb{Q})$  which are conjugate to each other. By group theory, there exists  $\sigma_0 \in \text{Gal}(L/\mathbb{Q})$  which belongs to no

$\text{Gal}(L/\mathbb{Q}(x_i))$ . Thus  $\sigma_0 x_i \neq x_i$  for  $i = 1, \dots, n$ . If  $\sigma \in \text{Gal}(\mathbb{Q})$  and  $\text{res}_L \sigma = \sigma_0$ , then  $\sigma x_i \neq x_i$  for  $i = 1, \dots, n$ . Hence  $\delta(A(\theta)) = \mu(A(\theta)) \geq \frac{1}{n!}$ . In particular, there exists infinitely many primes  $p$  such that  $f(X) \equiv 0 \pmod{p}$  has no solution.

*Remark:* The irreducibility of  $f$  is essential:  $f(X) = (X^2 - 2)(X^2 - 3)(X^2 - 6)$  is a counter example. Another example:  $f(X) = (X^2 + 3)(X^3 - 2)$ . Here note that  $\zeta = \zeta_3$  satisfies  $\zeta^2 + \zeta + 1 = 0$ . Hence  $\zeta = \frac{-1 + \sqrt{-3}}{2}$  and therefore  $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$ . If  $\sigma \sqrt[3]{2} = \zeta \sqrt[3]{2}$  and  $\sigma(\zeta \sqrt[3]{2}) = \zeta^2 \sqrt[3]{2}$ , then  $\sigma \zeta = \zeta$ , hence  $\sigma \sqrt{-3} = \sqrt{-3}$ . ■

*Example 4: Chevalley's theorem.* Every homogeneous polynomial  $f \in \mathbb{F}_p[X_0, \dots, X_n]$  of degree  $n$  has a non-trivial zero. If  $f(\mathbf{X}) = \sum_{i_0 + \dots + i_n = n} \mathbf{a}_i X_0^{i_0} X_1^{i_1} \dots X_n^{i_n}$ , then the corresponding sentence is:

$$\forall \mathbf{a} \exists \mathbf{X} \left[ \bigvee_{i=0}^n X_i \neq 0 \ \& \ f(\mathbf{X}) = 0 \right].$$

Thus  $\mathbb{F}_p$  is a  $C_1$ -field. Hence, almost all  $\tilde{\mathbb{Q}}(\sigma)$  is a  $C_1$ -field. ■

*A proof of Chevalley's theorem:* Source: Borevich and Shafarevich [BoS].

Motivation: If  $f \in K[X]$  vanishes at all  $x \in K$  and  $K$  is infinite, then  $f = 0$ . For  $K = \mathbb{F}_p$  we have  $X^p - X$  as a counter example.

*Definition:* A polynomial  $f \in \mathbb{F}_p[X_1, \dots, X_n]$  is **reduced** if  $\deg_{X_j} f < p$  for  $j = 1, \dots, n$ . Two polynomials  $f, g \in \mathbb{F}_p[X_1, \dots, X_n]$  are **equivalent** if  $f(\mathbf{x}) = g(\mathbf{x})$  for each  $\mathbf{x} \in \mathbf{F}_p^n$ . ■

Recall:  $x^p = x$  for each  $x \in \mathbb{F}_p$  and

$$x^{p-1} = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

LEMMA 1: Every polynomial  $f \in \mathbb{F}_p[X_1, \dots, X_n]$  is equivalent to a reduced one,  $f^*$  such that  $\deg(f^*) \leq \deg(f)$ .

*Proof:* Replace each occurrence of  $X_j^k$  with  $k \geq p$  by  $X_j^{k-(p-1)}$  and proceed by induction. ■

LEMMA 2: If  $f \in \mathbb{F}_p[X_1, \dots, X_n]$  is reduced and equivalent to 0, then  $f = 0$ .

*Proof:* Induction on  $n$ . ■

LEMMA 3: if  $f, g \in \mathbb{F}_p[X_1, \dots, X_n]$  are reduced and equivalent, then  $f = g$ .

*Proof:* Apply Lemma 2 on  $f - g$ . ■

LEMMA 4: If  $f, g \in \mathbb{F}_p[X_1, \dots, X_n]$  are equivalent, and  $f$  is reduced, then  $\deg_{X_j} f \leq \deg_{X_j} g$  for  $j = 1, \dots, n$ . Hence  $\deg(f) \leq \deg(g)$ .

*Proof:* By Lemma 1,  $g$  is equivalent to a reduced polynomial  $g^*$  with  $\deg_{X_j}(g^*) \leq \deg_{X_j}(g)$  for  $j = 1, \dots, n$ . By Lemma 3,  $f = g^*$ . Hence  $\deg(f) \leq \deg(g)$ . ■

LEMMA 5 (Waring): Let  $f \in \mathbb{F}_p[X_1, \dots, X_n]$  be a polynomial of degree  $< n$ . Then  $\#\{\mathbf{a} \in \mathbb{F}_p^n \mid f(\mathbf{a}) = 0\} \equiv 0 \pmod{p}$ .

*Proof:* Let  $A = \{\mathbf{x} \in \mathbb{F}_p^n \mid f(\mathbf{x}) = 0\}$  and let  $g(\mathbf{X}) = 1 - f(\mathbf{X})^{p-1}$ . Then

$$g(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \in A \\ 0 & \text{if } \mathbf{x} \notin A \end{cases}$$

and  $\deg(g(\mathbf{X})) = (p-1)\deg(f(\mathbf{X})) < (p-1)n$ . For each  $\mathbf{a} \in A$  consider

$$h_{\mathbf{a}}(\mathbf{X}) = \prod_{j=1}^n (1 - (X_j - a_j)^{p-1}) = (-1)^n X_1^{p-1} \cdots X_n^{p-1} + \text{lower terms.}$$

Then,  $h_{\mathbf{a}}(\mathbf{X})$  is a reduced polynomial and  $\deg(h_{\mathbf{a}}(\mathbf{X})) = (p-1)n$ . Also,

$$h_{\mathbf{a}}(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} = \mathbf{a} \\ 0 & \text{if } \mathbf{x} \neq \mathbf{a} \end{cases}$$

It follows that

$$(1) \quad h(\mathbf{X}) = \sum_{\mathbf{a} \in A} h_{\mathbf{a}}(\mathbf{X}) = (-1)^n |A| X_1^{p-1} \cdots X_n^{p-1} + \text{lower terms}$$

is a reduced polynomial and

$$h(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \in A \\ 0 & \text{if } \mathbf{x} \notin A. \end{cases}$$

Thus  $h(\mathbf{X})$  is equivalent to  $g(\mathbf{X})$ . By Lemma 4,  $\deg(h(\mathbf{X})) \leq \deg(g(\mathbf{X})) < (p-1)n$ . Hence, the highest term in the right hand side of (1) vanishes. That is  $|A| = 0$  in  $\mathbb{F}_p$ . Equivalently  $|A| \equiv 0 \pmod p$  in  $\mathbb{Z}$ . ■

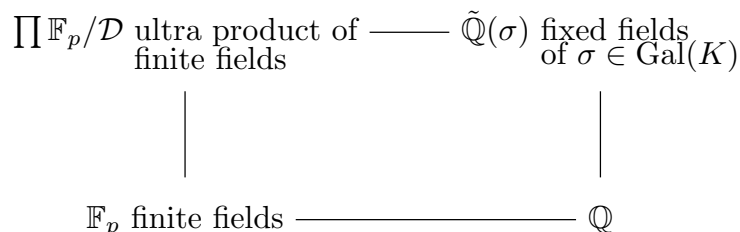
*Conclusion of the proof of Chevalley's theorem:* If  $f(X_0, \dots, X_n)$  is a form of degree  $n$ , then the number of its zeros is a multiple of  $p$ . Since  $f$  has the zero  $(0, \dots, 0)$  it must have at least another one. ■

*Example 5:* Let  $G$  be a finite group,  $K$  a field,  $t$  a transcendental element over  $K$ . Then ' $K(t)$  has a Galois extension  $F$  such that  $\text{Gal}(F/K(t)) \cong G$ ' is an elementary statement  $\theta$  about  $K$ . A special case of a theorem of Fried and Völklein [FrV] says that  $\theta$  is true in  $\tilde{\mathbb{Q}}(\sigma)$  for almost all  $\sigma$ . Hence:

For each finite group  $G$  there exists a finite set  $S$  of primes such that for each  $p \notin S$ ,  $\mathbb{F}_p(t)$  has a Galois extension  $F$  with Galois group  $G$ . ■

*Example 6:* Let  $f \in \mathbb{Z}[X_1, \dots, X_n]$  be an absolutely irreducible polynomial. Then, by a theorem of Weil (= Riemann hypothesis for function fields)  $f(\mathbf{X})$  has a zero in  $\mathbb{F}_p$  for almost all  $p$ . It follows that  $f(\mathbf{X})$  has a zero in  $\tilde{\mathbb{Q}}(\sigma)$  for almost all  $\sigma$ . ■

The proof of the transfer theorem travels along a rectagle each of its verticis consists of another family of fields:



Three basic theorems make this travel possible:

THE RIEMANN HYPOTHESIS FOR FUNCTION FIELDS (= Weil's theorem): For each  $d$  there exists  $p_0$  such that for all primes  $p \geq p_0$ , each absolutely irreducible polynomial  $f \in \mathbb{F}_p[X, Y]$  of degree  $\leq d$  has a zero  $(x, y) \in \mathbb{F}_p^2$ .

HILBERT IRREDUCIBILITY THEOREM: For each irreducible polynomial  $f \in \mathbb{Q}[X, Y]$  there exist infinitely many  $x \in \mathbb{Q}$  such that  $f(x, Y)$  is irreducible in  $\mathbb{Q}[Y]$ .

CHEBOTAREV DENSITY THEOREM: Let  $L$  be a finite Galois extension of  $\mathbb{Q}$  and let  $\mathcal{C}$  be a conjugacy class in  $\text{Gal}(L/\mathbb{Q})$ . Then the Dirichlet density of the set of all primes  $p$  whose Artin symbol  $\left(\frac{L/\mathbb{Q}}{p}\right) = \mathcal{C}$  is  $|\mathcal{C}|/[L:\mathbb{Q}]$ .

Examples for the Artin symbol: (a)  $L = \mathbb{Q}(\sqrt{a})$  ( $a$  nonsquare),  $p$  an odd prime,

$$\left(\frac{L/\mathbb{Q}}{p}\right) = \left(\frac{a}{p}\right) = \begin{cases} 1 & \exists x: x^2 \equiv a \pmod{p} \\ -1 & \text{otherwise.} \end{cases}$$

(b)  $L = \mathbb{Q}(\zeta_n)$ ,  $p \nmid n$ . If  $\left(\frac{L/\mathbb{Q}}{p}\right) = \{\sigma\}$ , then  $\zeta_n^\sigma = \zeta_n^p$ . ■

## 1. Infinite Galois theory

THE BASIC THEOREM OF FINITE GALOIS THEORY: *Let  $N/K$  be a finite Galois extension.*

$G = \text{Gal}(N/K)$  its Galois group;

$\mathcal{L} = \mathcal{L}(N/K)$  is the collection of all intermediate fields  $K \subseteq N \subseteq L$ ;

$\text{Sub}(G)$  is the collection of all subgroups of  $G$

For each  $L \in \mathcal{L}$  we have  $\text{Gal}(N/L) \in \text{Sub}(G)$ ;

For each  $H \in \text{Sub}(G)$  we have  $N(H) = \{x \in N \mid \sigma x = x \text{ for all } \sigma \in H\} \in \mathcal{L}$ .

The map  $L \mapsto \text{Gal}(N/L)$  is a bijection  $\mathcal{L}(N/K) \rightarrow \text{Sub}(G)$  whose inverse is  $H \mapsto N(H)$ .

Moreover:  $L/K$  is Galois if and only if  $\text{Gal}(N/L) \triangleleft G$ . In this case we have the following short exact sequence

$$1 \longrightarrow \text{Gal}(N/L) \longrightarrow \text{Gal}(N/K) \xrightarrow{\text{res}_L} \text{Gal}(L/K) \longrightarrow 1$$

The Galois correspondence satisfies the following rules:

(1a)  $L_1 \subseteq L_2$  if and only if  $\text{Gal}(N/L_1) \supseteq \text{Gal}(N/L_2)$ ;

(1b)  $H_1 \leq H_2$  if and only if  $N(H_1) \supseteq N(H_2)$ ;

(1c)  $N(H_1) \cap N(H_2) = N(\langle H_1, H_2 \rangle)$ ;

(1d)  $\text{Gal}(N/L_1 \cap L_2) = \langle \text{Gal}(N/L_1), \text{Gal}(N/L_2) \rangle$ ;

(1e)  $N(H_1 \cap H_2) = N(H_1)N(H_2)$ ;

(1f)  $N(H^\sigma) = N(H)^\sigma$ ;

(1g)  $\text{Gal}(N/L^\sigma) = \text{Gal}(N/L)^\sigma$ ;

(1h) If  $L/K$  is Galois and  $M/K$  is an arbitrary extension, then  $LM/M$  is Galois and  $\text{res}_L: \text{Gal}(LM/M) \rightarrow \text{Gal}(L/L \cap M)$  is an isomorphism;

(1i) If in addition  $M/K$  is Galois, then  $(L \cap M)/K$  is Galois and  $N = LM$  is Galois over  $K$ ; in this case

$$\text{Gal}(N/K) \cong \{(\sigma, \tau) \in \text{Gal}(L/K) \times \text{Gal}(M/K) \mid \text{res}_{L \cap M} \sigma = \text{res}_{L \cap M} \tau\},$$

where  $\rho \mapsto (\text{res}_L \rho, \text{res}_M \rho)$ . In particular, if  $L \cap M = K$ , then  $\text{Gal}(N/K) \cong \text{Gal}(L/K) \times \text{Gal}(M/K)$ .

THE KRULL TOPOLOGY. Now  $N/K$  is an arbitrary Galois extension. Let  $\mathcal{L}_0$  be the collection of all intermediate fields  $K \subseteq L \subseteq N$  such that  $L/K$  is finite Galois. Basic open neighborhoods of 1 in  $G = \text{Gal}(N/K)$  are  $\text{Gal}(N/L)$  with  $L \in \mathcal{L}_0$ . If  $L_1, L_2 \in \mathcal{L}_0$ , then  $L_1 L_2 \in \mathcal{L}_0$  and  $\text{Gal}(N/L_1) \cap \text{Gal}(N/L_2) = \text{Gal}(N/L_1 L_2)$ .

Basic open neighborhood of  $\sigma \in G$  is  $\sigma \text{Gal}(N/L)$  with  $L \in \mathcal{L}_0$ .

If  $\sigma_1, \dots, \sigma_n \in G$  represent  $G$  modulo  $\text{Gal}(N/L)$ , then

$$G = \bigcup_{i=1}^n \sigma_i \text{Gal}(N/L).$$

Hence each  $\sigma \text{Gal}(N/L)$  is both open and closed. Thus  $G$  is a totally disconnected topological group. In particular,  $G$  is Hausdorff. To prove that  $G$  is compact, we give another presentation to the Krull topology.

To each  $L/L' \in \mathcal{L}_0$  with  $L \subseteq L'$  we associate the restriction map

$$\text{res}_{L',L}: \text{Gal}(L'/K) \rightarrow \text{Gal}(L/K)$$

and note that if  $L' \subseteq L'' \in \mathcal{L}_0$ , then  $\text{res}_{L'',L} = \text{res}_{L',L} \circ \text{res}_{L'',L'}$ . Then  $\langle L, \text{res}_{L',L} \rangle_{L, L' \in \mathcal{L}_0}$  is an ‘inverse system of finite groups’.

PROFINITE GROUPS. In general we consider a set  $I$  with a partial ordering  $\leq$  such that

(2) for all  $i, j \in I$  there exists  $k \in I$  with  $i, j \leq k$ .

Suppose that for each  $i \in I$  there is a set  $S_i$  and for all  $i, j \in I$  with  $i \leq j$  there is a map  $\rho_{ji}: S_j \rightarrow S_i$  such that

(3a) if  $i \leq j \leq k$ , then  $\rho_{ki} = \rho_{ji} \circ \rho_{kj}$ ;

(3b)  $\rho_{ii}$  is the identity map of  $S_i$ .

We call  $\langle S_i, \rho_{ij} \rangle_{i, j \in I}$  and **inverse system**. Then **inverse limit** of  $\langle S_i, \rho_{ij} \rangle$  is the set

$$S = \{s \in \prod_{i \in I} S_i \mid \bigwedge_{i \leq j} \rho_{ji}(s_j) = s_i\}$$

together with the maps  $\rho_i: S \rightarrow S_i$  given by  $\rho_i(s) = s_i$ . We denote it by  $S = \varprojlim S_i$ .

If all  $S_i$  belong to a certain category, then we demand that the  $\rho_{ij}$  are morphisms in that category. Thus, if  $S_i$  are topological spaces, then  $\rho_{ji}$  are continuous maps. In

this case we endow  $S$  with the topology induced by that of  $\prod S_i$ . Then  $\rho_i$  are continuous. If  $S_i$  are groups, then  $\rho_{ji}$  are homomorphisms. In this case,  $S$  is a subgroup of  $\prod S_i$ . If  $S_i$  are finite groups, then we consider them also as discrete topological spaces. In this case we say that  $\varprojlim S_i$  is a **profinite group**.

*Example 1.1:*  $\langle \text{Gal}(L/K), \text{res}_{L'/L} \rangle_{L, L' \in \mathcal{L}_0}$  is an inverse system of finite groups in which each  $\text{res}_{L'/L}$  is surjective ■

LEMMA 1.2: *If each  $S_i$  is a Hausdorff space, then  $S$  is a closed subset of  $\prod S_i$ .*

*Proof:* Let  $s \in \bar{S}$  and  $j \geq i$ . We have to prove that  $\rho_{ji}(s_j) = s_i$ . Assume that  $\rho_{ji}(s_j) \neq s_i$ . Choose open disjoint subsets  $U_i$  and  $U'_i$  of  $S_i$  such that  $s_i \in U_i$  and  $\rho_{ji}(s_j) \in U'_i$ . Then  $U = U_i \times \rho_{ji}^{-1}(U'_i) \times \prod_{k \neq i, j} S_k$  is an open neighborhood of  $s$  in  $\prod S_i$ . So, there exists  $t \in U \cap S$ . In particular,  $t_i \in U_i$  and  $t_j \in \rho_{ji}^{-1}(U'_i)$ . Hence  $t_i = \rho_{ji}(t_j) \in U'_i$  and therefore  $U_i \cap U'_i \neq \emptyset$ , a contradiction. Conclude that  $s \in S$ . ■

LEMMA 1.3: *The inverse limit of a nonempty compact Hausdorff spaces is a nonempty compact Hausdorff space.*

*Proof:* By Lemma 1.2, we have only to prove that  $S = \varprojlim S_i$  is nonempty. Indeed, let  $k \geq j$ . As  $S_j$  and  $S_k$  are Hausdorff and  $\rho_{kj}$  is continuous, its graph  $\Gamma_{\rho_{kj}} = \{(s_k, s_j) \in S_k \times S_j \mid \rho_{kj}(s_k) = s_j\}$  is nonempty and closed. Hence,

$$R_{kj} = \{s \in \prod_{i \in I} S_i \mid \rho_{kj}(s_k) = s_j\} = (\rho_k \times \rho_j)^{-1}(\Gamma_{\rho_{kj}})$$

is nonempty and closed.

If  $k_1 \geq j_1, \dots, k_m \geq j_m$ , we choose  $j \geq j_1, \dots, j_m$  and  $k \geq k_1, \dots, k_m, j$ . Then  $R_{kj} \subseteq R_{k_1 j_1} \cap \dots \cap R_{k_m j_m}$ . It follows from the compactness of  $\prod_{i \in I} S_i$  that  $S = \prod_{k \leq j} R_{kj}$  is nonempty. ■

LEMMA 1.4: *The inverse limit  $S = \varprojlim S_i$  of totally disconnected spaces is totally disconnected.*

*Proof:* Assume that the connected component  $C(x)$  of a point  $x \in S$  contains another point  $y$ . Then there exists  $i$  such that  $\rho_i(x) \neq \rho_i(y)$ . Since  $\rho_i(C(x))$  is connected and

contains both  $\rho_i(x)$  and  $\rho_i(y)$  we must have  $\{\rho_i(x)\} = \rho_i(C(x)) = \rho_i(C(y)) = \{\rho_i(y)\}$ , a contradiction. ■

**COROLLARY 1.5:** *The inverse limit  $S = \varprojlim S_i$  of finite nonempty discrete spaces is nonempty, compact, Hausdorff, totally disconnected space. A basis for the open neighborhoods of a point  $x \in S$  is the collection  $\{\rho_i^{-1}(\rho_i(x)) \mid i \in I\}$ . It consists of open and closed sets. We call  $S$  a **profinite space**.*

*Remark 1.6:* In each topological space  $X$  the connected component  $C(x)$  of a point  $x \in X$  is contained in each open and closed set that contains  $x$ . So, if  $X$  is Hausdorff and has a basis for its topology which consists of open and closed sets, then  $C(x) = \{x\}$ .

Conversely, it can be shown, that if  $X$  is a totally disconnected, compact Hausdorff space, then  $X$  is a profinite space. ■

**COROLLARY 1.7:** *A profinite group  $G = \varprojlim G_i$  is a totally disconnected, compact Hausdorff group. A basis for the open neighborhoods of 1 consist of all normal open subgroups. Each open subgroup  $H$  of  $G$  is closed and has a finite index. Each closed subgroup  $H$  of finite index is open. Each closed subgroup  $H$  of  $G$  is an intersection of open subgroups.*

*Proof:* We prove only the latter statement. Suppose that  $x \in G$  belongs to every open subgroup that contains  $H$ . Then  $x \in NH$  for each open normal subgroup  $N$  of  $G$ . Thus  $xN \cap H \neq \emptyset$ . By compactness, there exists  $y \in \bigcap_N xN \cap H$ . Hence  $yx^{-1} \in \bigcap N = 1$ . Conclude that  $x = y \in H$ . ■

*Example 1.8:* Let  $N/K$  be a Galois extension and denote, as before, the collection of all finite Galois extensions  $L$  of  $K$  contained in  $N$  by  $\mathcal{L}_0$ . Then

$$\text{Gal}(N/K) \cong \varprojlim_{L \in \mathcal{L}_0} \text{Gal}(L/K) \quad \sigma \mapsto (\sigma|_L)_{L \in \mathcal{L}_0}$$

as topological groups. In particular,  $\text{Gal}(N/K)$  is a profinite group, hence compact. ■

**PROPOSITION 1.9** (The main theorem of Galois theory): *Let  $N/K$  be an arbitrary Galois extension. Then, the map  $L \mapsto \text{Gal}(N/L)$  maps the family of all intermediate*

fields between  $K$  and  $N$  onto the set of all closed subgroups of  $\text{Gal}(N/K)$ . The inverse map is given by  $H \mapsto N(H)$ . This correspondence satisfies the rule (1)

*Proof:* We prove here only that the correspondence is bijective.

Let  $L$  be an intermediate field. Then  $L \subseteq N(\text{Gal}(N/L))$ . Conversely, each  $x \in N(H)$  is contained in a finite Galois extension  $M$  of  $K$  contained in  $N$ . Since the map  $\text{res}: \text{Gal}(N/L) \rightarrow \text{Gal}(M/M \cap L)$  is surjective,  $\sigma x = x$  for each  $\sigma \in \text{Gal}(M/M \cap L)$ . Conclude from finite Galois theory that  $x \in M \cap L$ . Hence,  $N(\text{Gal}(N/L)) = L$ .

Conversely, let  $H$  be a closed subgroup of  $\text{Gal}(N/L)$  and let  $L = N(H)$ . Then  $H \leq \text{Gal}(N/L)$ . To show that  $\sigma \in \text{Gal}(N/L)$  belongs to  $H$  it suffices to show that  $\sigma$  belongs to the closure of  $H$ . Indeed, let  $M \subseteq N$  be a finite Galois extension of  $K$ . Then  $M \cap L = M(\text{res}_M H)$ . Hence, by finite Galois theory,  $\text{res}_M \sigma \in \text{Gal}(M/M \cap L) = \text{res}_M H$ . Therefore  $H \cap \sigma \text{Gal}(N/M)$  is nonempty. Conclude that  $\text{Gal}(N/N(H)) = H$ . ■

*Remark 1.10: Artin, Leptin, Waterhouse.* For each profinite group  $G$  there exists a Galois extension  $N/K$  such that  $\text{Gal}(N/K) \cong G$ . ■

THE GROUP (RING)  $\mathbb{Z}_p$  OF  $p$ -ADIC INTEGERS. It is defined as the inverse limit  $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i \mathbb{Z}$  with respect to the canonical maps  $\mathbb{Z}/p^j \mathbb{Z} \rightarrow \mathbb{Z}/p^i \mathbb{Z}$ ,  $z + p^j \mathbb{Z} \mapsto z + p^i \mathbb{Z}$ .  $\mathbb{Z}_p$  is both a profinite group and a profinite ring. The ring  $\mathbb{Z}$  naturally embeds into  $\mathbb{Z}_p$ , by  $z \mapsto (z + p^i \mathbb{Z})_{i=1,2,3,\dots}$ . The ring  $\mathbb{Z}$  is dense in  $\mathbb{Z}_p$  but is not equal to  $\mathbb{Z}_p$ :

$$\left( \sum_{i=0}^{n-1} p^i + p^n \mathbb{Z} \right)_{n=1,2,\dots} \in \mathbb{Z}_p \setminus \mathbb{Z},$$

(except for  $p = 2$ ; change the example in this case.) Each element of  $\mathbb{Z}_p$  can be uniquely written as a formal power series  $a = \sum_{i=0}^{\infty} a_i p^i$ , with  $0 \leq a_i \leq p - 1$ . The element  $a$  is invertible in  $\mathbb{Z}_p$  if and only if  $a_0 \neq 0$ .

THE LATTICE OF SUBGROUPS OF  $\mathbb{Z}_p$ .

(4a)  $p^i \mathbb{Z}_p$  is an open subgroup (ideal) of  $\mathbb{Z}_p$  of index  $p^i$ . It is isomorphic to  $\mathbb{Z}_p$  (as groups).

*Proof:* The subgroup  $p^i \mathbb{Z}_p$  is contained in the kernel of  $\rho_i: \mathbb{Z}_p \rightarrow \mathbb{Z}/p^i \mathbb{Z}$ . Conversely let  $x = (x_1, x_2, \dots) \in \mathbb{Z}_p$  be in the kernel of  $\rho_i$ . Then  $x_{j+i} \equiv x_j \equiv 0 \pmod{p^i}$  and

hence  $x_{j+i} = p^i y_j$  for each  $j \geq 1$ . If  $k \geq j$ , then  $x_{k+i} \equiv x_{j+i} \pmod{p^{j+i}}$  and hence  $y_k \equiv y_j \pmod{p^j}$ . So,  $y = (y_1, y_2, \dots) \in \mathbb{Z}_p$  and satisfies  $p^i y = x$ . Indeed,  $p^i y_j = x_{j+i} \equiv x_j \pmod{p^j}$  for  $j = 1, 2, \dots$ . It follows that  $p^i \mathbb{Z}_p = \text{Ker}(\rho_i)$ . Hence  $\mathbb{Z}_p/p_i \mathbb{Z} \cong \mathbb{Z}/p^i \mathbb{Z}$  and therefore  $p^i \mathbb{Z}_p$  has index  $i$  in  $\mathbb{Z}_p$ . ■

(4b) If  $H$  is a subgroup of  $\mathbb{Z}_p$  of a finite index, then  $H = p^i \mathbb{Z}_p$  for some  $i$ .

*Proof:* Let  $(\mathbb{Z}_p : H) = p^i k$  with  $p \nmid k$ . Then  $p^i \mathbb{Z}_p = p^i k \mathbb{Z}_p \leq H$ . Thus  $p^i = (\mathbb{Z}_p : p^i \mathbb{Z}_p) \geq (\mathbb{Z}_p : H) = p^i k \geq p^i$ . It follows that  $p^i \mathbb{Z}_p = H$ . ■

(4c) If  $H$  is a closed subgroup of  $\mathbb{Z}_p$  of infinite index, then  $H = 0$ .

THE PRÜFER GROUP (RING)  $\hat{\mathbb{Z}}$ . It is defined as the inverse limit

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

with respect to the natural maps  $x + n\mathbb{Z} \mapsto x + m\mathbb{Z}$  if  $m|n$ . So,  $\hat{\mathbb{Z}}$  is both a profinite group and a profinite ring.

(5a)  $\mathbb{Z}$  naturally embeds as a dense subset of  $\hat{\mathbb{Z}}$ .

(5b) Each  $n\hat{\mathbb{Z}}$  is an open subgroup of  $\hat{\mathbb{Z}}$  of index  $n$ . In fact, we have a short exact sequence  $0 \rightarrow n\hat{\mathbb{Z}} \rightarrow \hat{\mathbb{Z}} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$ .

(5c) If  $H$  is a subgroup of  $\hat{\mathbb{Z}}$  of index  $n$ , then  $H = n\hat{\mathbb{Z}}$ .

(5d)  $\hat{\mathbb{Z}} \cong \prod \mathbb{Z}_p$ .

*Proof:* The canonical maps  $\prod \mathbb{Z}_p \rightarrow \prod_{p|n} \mathbb{Z}/p^{k(p)}\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  with  $n = \prod p^{k(p)}$  (Chinese remainder theorem) are compatible and therefore define a continuous homomorphism  $f: \prod \mathbb{Z}_p \rightarrow \hat{\mathbb{Z}}$ , which is injective. It is the identity on  $\mathbb{Z}$ . So,  $f(\prod \mathbb{Z}_p)$  is a compact subset of  $\hat{\mathbb{Z}}$  which contains a dense subset. Thus  $f$  is also surjective. Finally, both spaces are Hausdorff and compact. Hence  $f$  is a homeomorphism. ■

THE ABSOLUTE GALOIS GROUP OF A FINITE FIELD.

$\mathbb{F}_q$  is the field with  $q$  elements.

$$\mathbb{F}_q = \{x \in \tilde{\mathbb{F}}_q \mid x^q = x\}.$$

$\mathbb{F}_{q^n}$  is the unique extension of  $\mathbb{F}_q$  of degree  $n$

$\varphi_n$  is the Frobenius generator of  $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ ,  $\varphi_n(x) = x^q$ .

Commutative diagram of isomorphisms

$$\begin{array}{ccc}
 \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} & & 1+n\mathbb{Z} & \longrightarrow & 1+m\mathbb{Z} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & \xrightarrow{\text{res}} & \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) & & \varphi_n & \longrightarrow & \varphi_m
 \end{array}$$

It follows that  $\text{Gal}(\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ , the Frobenius automorphism  $\varphi$  is mapped onto 1 and generates  $\text{Gal}(\mathbb{F}_q)$ .

In particular the discrete subgroup  $\{\varphi^n \mid n \in \mathbb{Z}\}$  has the same fixed field, namely  $\mathbb{F}_q$ , as the whole group  $\text{Gal}(\mathbb{F}_q)$ .

## 2. The Riemann Hypothesis over finite fields

A **place** of a field  $F$  is a function  $\varphi: F \rightarrow K \cup \{\infty\}$  such that  $\varphi(a + b) = \varphi(a) + \varphi(b)$  and  $\varphi(ab) = \varphi(a)\varphi(b)$ , whenever the right hand side is defined;

A **Prime divisor** is an equivalence class of places;

$\Gamma$  is an ordered abelian group;

A **valuation** of a field is a map  $v: F \rightarrow \Gamma \cup \{\infty\}$  such that  $v(ab) = v(a) + v(b)$ ,  $v(a + b) \geq \min\{v(a), v(b)\}$  and  $v(a) = \infty$  if and only if  $a = 0$ ;

A **valuation ring**  $R$  of a field, maximal ideal, residue field.

Correspondence between equivalence classes of places, equivalence classes of valuations and valuation rings of  $F$ .

*Example 2.1:*  $\mathbb{Z}_p$  is a valuation ring of  $\mathbb{Q}_p$ ;

$R$  a unique factorization domain with quotient field  $F$ . Each prime element  $p \in R$  corresponds to a prime divisor of  $F$ :

$$v_p\left(\frac{a}{b}p^i\right) = i, \quad a, b \in R, \quad p \nmid a, b;$$

$$\varphi_p\left(\frac{a}{b}p^i\right) = \begin{cases} 0 & i < 0 \\ \bar{a}/\bar{b} & i = 0; \\ \infty & i > 0 \end{cases} \quad R/pR \text{ is the residue field and } \bar{a} = a + pR$$

$$R_p = \left\{ \frac{a}{b} \mid a, b \in R, \quad p \nmid b \right\}$$

$R$  can be  $\mathbb{Z}$  with the primes  $2, 3, 5, 7, \dots$ . This gives all valuations of  $\mathbb{Q}$ . In addition there is the **infinite prime** associated with the absolute value.

Alternatively,  $R$  can be  $K[t]$ ; and the primes are irreducible polynomials  $p(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$ . The field  $F = K(t)$  has one more valuation:

$$v_\infty\left(\frac{f(t)}{g(t)}\right) = \deg(g) - \deg(f).$$

All these are example of **discrete valuations**. ■

**CHEVALLEY'S EXTENSION THEOREM:** Let  $\varphi_0: R_0 \rightarrow K$  be a homomorphism of an integral domain  $R_0$  into a field  $K$ . Let  $F$  be a field containing  $R_0$ . Then  $\varphi_0$  can be extended to a place  $\varphi: F \rightarrow \tilde{K} \cup \{\infty\}$ .

Let  $F$  be a finite extension of  $K(t)$  such that  $K$  is algebraically closed in  $F$ . Then  $F$  is a **function field of one variable** over  $K$ . Each prime  $\mathfrak{p}$  of  $K(t)/K$  extends to

finitely many primes  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  of  $F$ . The residue field  $\bar{F}_{\mathfrak{p}_i}$  is a finite extension of  $K$  and  $\deg(\mathfrak{p}_i) = [\bar{F}_{\mathfrak{p}_i} : K]$ .

We denote the space of all prime divisors of  $F/K$  by  $\mathcal{R}(F/K)$ . It is the **Riemann space** of  $F/K$ .

A **divisor** of  $F$  is a formal sum  $\mathfrak{a} = \sum_{i=1}^s a_i \mathfrak{q}_i$  with  $a_i \in \mathbb{Z}$ . We write  $v_{\mathfrak{q}_i}(\mathfrak{a}) = a_i$ .

**Degree of a divisor:**  $\deg(\mathfrak{a}) = \sum_{i=1}^s a_i \deg(\mathfrak{q}_i)$ .

To each  $f \in F^\times$  there corresponds a **principal divisor**

$$(f) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(f) \mathfrak{p}$$

where  $\mathfrak{p}$  ranges over all primes of  $F$ . However,  $v_{\mathfrak{p}}(f) \neq 0$  only for finitely many primes.

The **zero divisor** of  $f$ :  $(f)_0 = \sum_{v_{\mathfrak{p}}(f) > 0} v_{\mathfrak{p}}(f) \mathfrak{p}$ ;

The **pole divisor** of  $f$ :  $(f)_\infty = -\sum_{v_{\mathfrak{p}}(f) < 0} v_{\mathfrak{p}}(f) \mathfrak{p}$ ;

Then  $(f) = (f)_0 - (f)_\infty$  is the divisor of  $f$ . We have  $(fg) = (f) + (g)$ . By Chevalley's extension theorem,  $(f) = 0$  if and only if  $f \in K^\times$ .

If  $f \notin K$ , then  $\deg(f)_0 = \deg(f)_\infty = [F : K(f)]$  and  $\deg(f) = 0$ .

Partial order among divisors:  $\mathfrak{a} \leq \mathfrak{b}$  if and only if  $v_{\mathfrak{p}}(\mathfrak{a}) \leq v_{\mathfrak{p}}(\mathfrak{b})$  for all  $\mathfrak{p}$ .

Vector space over  $K$  attached to a divisor  $\mathfrak{a}$ :

$$\mathcal{L}(\mathfrak{a}) = \{f \in F \mid \mathfrak{a} + (f) \geq 0\}$$

$\dim(\mathfrak{a}) = \dim_K \mathcal{L}(\mathfrak{a}) < \infty$ .

Adele of  $F$  is a function  $\alpha: \mathcal{R}(F/K) \rightarrow F$  such that  $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \geq 0$  for almost all  $\mathfrak{p}$ .

We denote the  $F$ -algebra of adeles of  $F/K$  by  $\mathbb{A}$ .

Another vector space over  $K$  attached to a divisor  $\mathfrak{a}$ :

$$\Lambda(\mathfrak{a}) = \{\alpha \in \mathbb{A} \mid v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \geq 0 \text{ for all } \mathfrak{p} \in \mathcal{R}(F/K)\}$$

$$\delta(\mathfrak{a}) = \dim_K(\mathbb{A}/\Lambda(\mathfrak{a}) + F) < \infty.$$

**RIEMANN-ROCH THEOREM:** *There exists a unique nonnegative integer  $g$  (called the **genus** of  $F/K$ ) such that for each divisor  $\mathfrak{a}$ :*

$$\dim(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g + \delta(\mathfrak{a}).$$

Moreover:

- (1a)  $\dim(0) = 1$  ( $f \in F^\times$  implies  $\dim((f)) = 1$ );
- (2)  $\deg(\mathfrak{a}) < 0$  implies  $\dim(\mathfrak{a}) = 0$ ;
- (3)  $\deg(\mathfrak{a}) > 2g - 2$  implies  $\dim(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g$ .

*Example:* The genus of  $K(t)$  is 0. Conversely, if  $g(F) = 0$  and if  $F$  has a prime divisor of degree 1, then there exists  $u \in F$  such that  $F = K(u)$ .

THE FUNCTION FIELD OF A CURVE  $f(X, Y) = 0$ . Let  $f \in K[X, Y]$  be an absolutely irreducible polynomial of degree  $d$  over a field  $K$ . Thus  $f$  is irreducible in the ring  $\tilde{K}[X, Y]$ . Choose a transcendental element  $x$  over  $K$  and an element  $y \in \widetilde{K(x)}$  such that  $f(x, y) = 0$ . Then  $(x, y)$  is a **generic point** of the curve  $\Gamma: f(X, Y) = 0$ .

By assumption  $f(x, Y)$  is irreducible in  $\tilde{K}[x][Y]$  and **primitive** (i.e., the greatest common divisor in  $K[x]$  of the coefficients of  $f(x, Y)$  is 1). Hence, by Gauß lemma,  $f(x, Y)$  is irreducible in  $\tilde{K}(x)[Y]$ . It follows that  $[K(x, y) : K(x)] = \deg_Y f(x, Y) = [\tilde{K}(x, y) : \tilde{K}(x)]$ . Hence  $K(x, y) \cap \tilde{K}(x) = K(x)$  and since  $K(x) \cap \tilde{K} = K$ , also  $K(x, y) \cap \tilde{K} = K$ . Indeed, if  $K(x) \subset K(x, y) \cap \tilde{K}(x)$ , then  $[\tilde{K}(x, y) : \tilde{K}(x)] \leq [K(x, y) : K(x, y) \cap \tilde{K}(x)] < [K(x, y) : K(x)]$ .

Thus  $F = K(x, y)$  is a function field of one variable over  $K$ .

PROPOSITION ([FrJ, Cor. 4.8]): *The genus of  $F/K$  is at most  $\frac{1}{2}(d-1)(d-2)$ .*

THEOREM (Weil): *Let  $F$  be a function field of genus  $g$  over  $\mathbb{F}_q$ . Denote the number of prime divisors of  $F$  of degree 1 by  $N$ . Then*

$$(3) \quad |N - (q + 1)| \leq 2g\sqrt{q}.$$

*Remark:* One associates zeta functions to  $F$ :

$$\zeta_F(s) = \sum_{\mathfrak{a} \geq 0} q^{-\deg(\mathfrak{a})s}$$

$$Z_F(t) = \sum_{\mathfrak{a} \geq 0} t^{\deg(\mathfrak{a})}$$

where  $\mathfrak{a}$  ranges over all nonnegative divisors of  $F/\mathbb{F}_q$ . Then  $Z_F(t)$  has the following  $2g$  zeros  $w_i^{-1}$ ,  $i = 1, \dots, 2g$ . They satisfy

$$(4) \quad N - (q + 1) = w_1 + \dots + w_{2g}.$$

The Riemann Hypothesis for  $F$ , which Weil proved, states that all those zeros lie on the line  $\operatorname{Re}(s) = \frac{1}{2}$ . For each  $i$  there exists a zero  $s_i$  of  $\zeta_F(s)$  such that  $q^{-s_i} = w_i^{-1}$ . Hence,  $|w_i| = q^{\operatorname{Re}(s_i)} = \sqrt{q}$ . So, (2) is a consequence of (3).

Combine Weil's theorem with the estimate for the genus to get

$$(4) \quad |N - (q + 1)| \leq (d - 1)(d - 2)\sqrt{q}.$$

**THEOREM** ([FrJ, Thm. 4.9]): *Let  $f \in \mathbb{F}_q[X, Y]$  be an absolutely irreducible polynomial of degree  $d$ . Let  $N' = \{(a, b) \in \mathbb{F}_q^2 \mid f(a, b) = 0\}$ . Then*

$$(q + 1) - (d - 1)(d - 2)\sqrt{q} - d \leq N' \leq q + 1 + (d - 1)(d - 2)\sqrt{q}.$$

**COROLLARY:**

(a) *If  $q > (d - 1)^4$ , then  $N' > 0$ .*

(b) *For each  $m$  there exist  $q_0 = q_0(d, m)$  such that for all  $q \geq q_0$  we have  $N' \geq m$ .*

### 3. Elements of model theory

FIRST ORDER PREDICATE CALCULUS. A **signature** is a triple  $(\mu, \nu, K)$  consisting of two functions:  $\mu: I \rightarrow \mathbb{N}$ ,  $\nu: J \rightarrow \mathbb{N}$ , and a set  $K$ .

We associate a **language**  $\mathcal{L}(\mu, \nu, K)$  with this signature. The **letters** of  $\mathcal{L}(\mu, \nu, K)$  are:

**Variable symbols**  $X_1, X_2, X_3, \dots$

Constant symbols  $c_k$  for each  $k \in K$

$\mu_i$ -ary relation symbol  $R_i$ ,  $i \in I$

$\nu_j$ -ary function symbol  $F_j$ ,  $j \in J$

equality symbol  $=$

negative symbol  $\neg$ , disjunction symbol  $\vee$ , existential quantifier symbol  $\exists$

parenthesis  $( )$  and brackets  $[ ]$ .

*Example:* We denote the language of ring theory by  $\mathcal{L}(\text{ring})$ . It has of two binary function symbols:  $+$  and  $\cdot$ , and two constant symbols  $0$  and  $1$ . ■

A **string** is a finite sequence of letters. **words** are **terms** and **formulas**.

The collection of **terms** is the smallest set of strings that contains

$X_i$ ,  $i = 1, 2, 3, \dots$

$C_k$ ,  $k \in K$

and satisfies the following rule:

For each  $j \in J$ , if  $t_1, \dots, t_{\nu_j}$  are terms, then so is  $F_j(t_1, \dots, t_{\nu_j})$ .

For example, in  $\mathcal{L}(\text{ring})$ , polynomials in several variables are terms.

**Atomic formulas** are:

$t = t'$ , where  $t, t'$  are terms

$R_i(t_1, \dots, t_{\mu_i})$ , where  $i \in I$  and  $t_1, \dots, t_{\mu_i}$  are terms.

The set of **formulas** is the smallest collection of strings that contains all atomic formulas and satisfy the following rules:

$\varphi$  is a formula implies that  $\neg[\varphi]$  is a formula;

$\varphi_1, \varphi_2$  are formulas imply that  $\varphi_1 \vee \varphi_2$  is a formula;

$\varphi$  is a formula implies that  $(\exists X_i)[\varphi]$  is a formula.

Induction by structure for terms and formulas.

**Free occurrence** of  $X$  in a formulas  $\varphi$ :

Any occurrence of  $X$  in an atomic formula is free.

If an occurrence of  $X$  in  $\varphi$  is free,  $\psi$  is any formula and  $Y \neq X$ , then the occurrence of  $X$  in  $\neg[\varphi]$ ,  $\varphi \vee \psi$ , and  $(\exists Y)[\varphi]$  is free.

If  $X$  has a free occurrence in  $\varphi$ , then  $X$  is a **free variable** of  $\varphi$ . We write  $\varphi(X_1, \dots, X_n)$  to indicate that the free variables of  $\varphi$  belong to the set  $\{X_1, \dots, X_n\}$ . A formula without a free variables is a **sentence**.

*Examples:*  $(\exists X)[X^2 = 2]$  is a sentence.  $X_1^n + X_2^n = X_3^n$  is a formula with three free variables. ■

Abbreviations:

$\varphi \wedge \psi$  for  $\neg[\neg\varphi \vee \neg\psi]$       **conjunction**

$\varphi \rightarrow \psi$  for  $\neg\varphi \vee \psi$       **implication**

$\varphi \leftrightarrow \psi$  for  $[\varphi \rightarrow \psi] \wedge [\psi \rightarrow \varphi]$       **double implication**

$(\forall X_i)[\varphi]$  for  $\neg(\exists X_i)[\neg\varphi]$       **universal quantifier**

$\bigwedge_{i=1}^n \varphi_i$  for  $\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n$

$\bigvee_{i=1}^n \varphi_i$  for  $\varphi_1 \vee \varphi_2 \vee \dots \vee \varphi_n$ .

A formula in **prenex normal form**:

$$(Q_1 X_1) \cdots (Q_m X_m) \left[ \bigvee_{i=1}^m \bigvee_{j=1}^n [f_{ij}(\mathbf{X}, \mathbf{Y}) = 0 \wedge g_{ij}(\mathbf{X}, \mathbf{Y}) \neq 0] \right]$$

where each  $Q_i$  is either  $\exists$  or  $\forall$  and  $f_{ij}, G_{ij}$  are polynomials with coefficients in a field  $K$ .

**STRUCTURES.** A **structure** for a language  $\mathcal{L}(\mu, \nu, K)$  is a system

$$\mathcal{A} = \langle A, \bar{R}_i, \bar{F}_j, \bar{c}_k \mid i \in I, j \in J, k \in K \rangle$$

$A$  is a nonempty set — the **domain** of  $\mathcal{A}$ ;

$\bar{R}_i \subseteq A^{\mu_i}$  is a  $\mu_i$ -ary relation on  $A$ ;

$\bar{F}_j: A_j^\nu \rightarrow A$  is a  $\nu_j$ -ary function on  $A$ ;

$\bar{c}_k \in A$  is a constant.

**Substitution**  $f: \{X_1, X_2, \dots\} \rightarrow A$ ,  $f(X_i) = x_i$ , extends to terms:

$$f(c_k) = \bar{c}_k;$$

$$f(F_j(t_1, \dots, t_{\nu_j})) = \bar{F}_j(f(t_1), \dots, f(t_{\nu_j})).$$

**Truth value** of a formula under the substitution  $f$  is defined to be either ‘true’ or ‘false’ by induction on the structure:

$$t = t' \text{ is true if and only if } f(t) = f(t');$$

$$R_i(t_1, \dots, t_{\mu_i}) \text{ is true if and only if } (f(t_1), \dots, f(t_{\mu_i})) \in \bar{R}_i.$$

Suppose that the truth values of  $\varphi, \varphi_1, \varphi_2$  have been defined for all possible substitutions. Then under  $f$

$$\neg\varphi \text{ is true if and only if } \varphi \text{ is false;}$$

$$\varphi_1 \vee \varphi_2 \text{ is true if and only if } \varphi_1 \text{ is true or } \varphi_2 \text{ is true;}$$

$$(\exists X_l)[\varphi] \text{ is true if and only if there exists } x \in A \text{ such that } \varphi \text{ is true under the substitution } g \text{ which is defined by: } g(X_l) = x \text{ and } g(X_m) = f(X_m) \text{ if } m \neq l.$$

One proves that the truth value of a formula  $\varphi(X_1, \dots, X_n)$  depends only on  $f(X_1) = x_1, \dots, f(X_n) = x_n$ . We write then  $\mathcal{A} \models \varphi(x_1, \dots, x_n)$ . If  $\varphi$  is a sentence, then its truth value is independent of  $f$ . Either  $\mathcal{A} \models \varphi$  or  $\mathcal{A} \not\models \varphi$ .

**MODELS.** A **theory** for a language  $\mathcal{L} = \mathcal{L}(\mu, \nu, K)$  is a set of sentences of  $\mathcal{L}$ . A structure  $\mathcal{A}$  for  $\mathcal{L}$  is a **model** of  $T$  if  $\mathcal{A} \models \theta$  for each  $\theta \in T$ . We then write  $\mathcal{A} \models T$ .

A theory  $\Pi$  is a set of **axioms** for  $T$  if  $\Pi \models T$ . That is, each model of  $\Pi$  is also a model of  $T$ .

*Example:* The theory of fields has the following set of axioms:

$$(\forall X)(\forall Y)(\forall Z)[(X + Y) + Z = X + (Y + Z)]$$

$$(\forall X)(\forall Y)[X + Y = Y + X]$$

$$(\forall X)[X + 0 = X]$$

$$(\forall Y)(\exists X)[X + Y = 0]$$

$$(\forall X)(\forall Y)(\forall Z)[(XY)Z = X(YZ)]$$

$$(\forall X)(\forall Y)[XY = YX]$$

$$(\forall X)(X \cdot 1 = X)$$

$$\begin{aligned}
& (\forall X)[X \neq 0 \rightarrow (\exists Y)[XY = 1]] \\
& 0 \neq 1 \\
& (\forall X)(\forall Y)(\forall Z)[X(Y + Z) = XY + XZ]
\end{aligned}$$

Let  $R$  be an integral domain. Add the elements of  $R$  to the constant symbols of  $\mathcal{L}(\text{ring})$  to obtain the language  $\mathcal{L}(\text{ring}, R)$ . Add the **positive diagram** of  $R$  to the axioms  $\Pi$ :

$\Pi(R)$ : All equalities  $a + b = c$  and  $a'b' = c'$  that hold in  $R$ .

A **model** of  $\Pi(R)$  is a field that contains the set  $\bar{R} = \{\bar{a} \mid a \in R\}$  and satisfies  $\bar{a} + \bar{b} = \bar{c}$  and  $\bar{a}\bar{b} = \bar{c}$  whenever  $a + b = c$  and  $ab = c$ , respectively. Thus  $\bar{R}$  is a homomorphic image of  $R$  (e.g.,  $R = \mathbb{Z}$  and  $\bar{R}$  is a field of characteristic  $p$ ).

An **elementary statement** about models of  $\Pi(R)$  is a mathematical statement that applies to each model of  $\Pi(R)$  and for which there exists a sentence  $\theta$  of  $\mathcal{L}(\text{ring}, R)$  which is true in a model if and only if the statement is true in that model.

*Example:*  $f(X_1, \dots, X_n)$  is a polynomial of degree  $d$  with coefficients in  $R$ . Then ‘ $f(\mathbf{X})$  is irreducible’ is equivalent to ‘ $\bigwedge_{l+m=n}$  there exist no polynomials  $g(\mathbf{X})$  and  $h(\mathbf{X})$  of degrees  $d$  and  $e$  respectively such that  $f(\mathbf{X}) = g(\mathbf{X})h(\mathbf{X})$ ’. The phrase ‘there exists a polynomial  $g(\mathbf{X})$  of degree  $d$ ’ should be replaced by ‘ $(\exists u_1) \cdots (\exists u_k)$ ’, where  $u_1, \dots, u_k$  are the coefficients of  $g$ . The equality  $f(\mathbf{X}) = g(\mathbf{X})h(\mathbf{X})$  should be replaced by a conjunction of equalities between the coefficients of monomials of the same degrees on both sides.

ELEMENTARY EQUIVALENT STRUCTURES.  $\mathcal{A} \equiv \mathcal{B}$

EXTENSION OF STRUCTURES. Let  $\mathcal{A} = \langle A, \bar{R}_i, \bar{F}_j, \bar{c}_k \rangle$ ,  $\mathcal{B} = \langle B, R'_i, F'_j, c'_k \rangle$ . Then  $\mathcal{A} \subseteq \mathcal{B}$ , if

$$\begin{aligned}
& A \subseteq B \text{ and for } a_1, a_2, a_3, \dots \in A \text{ we have} \\
& (a_1, \dots, a_{\mu_i}) \in R_i \text{ if and only if } (a_1, \dots, a_{\mu_i}) \in R'_i \\
& \bar{F}_j(a_1, \dots, a_{\nu_j}) = F'_j(a_1, \dots, a_{\nu_j}) \\
& \bar{c}_k = c'_k.
\end{aligned}$$

ELEMENTARY EXTENSIONS.  $\mathcal{A} \prec \mathcal{B}$ :  $\mathcal{A} \subseteq \mathcal{B}$  and for all  $a_1, \dots, a_n \in A$  we have  $\mathcal{A} \models \varphi(a_1, \dots, a_n)$  if and only if  $\mathcal{B} \models \varphi(a_1, \dots, a_n)$ .

*Example:* If a field  $K$  is an elementary subfield of a field  $F$ , then  $K$  is algebraically closed in  $F$ .

Indeed, take  $x \in \tilde{K} \cap F$  and  $f = \text{irr}(x, K) = X^n + a_1X^{n-1} + \dots + a_n$ .

$$F \models (\exists X)[X^n + a_1X^{n-1} + \dots + a_n = 0].$$

Hence

$$K \models (\exists X)[X^n + a_1X^{n-1} + \dots + a_n = 0].$$

Hence,  $\deg(f) = 1$  and  $x \in K$ . ■

THE SKOLEM-LÖWENHEIM THEOREM: Let  $\mathcal{L}$  be a countable language. Consider a structure  $\mathcal{B} = \langle B, S_i, G_j, d_k \rangle$  for  $\mathcal{L}$ , and let  $A_0$  a countable subset of  $B$ . Then  $\mathcal{B}$  has a countable elementary substructure  $\mathcal{A} = \langle A, R_i, F_j, c_k \rangle$  such that  $A_0 \subseteq A$ .

*Proof:* By induction on  $n$  define sets  $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots \subseteq B$ . If  $A_n$  has been defined, then  $A_{n+1}$  consists of all  $d_k$  with  $k \in K$ . In addition, if  $\varphi(X_1, \dots, X_m)$  is a formula,  $x_1, \dots, x_{m-1} \in A_n$  and  $\mathcal{B} \models (\exists X_m)\varphi(x_1, \dots, x_{m-1}, X_m)$ , then choose one  $x_m \in B$  such that  $\mathcal{B} \models \varphi(x_1, \dots, x_{m-1}, x_m)$  and add it to  $A_{n+1}$ .

Define  $A = \bigcup_{i=0}^{\infty} A_i$ ,  $R_i = S_i \cap A^{\mu_i}$ ,  $F_j = G_j|_{A^{\nu_j}}$ . Then prove by induction on formulas  $\varphi(X_1, \dots, X_n)$  and for  $\mathbf{x} \in A^n$ :

$$\mathcal{A} \models \varphi(\mathbf{x}) \quad \text{if and only if} \quad \mathcal{B} \models \varphi(\mathbf{x}).$$

Note that each term  $t(X_1, \dots, X_n)$  has the same values on  $A^\mu$  in both  $\mathcal{A}$  and  $\mathcal{B}$ . Check for atomic formulas and then for compound formulas. ■

ULTRAFILTERS. An **ultrafilter** of a set  $S$  is a family  $\mathcal{D}$  of subsets of  $S$  with the following property:

- (1a)  $\emptyset \notin \mathcal{D}$
- (1b)  $A \in \mathcal{D}$  and  $A \subseteq B \subseteq S$  imply  $B \in \mathcal{D}$
- (1c)  $A \in \mathcal{D}$  and  $B \in \mathcal{D}$  imply  $A \cap B \in \mathcal{D}$

(1d) For each  $A \in S$ , either  $A \in \mathcal{D}$  or  $S - A \in \mathcal{D}$ .

It follows

(1e)  $S \in \mathcal{D}$

(1f)  $A \cup B \in \mathcal{D}$  implies  $A \in \mathcal{D}$  or  $B \in \mathcal{D}$ .

We refer to sets in  $\mathcal{D}$  as **big**. If a property of elements of  $S$  is true for all  $a \in S$  that belong to a set in  $\mathcal{D}$ , we say that it holds for almost all  $a \in S$ .

*Example:* For each  $a \in S$ , the family

$$\mathcal{D} = \{A \subseteq S \mid a \in A\}$$

is the **principal ultrafilter** generated by  $a$ .

If  $\mathcal{D}$  is a nonprincipal ultrafilter of  $S$ , then  $\mathcal{D}$  contains all cofinite subsets of  $S$ .

A family  $\mathcal{D}$  of subsets of  $S$  is a **filter** if it satisfies only (1a), (1b), and (1c). ■

LEMMA: *a filter  $\mathcal{D}$  of  $S$  is an ultrafilter if and only if it is maximal filter.*

*Proof:* If  $S - A \notin \mathcal{D}$ , then

$$\mathcal{D}' = \mathcal{D} \cup \{B \cap D \mid A \subseteq B \subseteq S \text{ and } D \in \mathcal{D}\}$$

is a filter that contains  $\mathcal{D}$ . So, if  $\mathcal{D}$  is maximal, then  $\mathcal{D}' = \mathcal{D}$  and  $A \in \mathcal{D}$ . ■

A family  $\mathcal{D}_0$  of subsets of  $S$  has the **finite intersection property** if it satisfies (1a) and (1c).

LEMMA:

(a) *Each family  $\mathcal{D}_0$  that satisfies the finite intersection property is contained in a filter  $\mathcal{D}_1$ .*

(b) *Each filter  $\mathcal{D}_1$  is contained in an ultrafilter  $\mathcal{D}$ .*

*Proof of (a):*  $\mathcal{D}_1 = \{E \subseteq S \mid \exists D_1, \dots, D_m \in \mathcal{D}_0: D_1 \cap \dots \cap D_m \subseteq E\}$ .

*Proof of (b):* Use Zorn's lemma to choose a maximal filter  $\mathcal{D}$  that contains  $\mathcal{D}_1$ . ■

LEMMA: Let  $\mathcal{D}_0$  be a family of sets with the following property:

$$A_1, \dots, A_m \in \mathcal{D}_0 \quad \text{implies} \quad A_1 \cap \dots \cap A_m \text{ is an infinite set.}$$

Then there exists a nonprincipal ultrafilter  $\mathcal{D}$  of  $S$  that contains  $\mathcal{D}_0$ .

*Proof:* The family  $\mathcal{D}_1$  that consists of  $\mathcal{D}_0$  and all cofinite sets of  $S$  has the finite intersection property. Take  $\mathcal{D}$  to be an ultrafilter that contains  $\mathcal{D}_1$ . ■

ULTRAPRODUCTS. Consider a language  $\mathcal{L} = \mathcal{L}(\mu, \nu, K)$ , a set  $S$  and an ultrafilter  $\mathcal{D}$  on  $S$ . For each  $s \in S$ , let  $\mathcal{A}_s = \langle A_s, R_{is}, F_{js}, c_{ks} \rangle_{i \in I, j \in J, k \in K}$  be a structure of the language  $\mathcal{L}$ .

Construct the **ultraproduct** of the structures  $\mathcal{A}_s$  modulo  $\mathcal{D}$ :  $\mathcal{A} = \prod_{s \in S} \mathcal{A}_s / \mathcal{D}$ . It is the structure  $\mathcal{A} = \langle A, R_i, F_j, c_k \rangle$ , where  $A$  is the cartesian product  $\prod_{s \in S} A_s$  modulo the equivalent relation:

$$a \sim b \quad \iff \quad \{s \in S \mid a_s = b_s\} \in \mathcal{D}.$$

Use representatives instead of classes:

$$(a_1, \dots, a_{\mu_i}) \in R_i \quad \iff \quad \{s \in S \mid (a_{1s}, \dots, a_{\mu_i s}) \in R_{is}\} \in \mathcal{D}$$

$F_j(b_1, \dots, b_{\nu_j})$  is the equivalence class of  $F_{js}(b_{1s}, \dots, b_{\nu_j s})$

$c_k$  is the equivalence class of  $c_{ks}$ .

CLAIM: If  $t(X_1, \dots, X_n)$  is a term of  $\mathcal{L}$  and  $x_1, \dots, x_n \in A$ , then

$$\{s \in S \mid t(x_1, \dots, x_n)_s = t(x_{1s}, \dots, x_{ns})\} \in \mathcal{D}.$$

THE FUNDAMENTAL PROPERTY OF ULTRAPRODUCT (Łos):

For each formula  $\varphi(X_1, \dots, X_n)$  and all  $x_1, \dots, x_n \in A$  we have:

$$\mathcal{A} \models \varphi(x_1, \dots, x_n) \quad \iff \quad \{s \in S \mid \mathcal{A}_s \models \varphi(x_{1s}, \dots, x_{ns})\} \in \mathcal{D}.$$

COROLLARY: If  $\theta$  is a sentence of  $\mathcal{L}$ , then

$$\mathcal{A} \models \theta \quad \iff \quad \{s \in S \mid \mathcal{A}_s \models \theta\} \in \mathcal{D}.$$

*Example: Ultraproduct of fields.* If  $\mathcal{A}_s$  is a field, so is  $\mathcal{A} = \prod \mathcal{A}_s/\mathcal{D}$ .

If each  $\mathcal{A}_s$  is algebraically closed, so is  $\mathcal{A}$ .

If  $K_p$  is of characteristic  $p$ , and  $\mathcal{D}$  is nonprincipal, then  $\prod K_p/\mathcal{D}$  is of characteristic 0.

An ultraproduct of perfect fields of characteristic  $p$  is perfect. ■

**SATURATION THEOREM:** Let  $\mathcal{A} = \prod_{s \in \mathbb{N}} \mathcal{A}_s/\mathcal{D}$  be a nonprincipal ultraproduct. Suppose that  $r(1) < r(2) < r(3) < \dots$  is an increasing sequence of positive integers and for each  $n \in \mathbb{N}$ ,  $\varphi_n(X_1, \dots, X_{r(n)})$  is a formula of  $\mathcal{L}$  such that

$$(2) \quad \mathcal{A} \models (\exists X_1) \cdots (\exists X_{r(n)}) \left[ \bigwedge_{i=1}^n \varphi_i(X_1, \dots, X_{r(i)}) \right]$$

Then there exist  $x_1, x_2, x_3, \dots$  such that

$$(3) \quad \mathcal{A} \models \varphi_n(x_1, \dots, x_{r(n)}) \quad \text{for } n = 1, 2, 3, \dots$$

We say that  $\mathcal{A}$  is  $\aleph_1$ -saturated.

*Proof:* To simplify notation suppose that  $r(n) = n$ . Then

$$D_n = \{s \in \mathbb{N} \mid \mathcal{A}_s \models (\exists X_1) \cdots (\exists X_n) \left[ \bigwedge_{k=1}^n \varphi_k(X_1, \dots, X_{r(i)}) \right]\}$$

belongs to  $\mathcal{D}$  and  $D_1 \supseteq D_2 \supseteq D_3 \supseteq \dots$ . Since  $\mathcal{D}$  is nonprincipal  $D'_n = D_n \setminus \{1, 2, \dots, n\}$  also belongs to  $\mathcal{D}$ ,  $D'_1 \supseteq D'_2 \supseteq D'_3 \supseteq \dots$ , and  $\bigcap_{n=1}^{\infty} D'_n = \emptyset$ .

For each  $s \in D'_n \setminus D'_{n+1}$  choose  $x_{1s}, \dots, x_{ns} \in \mathcal{A}_s$  such that

$$\mathcal{A}_s \models \bigwedge_{k=1}^n \varphi_k(x_{1s}, \dots, x_{ks}).$$

Since,  $\bigcap_{n=1}^{\infty} D'_n = \emptyset$ , this defines  $x_{ks}$  for each  $s \in D'_k$ . For  $s \in \mathbb{N} \setminus D'_k$  define  $x_{ks}$  arbitrarily. Then  $x_k$  satisfies (3). ■

*Example:* If  $K_n/K$  is separable of degree  $> n$ , then  $\prod K_n/\mathcal{D}$  is not algebraic over  $K^{\mathbb{N}}/\mathcal{D}$ .

Let  $K_n$  is the field generated over  $\mathbb{Q}$  by all Galois extensions of order  $\leq n$ . The order of each element of  $\text{Gal}(K_n/K)$  is at most  $n$ . Hence  $K_n \neq \tilde{\mathbb{Q}}$ . But  $\prod K_n/\mathcal{D}$  contains  $\tilde{\mathbb{Q}}$ . ■

#### 4. Ultraproducts of finite fields

Ultraproducts of finite fields have the elementary properties which almost all finite fields have. For example ‘absolute irreducibility’ is an elementary property.

LEMMA: Let  $f \in K[X_0, \dots, X_{n-1}]$  be a polynomial of degree  $< d$ . If  $f$  factors over  $\tilde{K}$ , then it factors over an extension of  $K$  of degree  $< d^n!$ .

*Proof:* Suppose that  $f(\mathbf{X}) = g(\mathbf{X})h(\mathbf{X})$  with  $g, h \in \tilde{K}[\mathbf{X}]$ . Make the **Kronecker substitution**

$$X_0 \mapsto T, \quad X_1 \mapsto T^d, \quad \dots, \quad X_{n-1} \mapsto T^{d^{n-1}}$$

to get polynomials  $f^*(T), g^*(T), h^*(T)$  with  $f^*(T) = g^*(T)h^*(T)$ . Thus, if

$$f(\mathbf{X}) = \sum a_i X_0^{i_0} X_1^{i_1} \dots X_{n-1}^{i_{n-1}},$$

then

$$f^*(T) = \sum a_i T^{i_0 + i_1 d + \dots + i_{n-1} d^{n-1}}.$$

Note that  $(i_0, \dots, i_{n-1}) \neq (j_0, \dots, j_{n-1})$  implies

$$i_0 + i_1 d + \dots + i_{n-1} d^{n-1} \neq j_0 + j_1 d + \dots + j_{n-1} d^{n-1}.$$

Hence, the set of coefficients of  $f(\mathbf{X})$  (resp.,  $g(\mathbf{X}), h(\mathbf{X})$ ) is the same as that of  $f^*(T)$  (resp.,  $g^*(T), h^*(T)$ ).

Since  $\deg(f^*(T)) < d^n$ , the coefficients of  $g^*(T)$  and  $h^*(T)$ , hence those of  $g(T)$  and  $h(T)$ , belong to an extension of degree  $< d^n!$  of  $K$ , namely, the splitting field of  $f^*(T)$  over  $K$ . ■

PROPOSITION: The close ‘each absolutely irreducible polynomial of degree  $< d$  in  $K[X_1, \dots, X_n]$ ’ is elementary.

*Proof:* Let  $f \in K[X_1, \dots, X_n]$  be a polynomial of degree  $d$ . Then

(1)  $f$  is absolutely irreducible

is equivalent to

(2a)  $f$  is irreducible over each separable extension of  $K$  of degree  $< d^n!$  and

(2b)  $\bigvee_{i=1}^n \frac{\partial f}{\partial X_i} \neq 0$  (which means that  $f$  is not a  $p$ th power of a polynomial over  $\tilde{K}$ , where  $p = \text{char}(K)$ ).

If  $L$  is a separable extension of degree  $< d^{n!}$ , then  $L = K(y)$ , where  $h = \text{irr}(y, K)$  has degree  $< d^{n!}$ . Thus (2a) is equivalent to

- (3) There exist no polynomials  $g_1, g_2, g_3 \in K[\mathbf{X}, Y]$  such that
- (a)  $\deg_Y(g_i) < d^{n!}, \quad \deg_{\mathbf{X}}(g_i) < d$
  - (b)  $\deg_Y(g_3) < 2(d^{n!}) \quad \deg_X(g_3) < d$
  - (c)  $f(\mathbf{X}) = g_1(\mathbf{X}, Y)g_2(\mathbf{X}, Y) + g_3(\mathbf{X}, Y)h(Y)$ . ■

**COROLLARY:** Let  $F = \prod_{s \in S} F_s / \mathcal{D}$  be a nonprincipal ultraproduct of finite fields such that  $\{s \in S \mid |F_s| \leq n\}$  is finite for each  $n$ . Then each absolutely irreducible polynomial  $f \in F[X, Y]$  has infinitely many zeros in  $F$ .

**COROLLARY:** Let  $F = \prod_{s \in S} F_s / \mathcal{D}$  be a nonprincipal ultraproduct of finite fields such that  $\{s \in S \mid |F_s| \leq n\}$  is finite for each  $n$ . Then each absolutely irreducible polynomial  $f \in F[X_1, \dots, X_n]$  has infinitely many zeros in  $F$ .

*Proof:* Use Bertini-Noether to reduce to the case where  $n = 2$ . ■

To investigate the absolute Galois group of ultraproducts of finite fields, we have to prove that realizability of a finite group over a field is an elementary statement on this field.

**LEMMA:** Let  $L = K(x)$  be a Galois extension of degree  $n$  of a field  $K$  and let  $f = \text{irr}(x, K)$ . Let  $p_i \in K[X]$  be polynomials of degree at most  $n - 1$  such that  $p_1(X) = X$  and  $x_i = p_i(x)$ ,  $i = 1, \dots, n$  are the  $n$  roots of  $f$ . Let  $G$  be a subgroup of  $S_n$ . Then  $\text{Gal}(f, K) = G$  if and only if

$$(4) \quad \bigwedge_{\sigma \in G} \bigwedge_{i=1}^n [p_{\sigma(i)}(x) = p_i(p_{\sigma(1)}(x))] \wedge \bigwedge_{\sigma \in S_n \setminus G} \bigvee_{i=1}^n [p_{\sigma(i)}(x) \neq p_i(p_{\sigma(1)}(x))].$$

*Proof:* We identify  $\text{Gal}(f, K)$  with a subgroup of  $S_n$  through its action on  $\{x_1, \dots, x_n\}$ . Thus, each  $\sigma \in \text{Gal}(f, K)$  satisfies

$$(5) \quad \sigma x_i = x_{\sigma(i)}, \quad i = 1, \dots, n.$$

Since  $\sigma$  is an automorphism of  $L$  over  $K$ , Condition (5) is equivalent to

$$(6) \quad p_i(p_{\sigma(1)}(x)) = p_{\sigma(i)}(x) \quad i = 1, \dots, n.$$

Conversely, suppose that an element  $\sigma \in S_n$  satisfies (6). As  $f$  is irreducible, there exists a unique  $\tau \in \text{Gal}(f, K)$  such that  $\tau x = x_{\sigma(1)}$ . By (5) and (6),

$$x_{\tau(i)} = \tau x_i = \tau p_i(x) = p_i(\tau x) = p_i(x_{\sigma(1)}) = p_i(p_{\sigma(1)}(x)) = p_{\sigma(i)}(x) = x_{\sigma(i)},$$

for  $i = 1, \dots, n$ . Hence  $\sigma = \tau \in \text{Gal}(f, K)$ .

Conclude that  $\text{Gal}(f, K) = G$  if and only if (4) holds.  $\blacksquare$

**COROLLARY:** For each monic Galois polynomial  $f \in K[X]$  of degree  $n$  and each  $G \leq S_n$ , the statement ‘ $\text{Gal}(f, K) \cong G$ ’ is elementary.

**COROLLARY:** Let  $F$  be an ultraproduct of finite fields. Then

- (a) every finite extension of  $F$  is cyclic;
- (b) each  $\mathbb{Z}/n\mathbb{Z}$  occurs as a Galois group over  $F$ ;
- (c)  $\text{Gal}(F) \cong \hat{\mathbb{Z}}$ .

The proof of (c) includes depends on the following results:

**LEMMA:** For each profinite group  $G$  and each  $\sigma \in G$  there exists a unique homomorphism  $h: \hat{\mathbb{Z}} \rightarrow G$  such that  $h(1) = \sigma$ .

*Proof:* First for  $G$  finite. Uniqueness allows  $G$  to be infinite.  $\blacksquare$

**LEMMA:**

- (a) If each finite quotient of  $G$  is cyclic, then  $G$  is generated by one element ( $G$  is **pro-cyclic**).
- (b) If in addition, each  $\mathbb{Z}/n\mathbb{Z}$  is a quotient of  $G$ , then  $G \cong \hat{\mathbb{Z}}$ .

*Proof of (a):* If  $G = \varprojlim G_i$ , then the inverse limit of  $S_i = \{\sigma \in G_i \mid G_i = \langle \sigma \rangle\}$  is nonempty.

*Proof of (b):* There exists an epimorphism  $\alpha: \hat{\mathbb{Z}} \rightarrow G$ . For each  $n$ ,  $G$  has an open normal subgroup  $G_n$  such that  $G/G_n \cong \mathbb{Z}/n\mathbb{Z}$ . Hence  $\alpha^{-1}(G_n) = n\hat{\mathbb{Z}}$ . So,  $\text{Ker}(\alpha) \leq \bigcap_{n=1}^{\infty} \alpha^{-1}(G_n) = \bigcap_{n=1}^{\infty} n\hat{\mathbb{Z}} = 0$ .  $\blacksquare$

The proof of (b) gives:

COROLLARY: *If  $\alpha: \hat{\mathbb{Z}} \rightarrow \hat{\mathbb{Z}}$  is an epimorphism, then it is an isomorphism. If  $\hat{\mathbb{Z}} \xrightarrow{\alpha} G \xrightarrow{\beta} \hat{\mathbb{Z}}$  are epimorphisms, then they are isomorphisms.*

## 5 Linear disjointness of fields

Central to field theory is the concept “linear disjointness of fields,” an analog of linear independence of vectors.

LEMMA 5.1: *Let  $E$  and  $F$  be extensions of a field  $K$ . The following conditions are equivalent:*

- (a) *Each  $m$ -tuple  $(x_1, \dots, x_m)$  of elements of  $E$  which is linearly independent over  $K$  is also linearly independent over  $F$ .*
- (b) *Each  $n$ -tuple  $(y_1, \dots, y_n)$  of elements of  $F$  which is linearly independent over  $K$  is also linearly independent over  $E$ .*

*Proof:* Obviously it suffices to prove that (a) implies (b). Let  $y_1, \dots, y_m$  be elements of  $F$  for which there exist  $a_1, \dots, a_m \in E$  with  $a_1 y_1 + \dots + a_m y_m = 0$ . Let  $\{x_j \mid j \in J\}$  be a linear basis for  $E$  over  $K$  and write  $a_i = \sum_{j \in J} a_{ij} x_j$  with  $a_{ij}$  elements of  $K$ , only finitely many different from 0. By (a),  $\{x_j \mid j \in J\}$  is linearly independent over  $F$ . Therefore  $\sum a_{ij} y_i = 0$  for every  $j$ . If  $y_1, \dots, y_m$  are linearly independent over  $K$ , then  $a_{ij} = 0$  for every  $i$  and  $j$ , and therefore  $a_i = 0$ ,  $i = 1, \dots, m$ . Thus  $y_1, \dots, y_m$  are linearly independent over  $E$ . This proves (b). ■

*Definition:* With  $E$  and  $F$  field extensions of a field  $K$ , refer to  $E$  and  $F$  as **linearly disjoint over  $K$**  if (a) (or (b)) of Lemma 9.1 holds.

COROLLARY 5.2: *Let  $E$  and  $F$  be extensions of a field  $K$  such that  $[E : K] < \infty$ . Then  $E$  and  $F$  are linearly disjoint over  $K$  if and only if  $[E : K] = [EF : F]$ . If in addition  $[F : K] < \infty$ , then this is equivalent to  $[EF : K] = [E : K][F : K]$ .*

*Proof:*  $E$  and  $F$  are linearly disjoint over  $K$  and  $w_1, \dots, w_n$  is a basis for  $E/K$ , then  $w_1, \dots, w_n$  is also a basis for  $EF$  over  $F$ . Hence  $[EF : F] = n = [E : K]$ . Conversely, suppose that  $[E : K] = [EF : F]$  and let  $x_1, \dots, x_m \in E$  be linearly independent over  $K$ . Extend  $\{x_1, \dots, x_m\}$  to a basis  $\{x_1, \dots, x_n\}$  of  $E/K$ . Since  $\{x_1, \dots, x_n\}$  generates  $EF$  over  $K$  and  $n = [EF : F]$ ,  $\{x_1, \dots, x_n\}$  is a basis of  $EF/F$ . In particular  $x_1, \dots, x_m$  are linearly independent over  $F$ . ■

If  $E$  is a Galois extension of  $K$ , then  $E$  and  $F$  are linearly disjoint over  $K$  if and

only if  $E \cap F = K$ . For arbitrary extensions this is clearly necessary, but not sufficient. Let  $L$  be a degree  $n > 1$  extension of  $K$  for which  $L'$  is conjugate to  $L$  over  $K$ , but  $L' \cap L = K$ . Then  $[LL' : K] \leq n(n-1)$ . Thus, according to Corollary 5.2,  $L$  and  $L'$  are not linearly disjoint over  $K$ .

LEMMA 5.3 (The tower property): *Let  $K \subseteq E$  and  $K \subseteq L \subseteq F$  be four fields. Then  $E$  is linearly disjoint from  $F$  over  $K$  if and only if  $E$  is linearly disjoint from  $L$  over  $K$  and  $EL$  is linearly disjoint from  $F$  over  $L$ .*

*Proof:* The only nontrivial part is to show that if  $E$  and  $F$  are linearly disjoint over  $K$ , then  $EL$  and  $F$  are linearly disjoint over  $L$ .

Apply Lemma 9.1. Suppose that  $y_1, \dots, y_m$  are elements of  $F$  which are linearly independent over  $L$ , but  $a_1, \dots, a_m$  are elements of  $EL$  such that  $\sum_{i=1}^m a_i y_i = 0$ . Clear denominators to assume that  $a_i \in L[E]$ , so that  $a_i = \sum a_{ij} x_j$  with  $a_{ij} \in L$ , where  $\{x_j \mid j \in J\}$  is a linear basis for  $E$  over  $K$ . Then  $\sum_j (\sum_i a_{ij} y_i) x_j = 0$  and  $a_i = 0$ ,  $i = 1, \dots, m$ . ■

Tensor products give an alternative approach to linear disjointness. Let  $E_1, \dots, E_n$  be  $n$  extensions of a field  $K$  which are contained in a common field. Then  $E_1, \dots, E_n$  are linearly disjoint over  $K$  if and only if the canonical homomorphism of  $E_1 \otimes_K \dots \otimes_K E_n$  into  $E_1 \dots E_n$  that maps  $x_1 \otimes \dots \otimes x_n$  onto  $x_1 \dots x_n$  is injective. Associativity of the tensor product construction shows that  $E_1, \dots, E_n$  are linearly disjoint over  $K$  if and only if  $E_i$  is linearly disjoint from  $E_1 \dots E_{i-1}$  over  $K$ ,  $i = 2, \dots, n$ . Finally, for any sequence  $\{E_1, E_2, E_3, \dots\}$  of field extensions of  $K$  contained in a common field, define  $\{E_1, E_2, E_3, \dots\}$  to be **linearly disjoint over  $K$**  if every finite subfamily of  $\{E_1, E_2, E_3, \dots\}$  is linearly disjoint over  $K$ . The next lemma is an easy observation.

LEMMA 9.4: *Let  $E_1, \dots, E_n$  (resp.,  $F_1, \dots, F_n$ ) be linearly disjoint field extensions of  $K$  (resp.,  $L$ ). Let  $\sigma_i: E_i \rightarrow F_i$ , be isomorphisms which coincide on  $K$  and for which  $\sigma_i(K) = L$ ,  $i = 1, \dots, n$ . Then*

$$\sigma_1 \otimes \dots \otimes \sigma_n: E_1 \otimes_K \dots \otimes_K E_n \rightarrow F_1 \otimes_L \dots \otimes_L F_n$$

*is a well defined isomorphism. Therefore, there exists an isomorphism  $\sigma: E_1 \dots E_n \rightarrow F_1 \dots F_n$  that extends each of the  $\sigma_i$ 's.*

## 6. Separable and regular extensions

We generalize the notion of ‘separable algebraic extension’ to arbitrary field extensions.

Denote the characteristic of a field  $K$  by  $p$ . If  $p > 0$ , then  $K^{1/p}$  is the field generated over  $K$  by the  $p$ th roots of all elements of  $K$ . If  $p = 0$ , then  $K^{1/p} = K$ . Use  $K^{1/p^\infty}$  for the maximal purely inseparable extension of  $K$ . Let  $E$  be a finitely generated extension of  $K$ . A collection  $t_1, \dots, t_r \in E$  of elements algebraically independent over  $K$  is a **separating transcendence basis** if  $E/K(t_1, \dots, t_r)$  is a finite separable extension.

LEMMA 6.1: An extension  $E$  of a field  $K$  is said to be **separable** if it satisfies one of the following equivalent conditions:

- (a)  $E$  is linearly disjoint from  $K^{1/p^\infty}$  over  $K$ ;
- (b)  $E$  is linearly disjoint from  $K^{1/p}$  over  $K$ ; or
- (c) every finitely generated extension  $F$  of  $K$  which is contained in  $E$  has a separating transcendence basis.

Moreover, a separating transcendence basis can be selected from a given set of generators for  $E/K$ .

*Proof:* The implications ‘(a)  $\implies$  (b)’ and ‘(c)  $\implies$  (a)’ are easy. For ‘(b)  $\implies$  (c)’ see [L4, p. 54]. [FrJ, Lemma 17.7] gives a constructive proof. ■

Now apply the rules of linear disjointness.

COROLLARY 6.2:

- (a) If  $E/K$  and  $F/E$  are separable extensions, then  $F/K$  is also separable.
- (b) If  $F/K$  is a separable extension, then  $E/K$  is separable for every field  $K \subseteq E \subseteq F$ .
- (c) Every extension of a perfect field is separable.

*Example:* A separable tower does not imply separable steps. Consider the tower of fields  $\mathbb{F}_p \subseteq \mathbb{F}_p(t^p) \subseteq \mathbb{F}_p(t)$ , where  $t$  is transcendental over  $\mathbb{F}_p$ . The extension  $\mathbb{F}_p(t)/\mathbb{F}_p$  is separable, but  $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$  is not. ■

LEMMA 6.3: Call a field extension  $F/K$  **regular** if it satisfies one of the following equivalent conditions:

- (a) the extension  $F/K$  is separable and  $K$  is algebraically closed in  $F$ ; or

(b) *the field  $F$  is linearly disjoint from  $\tilde{K}$  over  $K$ .*

*Proof:* The implication "(b)  $\implies$  (a)" is immediate.

To prove "(a)  $\implies$  (b)" it suffices to assume that  $F/K$  is finitely generated. Then  $F/K$  has a separating transcendence basis,  $t_1, \dots, t_r$ , which is also a separating transcendence basis for the extension  $FK_s/K_s$ . It follows that  $FK_s$  is linearly disjoint from  $\tilde{K}$  over  $K_s$ . Also,  $K_s/K$  is a Galois extension and  $F \cap K_s = K$ . Hence  $F$  is linearly disjoint from  $K_s$  over  $K$ . From Lemma 5.3 conclude that  $F$  is linearly disjoint from  $\tilde{K}$  over  $K$ . ■

COROLLARY 6.4:

- (a) *If  $E/K$  and  $F/E$  are regular extensions, then  $F/K$  is regular.*
- (b) *If  $F/K$  is a regular extension, then  $E/K$  is regular for every field  $K \subseteq E \subseteq F$ .*
- (c) *Every extension of an algebraically closed field is regular.*

An extension  $E$  of  $K$  is said to be **algebraically independent** (or **free**) from an extension  $F$ , if every finite set of elements of  $E$  algebraically independent over  $K$  remains algebraically independent over  $F$ . By considering monomials in elements  $x_1, \dots, x_n$  of  $E$ , it is clear that if  $E$  and  $F$  are linearly disjoint over  $K$ , then they are also algebraically independent over  $K$ . The converse, however, is false: Any two algebraic extensions of  $K$  are algebraically independent over  $K$ . But here is a partial converse.

LEMMA 6.5: *Let  $E$  be a regular extension of a field  $K$  and let  $F$  be an extension of  $K$ . If  $E$  is algebraically independent from  $F$  over  $K$ , then  $E$  is linearly disjoint from  $F$  over  $K$ .*

*Proof (Artin):* Let  $x_1, \dots, x_n$  be elements of  $E$  for which there exist  $a_1, \dots, a_n \in F$ , not all zero, such that  $\sum a_i x_i = 0$ . Let  $\varphi$  be a  $K$ -place of  $F$  into  $\tilde{K} \cup \{\infty\}$  and let  $T$  be a transcendence basis for  $E$  over  $K$ . Then the elements of  $T$  are algebraically independent over  $F$ . Hence  $\varphi$  extends to a  $K(T)$ -place of  $F(T)$ . Since  $E$  is an algebraic extension of  $K(T)$ ,  $\varphi$  extends to an  $E$ -place of  $EF$ .

With no loss we may divide  $a_1, \dots, a_n$  by, say  $a_1$ , to assume that  $a_1 = 1$  and that all the  $a_i$  are finite under  $\varphi$ . Thus  $\sum \varphi(a_i)x_i = 0$  is a nontrivial linear combination of

the  $x_i$  over  $\tilde{K}$ . But  $E$  is linearly disjoint from  $\tilde{K}$  over  $K$ . Hence  $x_1, \dots, x_n$  are also linearly dependent over  $K$ . ■

COROLLARY 6.6:

- (a) *Let  $F$  be regular extension of a field  $K$ , algebraically independent from an extension  $E$  of  $K$ . Then  $FE$  is a regular extension of  $E$ .*
- (b) *If two regular extensions  $F$  and  $E$  of  $K$  are algebraically independent from each other, then  $FE/K$  is regular.*

*Proof:* For (a) note that  $F$  is also algebraically independent from  $\tilde{E}$  over  $K$ . From Lemma 6.5,  $F$  is linearly disjoint from  $\tilde{E}$  over  $K$ . Therefore  $FE$  is linearly disjoint from  $\tilde{E}$  over  $E$ . That is,  $FE/E$  is regular.

For (b) use (a) and Corollary 6.4(a). ■

## 7. Varieties

Concepts: **Basic field**  $K$ , **universal domain**  $\Omega$ , **Affine  $n$ -space**  $\mathbb{A}^n$ , **point in**  $\mathbb{A}^n$ , **the polynomial ring**  $K[\mathbf{X}]$ , **algebraic set**.

HILBERT'S BASIS THEOREM (Lan, p. 145): *The polynomial ring  $K[\mathbf{X}]$  in  $n$  variables over a field  $K$  is **Noetherian**. That is, it satisfies the following equivalent conditions:*

- (a) *Every ideal in  $K[\mathbf{X}]$  is finitely generated; or*
- (b) *Every ascending sequence of ideals of  $K[\mathbf{X}]$  is eventually stationary.*

Concepts: **Zariski topology**, **irreducible varieties**, **prime ideal**, **generic point**, **coordinate ring**:

$$0 \longrightarrow \mathfrak{p} \longrightarrow K[\mathbf{X}] \longrightarrow K[\mathbf{x}] \longrightarrow 0$$

**$K$ -specialization**, **function field**, **dimension**,  **$K$ -curve**,  **$K$ -hypersurface**,  **$K$ -hyperplane**.

Concepts: **absolutely irreducible variety**, **field of definition**.

LEMMA: *Let  $W$  be a  $K$ -variety with a generic point  $\mathbf{x}$ . For each extension  $L$  of  $K$  let  $\mathfrak{p}_L$  be the prime ideal of all  $f \in L[\mathbf{X}]$  such that  $f(\mathbf{x}) = 0$ . Then the following statements are equivalent:*

- (a)  *$K(\mathbf{x})/K$  is a regular extension;*
- (b)  $\mathfrak{p}_{\tilde{K}} = \tilde{K} \cdot \mathfrak{p}_K$ ;
- (c)  *$W$  is an absolutely irreducible variety defined over  $K$ .*

*Proof of (a)  $\implies$  (b):* Let  $f \in \mathfrak{p}_{\tilde{K}}$  and write  $f(\mathbf{X}) = \sum_{i \in I} w_i f_i(\mathbf{X})$ , with  $\{w_i \mid i \in I\}$  is a basis for  $\tilde{K}/K$  and  $f_i \in K[\mathbf{X}]$ . Then the  $w_i$  are linearly independent over  $K(\mathbf{x})$  and  $0 = \sum w_i f_i(\mathbf{x})$ . Hence,  $f_i(\mathbf{x}) = 0$  and therefore  $f_i \in \mathfrak{p}_K$  for each  $i \in I$ . Conclude that  $\mathfrak{p}_{\tilde{K}} = \tilde{K} \cdot \mathfrak{p}_K$ .

*Proof (b)  $\implies$  (a):* Suppose again that  $\{w_i \mid i \in I\}$  is a basis for  $\tilde{K}/K$ . We have to prove that it is linearly independent over  $K(\mathbf{x})$ . So, suppose that  $g_i$  are elements of  $K[\mathbf{X}]$  such that  $\sum w_i g_i(\mathbf{x}) = 0$ . Then  $\sum w_i g_i(\mathbf{X}) \in \mathfrak{p}_{\tilde{K}}$  and therefore there exist  $f_i \in \mathfrak{p}_K$  such that  $\sum w_i g_i(\mathbf{X}) = \sum w_i f_i(\mathbf{X})$ . Conclude that  $g_i = f_i \in \mathfrak{p}_K$  and hence  $g_i(\mathbf{x}) = 0$  for each  $i \in I$ .

*Proof (b)  $\implies$  (c):* Observe that  $\mathfrak{p}_{\tilde{K}} = \tilde{K} \cdot \mathfrak{p}_K$  implies that  $I_{\tilde{K}}(W) = \mathfrak{p}_{\tilde{K}}$ . Since  $\mathfrak{p}_{\tilde{K}}$  is prime,  $W$  is irreducible over  $\tilde{K}$ , and defined over  $K$ .

*Proof (c)  $\implies$  (b):* Let  $\mathbf{x}'$  be a generic point of  $W$  over  $\tilde{K}$ . Then the map  $\mathbf{x}' \rightarrow \mathbf{x}$  extends to a  $\tilde{K}$ -homomorphism  $\tilde{K}[\mathbf{x}'] \rightarrow \tilde{K}[\mathbf{x}]$ . In particular,  $\text{trans.deg}\tilde{K}(\mathbf{x}') \geq \text{trans.deg}\tilde{K}(\mathbf{x})$ . On the other hand,  $\mathbf{x}'$  is a point of  $W$  and therefore the map  $\mathbf{x} \rightarrow \mathbf{x}'$  extends to a  $K$ -homomorphism  $K[\mathbf{x}] \rightarrow K[\mathbf{x}']$ . In particular  $\text{trans.deg}K(\mathbf{x}) \geq \text{trans.deg}K(\mathbf{x}')$  and therefore also  $\text{trans.deg}\tilde{K}(\mathbf{x}) \geq \text{trans.deg}\tilde{K}(\mathbf{x}')$ . So, the equality holds. It follows that  $I_{\tilde{K}}(W) = \mathfrak{p}_{\tilde{K}}$ . Since  $W$  is defined over  $K$ , this implies that  $\mathfrak{p}_{\tilde{K}} = \tilde{K} \cdot \mathfrak{p}$ .  $\blacksquare$

LEMMA (Weil [Lan, p. 74]): *Every absolutely irreducible  $K$ -variety  $V$  has a smallest field of definition  $L$ , which is a finite purely inseparable extension of  $K$ .*

## 8. Pseudo algebraically closed field

We say that a field  $K$  is **pseudo algebraically closed** (abbreviated **PAC**) if each absolutely irreducible variety  $V$  defined over  $K$  has a  $K$ -rational point.

Equivalently, for each absolutely irreducible polynomial  $f \in K[T_1, \dots, T_r, X]$  with  $\frac{\partial f}{\partial X} \neq 0$  and each  $0 \neq g \in K[T_1, \dots, T_r]$ , there exists  $(\mathbf{a}, b) \in K^{r+1}$  such that  $f(\mathbf{a}, b) = 0$  and  $g(\mathbf{a}) \neq 0$ .

Equivalently (using intersection with general hyperplanes), each absolutely irreducible polynomial  $f \in K[T, X]$  has infinitely many  $K$ -rational points.

Equivalently, if  $R$  is a finitely generated integral domain over  $K$  with quotient field which is regular over  $K$ , then there exists a homomorphism  $\varphi: R \rightarrow K$  such that  $\varphi(a) = a$  for each  $a \in K$ .

If  $K$  is PAC,  $V$  is an absolutely irreducible variety defined over  $K$  and  $U$  is a nonempty Zariski open subset of  $K$ , then  $V(K) \neq \emptyset$ .

Suppose that  $K$  is PAC and  $\aleph_1$ -saturated. Let  $R$  be a countably generated integral domain over  $K$  and whose quotient field is regular over  $K$ . Then there exists a homomorphism  $\varphi: R \rightarrow K$  such that  $\varphi(a) = a$  for each  $a \in K$ .

*Examples:* (a) Every algebraically closed field is PAC. (b) Every separably closed field is PAC. (c) (Ershov) Every infinite algebraic extension of a PAC field is PAC. (d) Ultraproducts of PAC fields are PAC. (e) (Ax-Roquette) Every algebraic extension of a PAC field is PAC. (f) Finite fields are not PAC fields. (g) If a field  $K$  has a valuation with a finite residue field, then  $K$  is not PAC. In particular, global and local fields are not PAC. (h) If  $K$  has an ordering, then  $K$  is not PAC. ■

See [FrJ, Chap. 10] for proofs.

**THE EMBEDDING LEMMA** ([FrJ, Lemma 18.2]): *Let  $L$  and  $M$  be perfect fields. Let  $E$  be a countable extension of  $L$  which is perfect. Let  $F$  be a perfect PAC  $\aleph_1$ -saturated field which contains  $M$ . Suppose that there exists an isomorphism  $\Phi_0: \tilde{L} \rightarrow \tilde{M}$  such*

that  $\Phi_0(L) = M$ . Assume also that there is a commutative diagram

$$(1) \quad \begin{array}{ccc} \text{Gal}(E) & \xleftarrow{\varphi} & \text{Gal}(F) \\ \text{res} \downarrow & & \downarrow \text{res} \\ \text{Gal}(L) & \xleftarrow{\varphi_0} & \text{Gal}(M) \end{array}$$

where  $\varphi_0$  is the isomorphism induced by  $\Phi_0$  and  $\varphi$  is a homomorphism.

Then, there exists an extension of  $\Phi_0$  to an embedding  $\Phi: \tilde{E} \rightarrow \tilde{F}$  such that  $\Phi(\varphi(\sigma)x) = \sigma\Phi(x)$  for each  $\sigma \in \text{Gal}(F)$  and each  $x \in \tilde{E}$ .

LEMMA ([FrJ, Lemma 18.3]): Let  $E/L$  and  $F/M$  be extensions of perfect fields. Suppose that both  $L$  and  $M$  are countable and contain a field  $K$ . Assume that  $E$  and  $F$  are PAC field,  $\aleph_1$ -saturated, and there exists a  $K$ -isomorphism  $\Phi_0: \tilde{L} \rightarrow \tilde{M}$  such that  $\Phi_0(L) = M$ . Assume also that (1) holds with  $\varphi$  an isomorphism. Then  $E$  is  $K$ -elementarily equivalent to  $F$ .

LEMMA ([FrJ, Corollary 18.5]): Let  $E$  and  $F$  be two fields and let  $\varphi_0: \text{Gal}(F) \rightarrow \text{Gal}(E)$  be an isomorphism. Let  $\mathcal{D}$  be an ultrafilter on  $I$ . Let  $E^* = E^I/\mathcal{D}$  and  $F^* = F^I/\mathcal{D}$ . Then there exists a commutative diagram

$$(1) \quad \begin{array}{ccc} \text{Gal}(E^*) & \xleftarrow{\varphi} & \text{Gal}(F^*) \\ \text{res} \downarrow & & \downarrow \text{res} \\ \text{Gal}(E) & \xleftarrow{\varphi_0} & \text{Gal}(F) \end{array}$$

where  $\varphi$  is an isomorphism.

THE ELEMENTARY EQUIVALENCE THEOREM FOR PAC FIELDS: Let  $E/L$  and  $F/M$  be perfect fields with both  $L$  and  $M$  containing a field  $K$ . Assume that  $E$  and  $F$  are PAC, that there exists a  $K$ -isomorphism  $\Phi_0: \tilde{L} \rightarrow \tilde{M}$  such that  $\Phi_0(L) = M$ , and there exists a commutative diagram

$$(3) \quad \begin{array}{ccc} \text{Gal}(E) & \xleftarrow{\varphi} & \text{Gal}(F) \\ \text{res} \downarrow & & \downarrow \text{res} \\ \text{Gal}(L) & \xleftarrow{\varphi_0} & \text{Gal}(M) \end{array}$$

with  $\varphi_0$  induced by  $\Phi_0$  and  $\varphi$  an isomorphism. Then  $E$  is  $K$ -elementarily equivalent to  $F$ .

We call a field  $F$  **pseudo finite** if it is perfect, PAC, and  $\text{Gal}(F) \cong \hat{\mathbb{Z}}$ .

THE ELEMENTARY EQUIVALENCE THEOREM FOR PSEUDO FINITE FIELDS: *Let  $E$  and  $F$  be two pseudo finite fields that contain a subfield  $K$ . If  $\tilde{K} \cap E \cong_K \tilde{K} \cap F$ , then  $E$  is  $K$ -elementarily equivalent to  $F$ .*

## 9. Haar measure

**Haar measure** of a profinite group  $G$ :

$\mathcal{B}$  =  $\sigma$ -algebra of subsets of  $G$  that contains all closed subset of  $G$

$$\mu: \mathcal{B} \rightarrow [0, 1]$$

$$0 \leq \mu(B) \leq 1,$$

$$\mu(\emptyset) = 0, \quad \mu(G) = 1$$

$B_1, B_2, B_3, \dots$  pairwise disjoint:  $\mu(\bigcup_{i=1}^{\infty} B_i) = \sum_{i=1}^{\infty} \mu(B_i)$  ( **$\sigma$ -additivity**)

$\mu(gB) = \mu(Bg) = \mu(B)$  (**invariance under translations**)

For all  $B \in \mathcal{B}$  and for all  $\varepsilon > 0$  there exist an open subset  $U$  and a closed subset  $C$  such that  $C \subseteq B \subseteq U$  and  $\mu(U \setminus C) < \varepsilon$  (**regularity**)

$B \in \mathcal{B}$  and  $\mu(B) = 0$  and  $B_0 \subseteq B$  imply  $B_0 \in \mathcal{B}$  (**completeness**).

Consequences:

$A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$  imply  $\mu(\bigcup_{i=1}^{\infty} A_i) = \lim_{i \rightarrow \infty} \mu(A_i)$

$A_1 \supseteq A_2 \supseteq A_3 \supseteq \dots$  imply  $\mu(\bigcap_{i=1}^{\infty} A_i) = \lim_{i \rightarrow \infty} \mu(A_i)$

If  $H < G$  is an open subgroup of index  $n$ , then  $\mu(H) = \frac{1}{n}$ .

If  $\alpha: G \rightarrow \bar{G}$  is an epimorphism a finite group and  $\bar{S} \subseteq \bar{G}$ , then  $\mu(\alpha^{-1}(\bar{S})) = \frac{|\bar{S}|}{|\bar{G}|}$ .

*Definition:* A sequence  $A_1, A_2, A_3, \dots$  are **independent** if  $\mu(\bigcap_{i \in I} A_i) = \prod_{i \in I} \mu(A_i)$  for every finite set  $I$ . In this case the sequence of complements

$$G \setminus A_1, G \setminus A_2, G \setminus A_3, \dots$$

is also independent. ■

**LEMMA:** Let  $A_1, A_2, A_3, \dots$  be an independent sequence of subsets of  $G$ . Suppose that  $\sum_{i=1}^{\infty} \mu(A_i) = \infty$ . Then  $\mu(\bigcup_{i=1}^{\infty} A_i) = 1$ .

*Proof:*  $\mu(G \setminus \bigcup_{i=1}^{\infty} A_i) = \mu(\bigcap_{i=1}^{\infty} G \setminus A_i) = \prod_{i=1}^{\infty} \mu(G \setminus A_i) = \prod_{i=1}^{\infty} (1 - \mu(A_i)) \rightarrow 0$ .

■

**LEMMA:** Let  $H_1, \dots, H_n$  be open subgroup of  $G$ . They are independent if and only if  $(G : H) = \prod_{i=1}^n (G : H_i)$ .

*Proof:* Consider  $K = H_1 \cap \dots \cap H_m$  with  $m \leq n$ . The map  $G/K \mapsto \prod_{i=1}^m G/H_i$ ,  $gK \mapsto (gH_1, \dots, gH_m)$  of cosets is injective. Hence  $(G : K) \leq \prod_{i=1}^m (G : H_i)$ . Similarly,

$(K : H) \leq \prod_{i=m+1}^n (K : H_i \cap K) \leq \prod_{i=m+1}^n (G : H_i)$ . Hence  $(G : H) = (G : K)(K : H)$  and  $(G : H) = \prod_{i=1}^n (G : H_i)$  gives  $(G : K) = \prod_{i=1}^m (G : H_i)$ . ■

LEMMA: For each  $i$  let  $\alpha_i: G \rightarrow G_i$  be an epimorphism of finite group,  $\bar{A}_i \leq G_i$ ,  $A_i = \alpha_i^{-1}(\bar{A}_i)$ , and  $N_i = \text{Ker}(\alpha_i)$ . Suppose that  $(G : N_1 \cap \dots \cap N_n) = \prod_{i=1}^n (G : N_i)$  for each  $n$ . Then  $A_1, A_2, A_3, \dots$  are independent. If  $\sum_{i=1}^{\infty} |\bar{A}_i|/|G_i| = \infty$ , then  $\mu(\bigcup_{i=1}^{\infty} A_i) = 1$ .

*Proof:* Let  $N = N_1 \cap \dots \cap N_n$  and  $\alpha: G \rightarrow \prod_{i=1}^n G/N_i$ ,  $\alpha(g) = (gN_1, \dots, gN_n)$ . Then  $\alpha$  decomposes through  $G/N$  and is therefore surjective. Hence,  $A_1 \cap \dots \cap A_n = \alpha^{-1}(\bar{A}_1 \times \dots \times \bar{A}_n)$  and therefore

$$\mu(A_1 \cap \dots \cap A_n) = \frac{|\bar{A}_1 \times \dots \times \bar{A}_n|}{|G/N|} = \prod_{i=1}^n \frac{|\bar{A}_i|}{|G_i|} = \prod_{i=1}^n \mu(A_i). \quad \blacksquare$$

COROLLARY: Let  $L_1, L_2, L_3, \dots$  be a sequence of finite separable extensions of a field  $K$ . Let  $G = \text{Gal}(K)$ .

(a)  $\text{Gal}(L_1), \text{Gal}(L_2), \text{Gal}(L_3), \dots$  is independent if and only if  $L_1, L_2, L_3, \dots$  is linearly disjoint over  $K$ .

So, suppose that  $L_1, L_2, L_3, \dots$  is linearly disjoint.

(b) If  $\sum_{i=1}^{\infty} \frac{1}{[L_i:K]} = \infty$ , then  $\mu(\bigcup_{i=1}^{\infty} \text{Gal}(L_i)) = 1$ .

(c) Suppose that  $L_i/K$  is Galois,  $\bar{A}_i \subseteq \text{Gal}(L_i/K)$ ,  $A_i = \{\sigma \in G \mid \sigma|_{L_i} \in \bar{A}_i\}$ , and  $\sum_{i=1}^{\infty} |\bar{A}_i|/[L_i:K] = \infty$ , then  $\mu(\bigcup_{i=1}^{\infty} A_i) = 1$ .

## 10. Hilbertian fields

Let  $K$  be a field. Consider irreducible polynomials

$$f_1, \dots, f_m \in K(T_1, \dots, T_r)[X_1, \dots, X_n]$$

and  $0 \neq g \in K[T_1, \dots, T_r]$ . They define a **Hilbert subset** of  $K^r$ :

$$H_K(f_1, \dots, f_m; g) = \{\mathbf{a} \in K^r \mid \bigwedge_{i=1}^m f_i(\mathbf{a}, \mathbf{X}) \text{ is defined and irreducible in } K[\mathbf{X}], \\ \text{and } g(\mathbf{a}) \neq 0\}$$

$K$  is **Hilbertian** if all its Hilbert sets are nonempty.

If  $K$  is Hilbertian, then every finite extension  $L$  of  $K$  is Hilbertian. Moreover, if  $L/K$  is separable, then every Hilbert subset of  $L^r$  contains a subset of  $K^r$ .

LEMMA: Let  $f \in K(T_1, \dots, T_r)[X]$  be a separable polynomial. Then

$$\{\mathbf{a} \in K^r \mid \text{Gal}(f(\mathbf{a}, X), K) \cong \text{Gal}(f(\mathbf{T}, X), K(\mathbf{T}))\}$$

contains a Hilbert subset of  $K^r$ .

*Examples of Hilbertian fields:*  $\mathbb{Q}$ ,  $K_0(t)$  ( $K_0$  any field). Hence, every number field. Every finitely generated transcendental extension of  $K_0$ .

$K_0((t_1, t_2, \dots, t_r))$ ,  $K_0$  any field,  $r \geq 2$ . ■

*Examples of infinite extensions of a Hilbertian field  $K$  which are Hilbertian:*

If  $\text{Gal}(N/K)$  is finitely generated, then  $N$  is Hilbertian.

If  $\text{Gal}(N/K)$  is abelian, then  $N$  is Hilbertian.

If  $N/K$  is Galois and  $M$  is a proper finite separable extension, then  $M$  is Hilbertian (Weissauer)

If  $N = N_1 N_2$ ,  $N_i/K$  is Galois,  $i = 1, 2$  and  $N_1 \not\subseteq N_2$ ,  $N_2 \not\subseteq N_1$ , then  $N$  is Hilbertian.

*Examples of non Hilbertian fields:*

$K$  finite

$K$  separably closed

$\text{Gal}(K)$  finitely generated

$K$  Henselian, e.g.,  $K = \mathbb{Q}_p$  or  $K = K_0((t))$

$K$  is the maximal pro- $p$  extension of a field  $K_0$

$K$  is the maximal prosolvable extension of a field  $K_0$  ■

LEMMA: Let  $K$  be a Hilbertian field,  $f \in K(T_1, \dots, T_r)[X]$  an absolutely irreducible Galois polynomial,  $G = \text{Gal}(f(\mathbf{T}, X), K(\mathbf{T}))$ . Then  $K$  has a linearly disjoint sequence  $L_1, L_2, L_3, \dots$  of Galois extensions such that  $\text{Gal}(L_i/K) \cong G$ ,  $i = 1, 2, \dots$

PROPOSITION: Let  $K$  be a Hilbertian field. Then  $\langle \sigma \rangle \cong \hat{\mathbb{Z}}$  for almost all  $\sigma \in \text{Gal}(K)$ .

THEOREM: Let  $K$  be a countable Hilbertian field. Then  $K_s(\sigma)$  and  $\tilde{K}(\sigma)$  are PAC for almost all  $\sigma \in \text{Gal}(K)$ .

## 11. Elements of algebraic number theory

An integral domain  $R$  is a **Dedekind domain** if

- (1a)  $R$  is Noetherian (i.e., each ideal is finitely generated);
- (1b) integrally closed (i.e., if an element  $x$  of the quotient field  $K$  of  $R$  satisfies an equation  $x^n + a_1x^{n-1} + \cdots + a_n = 0$  with  $a_i \in R$ , then  $x \in R$ . We say that  $x$  is **integral** over  $R$ .); and
- (1c) every nonzero ideal  $\mathfrak{p}$  of  $R$  is maximal (i.e.,  $\bar{K}_{\mathfrak{p}} = R/\mathfrak{p}$  is a field).

We make the set of all nonzero ideals of  $R$  into a semigroup:  $\mathfrak{a}\mathfrak{b} = \{\sum a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ . The unit element of this semigroup is  $R$ . Every ideal  $\mathfrak{a}$  of  $R$  has a unique presentation,  $\mathfrak{a} = \mathfrak{p}_1^{m_1} \mathfrak{p}_2^{m_2} \cdots \mathfrak{p}_r^{m_r}$ , where  $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$  are maximal ideals and  $m_1, m_2, \dots, m_r$  are positive integers. We say that  $\mathfrak{p}_i$  **divides**  $\mathfrak{a}$ .

*Examples:* Every principal ideal domain is a Dedekind domain. In particular,  $\mathbb{Z}$ ,  $F[t]$  ( $F$  a field,  $t$  transcendental element over  $F$ ) and every discrete valuation ring are Dedekind domains.

Let  $R$  be a Dedekind domain with quotient field  $K$ . Let  $L$  be a finite extension of  $K$ . Then the set  $S$  of all elements  $x \in L$  which are integral over  $R$  is a Dedekind domain ( $S$  is the **integral closure** of  $R$  in  $L$ .) In particular, if  $\mathfrak{p}$  is a prime ideal of  $R$ , then  $S\mathfrak{p} = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}$  with distinct prime ideals  $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_g$  of  $S$  and positive integers  $e_1, e_2, \dots, e_g$ . If  $e_1 = e_2 = \cdots = e_g = 1$ , then  $\mathfrak{p}$  is **unramified** in  $L$ . If, in addition  $L/K$  is separable, then only finitely many ideals of  $R$  are ramified in  $L$ . Indeed,  $R$  has an ideal  $\mathfrak{d}$ , called the **discriminant** of  $S/R$  such that  $\mathfrak{p}$  is ramified in  $L$  if and only if  $\mathfrak{p}$  divides  $\mathfrak{d}$ .

Assume in addition, that  $L$  is a finite Galois extension of  $K$ . Let  $\mathfrak{p}$  be a prime ideal of  $R$  which does not ramify in  $L$  and let  $\mathfrak{P}$  be a prime divisor of  $\mathfrak{p}$  in  $L$  that **lies above**  $\mathfrak{p}$  (i.e,  $\mathfrak{P} \cap R = \mathfrak{p}$ ). The **decomposition group** of  $\mathfrak{P}$  over  $K$  is the following subgroup of  $\text{Gal}(L/K)$ :

$$D_{\mathfrak{P}} = \{\sigma \in \text{Gal}(L/K) \mid \mathfrak{P}^{\sigma} = \mathfrak{P}\}.$$

The fixed field  $L(\mathfrak{P})$  of  $D(\mathfrak{P})$  in  $L$  is the **decomposition field** of  $\mathfrak{P}$  over  $K$ . In this set up,  $\bar{K}_{\mathfrak{p}} = R/\mathfrak{p}$  embeds into  $\bar{L}_{\mathfrak{P}} = S/\mathfrak{P}$  by  $x + \mathfrak{p} \mapsto x + \mathfrak{P}$ .

Assume that  $\mathfrak{P}$  is unramified over  $K$ , Then  $\bar{L}_{\mathfrak{P}}/\bar{K}_{\mathfrak{p}}$  is a Galois extension and  $D(\mathfrak{P}) \cong \text{Gal}(\bar{L}_{\mathfrak{P}}/\bar{K}_{\mathfrak{p}})$ . Under this isomorphism  $\sigma \in D(\mathfrak{P})$  is mapped onto the element  $\bar{\sigma} \in \text{Gal}(\bar{L}_{\mathfrak{P}}/\bar{K}_{\mathfrak{p}})$  such that  $\bar{\sigma}\bar{x} = \overline{\sigma x}$  for each  $x \in S$ . Here  $\bar{x} = x + \mathfrak{P}$ .

If  $\mathfrak{P}'$  is another prime ideal of  $S$  that lies above  $\mathfrak{p}$ , then there exists  $\tau \in \text{Gal}(L/K)$  such that  $\mathfrak{P}' = \mathfrak{P}^\tau$ . We then have  $D(\mathfrak{P}') = D(\mathfrak{P})^\sigma$ .

A **global field**  $K$  is either a finite extension of  $\mathbb{Q}$  or a finite extension of  $\mathbb{F}_q(t)$  for some prime power  $q$  and a transcendental element  $t$ . In the first case  $K$  is a **number field**. Its **ring of integers**  $O_K$  is the integral closure of  $\mathbb{Z}$  in  $K$ . In the latter case,  $K$  is a **function field**. Its **ring of integers**  $O_K$  is the integral closure of  $\mathbb{F}_p[t]$  in  $K$ . In both cases  $O_K$  is a Dedekind domain.

Also, if  $\mathfrak{p}$  is a maximal ideal of  $O_K$  then  $\bar{K}_{\mathfrak{p}} = O_K/\mathfrak{p}$  is a finite field. Indeed, in the number field case, it is a finite extension of  $\mathbb{F}_p$ , where  $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ . In the number field case  $\bar{K}_{\mathfrak{p}}$  is a finite extension of  $\mathbb{F}_q$ . In both cases we denote the number of elements of  $\bar{K}_{\mathfrak{p}}$  by  $N\mathfrak{p}$ . Denote the set of all nonzero prime ideals of  $K$  by  $P(K)$ . For each  $m$  there are only finitely many  $\mathfrak{p} \in P(K)$  such that  $N\mathfrak{p} \leq m$ .

Suppose that  $L$  is a finite Galois extension of  $K$ . Suppose that  $\mathfrak{p}$  does not ramify in  $L$ . Let  $\mathfrak{P}$  be a prime ideal of  $O_L$  above  $\mathfrak{p}$ . Then  $D_{\mathfrak{P}}$  is isomorphic to the group  $\text{Gal}(\bar{L}_{\mathfrak{P}}/\bar{K}_{\mathfrak{p}})$ . The latter group is cyclic with a canonical generator Frob defined by  $\text{Frob } x = x^{N\mathfrak{p}}$ . The unique element of  $D(\mathfrak{P})$  which is mapped onto Frob is the **Frobenius element of  $\mathfrak{P}/\mathfrak{p}$** . It is denoted by  $\left[\frac{L/K}{\mathfrak{P}}\right]$  and is the unique element of  $\text{Gal}(L/K)$  such that

$$\left[\frac{L/K}{\mathfrak{P}}\right] x \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}}$$

for each  $x \in O_L$ . If  $\tau \in \text{Gal}(L/K)$ , then  $\left[\frac{L/K}{\mathfrak{P}^\tau}\right] = \left[\frac{L/K}{\mathfrak{P}}\right]^\tau$ . Thus, when  $\tau$  ranges over all elements of  $\text{Gal}(L/K)$ ,  $\left[\frac{L/K}{\mathfrak{P}^\tau}\right]$  ranges over a conjugacy class of  $\text{Gal}(L/K)$  known as the **Artin symbol** of  $\mathfrak{p}$  in  $L$ :

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

**THE CHEBOTAREV DENSITY THEOREM:** *Let  $L/K$  be a Galois extension of global field and let  $C$  be a conjugacy class of  $\text{Gal}(L/K)$ . Then, the Dirichlet density of the set of all prime ideals  $\mathfrak{p}$  of  $O_K$  such that  $\left(\frac{L/K}{\mathfrak{p}}\right) = C$  is equal to  $|C|/[L : K]$ .*

Here the **Dirichlet density** of a set  $A$  of primes of  $O_K$  is defined as the limit (if it exists)

$$\delta(A) = \lim_{s \rightarrow 1^-} \frac{\sum_{\mathfrak{p} \in A} 1/N\mathfrak{p}^s}{\sum_{\text{all } \mathfrak{p}} 1/N\mathfrak{p}^s}.$$

LEMMA: Let  $L/K$  be a finite Galois extension of global fields. Suppose that  $f \in K[X]$  is a polynomial which decomposes over  $L$  into linear factors. Then, for almost all  $\mathfrak{p} \in P(K)$ ,  $f(X)$  has a root modulo  $\mathfrak{p}$  if and only if there exists (for all)  $\mathfrak{P} \in P(L)$  over  $\mathfrak{p}$  such that  $f(X)$  has a root in  $L(\mathfrak{P})$ .

## 12. The transfer theorem

REGULAR ULTRAPRODUCTS OF  $\tilde{K}(\sigma)$ . An ultrafilter  $\mathcal{D}$  of  $\text{Gal}(K)$  is **regular** if each subset of  $\text{Gal}(K)$  of measure 1 belongs to  $\mathcal{D}$ .

LEMMA: Let  $\mathcal{D}_0$  be a collection of subsets of  $G = \text{Gal}(K)$ . Suppose that  $A_1, \dots, A_n \in \mathcal{D}_0$  implies  $A_1 \cap \dots \cap A_n$  is not a zero set. Then  $G$  has a regular ultrafilter  $\mathcal{D}$  which contains  $\mathcal{D}_0$ .

*Proof:* Let  $\mathcal{D}_1 = \mathcal{D}_0 \cup \{1\text{-sets}\}$ . If  $A_i \in \mathcal{D}_0$ ,  $B_j$  are 1-sets and  $A_1 \cap \dots \cap A_m \cap B_1 \cap \dots \cap B_n = \emptyset$ , then  $A_1 \cap \dots \cap A_n \subseteq G \setminus (B_1 \cap \dots \cap B_n)$ , and hence  $A_1, \dots, A_n$  is a zero set, a contradiction. Take  $\mathcal{D} \supseteq \mathcal{D}_1$ . ■

LEMMA: For each  $\tau \in \text{Gal}(K)$  there exists a regular ultrafilter  $\mathcal{D}$  of  $\text{Gal}(K)$  such that  $\tilde{K} \cap \prod \tilde{K}(\sigma)/\mathcal{D} \cong \tilde{K}(\tau)$ .

*Proof:* For each finite Galois extension  $L$  of  $K$  let  $A_L = \{\sigma \in \text{Gal}(K) \mid \sigma|_L = \tau|_L\}$ . Take a regular ultrafilter  $\mathcal{D}$  which contains all  $A_L$ .

PROPOSITION: Let  $K$  be a countable Hilbertian field and let  $\theta$  be a sentence in the language  $\mathcal{L}(\text{ring}, K)$ . Equivalent:

- (a)  $\tilde{K}(\sigma) \models \theta$  for almost all  $\sigma \in \text{Gal}(K)$ .
- (b)  $F \models \theta$  for all perfect pseudo finite fields that contain  $K$ .

COROLLARY: Let  $K$  be a global field. If a sentence  $\theta$  of  $\mathcal{L}(\text{ring}, O_K)$  is true in  $\tilde{K}(\sigma)$  for almost all  $\sigma \in \text{Gal}(K)$ , then  $\theta$  is true in  $\bar{K}_{\mathfrak{p}}$  for almost all  $\mathfrak{p} \in P(K)$ .

BOOLEAN ALGEBRAS. Let  $K$  be a global field and let  $G = \text{Gal}(K)$ . For each sentence  $\theta$  of  $\mathcal{L}(\text{ring}, K)$  let

$$S(\theta) = \{\sigma \in \text{Gal}(K) \mid \tilde{K}(\sigma) \models \theta\}.$$

Then  $S(\theta_1 \vee \theta_2) = S(\theta_1) \cup S(\theta_2)$ ,  $S(\theta_1 \wedge \theta_2) = S(\theta_1) \cap S(\theta_2)$ ,  $S(\neg\theta) = G \setminus S(\theta)$ .

Denote the Boolean algebra generated by all basic test sets and all zero sets by  $\mathcal{S}$ . Here  $S(\exists: f(X) = 0)$  is a **basic test set** if  $f \in K[X]$  is a monic separable polynomial. A Boolean combination of basic test sets is a **test set**.

LEMMA: Let  $A \subseteq G$ ,  $A \notin \mathcal{S}$ . Then there exist regular ultrafilters  $\mathcal{D}, \mathcal{D}'$  of  $G$  such that  $\mathcal{D} \cap \mathcal{S} = \mathcal{D}' \cap \mathcal{S}$ ,  $A \in \mathcal{D}$ , but  $A \notin \mathcal{D}'$ .

*Proof:* Let  $\mathcal{S}_0$  be the collection of all  $B \in \mathcal{S}$  such that either  $A \lesssim B$  or  $G \setminus A \lesssim B$ . Then

(1)  $B_1, \dots, B_m \in \mathcal{S}_0$  implies  $B_1 \cap \dots \cap B_m$  is not a zero set.

Indeed, suppose  $B_1, \dots, B_m \in \mathcal{S}_1$  and  $B_1 \cap \dots \cap B_m \approx \emptyset$ . Assume without loss that  $A \lesssim B_i$ ,  $i = 1, \dots, l$  and  $G \setminus A \lesssim G \setminus B_i$ ,  $i = l+1, \dots, m$ . Then  $G = A \cup (G \setminus A) \lesssim (B_1 \cup \dots \cup B_l) \cup (B_{l+1} \cup \dots \cup B_m)$ . Hence,  $A \approx B_1 \cup \dots \cup B_l$ , so  $A \in \mathcal{S}_1$ . This contradicts our assumption on  $A$ .

Use Zorn's lemma to choose a maximal subcollection  $\mathcal{S}_1$  of  $\mathcal{S}$  that contains  $\mathcal{S}_0$  and satisfies (1). In particular

(2)  $C_1, \dots, C_m \in \mathcal{S}_1$  implies  $C_1 \cap \dots \cap C_m \in \mathcal{S}_1$ .

Now let  $\mathcal{C} = \mathcal{S}_1 \cup \{A\}$ . Then  $\mathcal{C}$  satisfies (1). Indeed, let  $C_1, \dots, C_m \in \mathcal{S}_1$  and  $C = C_1 \cap \dots \cap C_m$ . By (2),  $C \in \mathcal{S}_1$ . Assume that  $A \cap C \approx \emptyset$ . Then  $A \lesssim G \setminus C$ , so  $G \setminus C \in \mathcal{S}_0 \subseteq \mathcal{S}_1$ . This contradicts (1).

It follows that  $\mathcal{C}$  is contained in a regular ultrafilter  $\mathcal{D}$ . Since  $\mathcal{S} \subseteq \mathcal{S} \cap \mathcal{D}$  and  $\mathcal{S} \cap \mathcal{D}$  satisfies (1), we have  $\mathcal{S}_1 = \mathcal{S} \cap \mathcal{D}$ .

Similarly, there exists a regular ultrafilter  $\mathcal{D}'$  which contains  $\mathcal{S}_1 \cup \{G \setminus A\}$ . It also satisfies  $\mathcal{S}_1 = \mathcal{S} \cap \mathcal{D}'$ . ■

For each test set  $\theta$  let

$$A(\theta) = \{\mathfrak{p} \in P(K) \mid \bar{K}_{\mathfrak{p}} \models \theta\}.$$

COROLLARY: For each sentence  $\theta$  there exists a test sentence  $\lambda$  such that  $S(\theta) \approx S(\lambda)$  and  $A(\theta) \approx A(\lambda)$ .

THEOREM: For each sentence  $\theta$ ,  $\mu(S(\theta)) = \delta(S(\theta))$ . Moreover,  $\delta(A(\theta))$  is a rational number and  $\delta(A(\theta)) > 0$  if and only if  $A(\theta)$  is infinite.

*Proof:* By the corollary, it suffices to take a test sentence  $\lambda$  which depends on

$$(\exists X)[f_1(X) = 0], \dots, (\exists X)[f_m(X) = 0].$$

Let  $L$  be the splitting field of  $f_1, \dots, f_m$ . Let  $C = \{\sigma \in \text{Gal}(L/K) \mid L(\sigma) \models \lambda\}$ . Then  $\tilde{K}(\sigma) \models \lambda$  if and only if  $\sigma|_L \in C$ . Hence  $\nu(S(\lambda)) = |C|/[L : K]$ .  $C$  is a union of conjugacy classes of  $\text{Gal}(L/K)$ . By the Chebotarev density theorem, the set

$$A'(\lambda) = \{\mathfrak{p} \in P(K) \mid \left(\frac{L/K}{\mathfrak{p}}\right) \subseteq C\}$$

has density  $|C|/[L : K]$ . So, it suffices to prove that  $A'(\lambda) \approx A(\lambda)$ .

Induction on the structure of  $\lambda$  reduces the proof to the case where  $\lambda$  has the form  $(\exists X)[f(X) = 0]$ , where  $f \in K[X]$  monic irreducible polynomial.

Let  $x_1, \dots, x_n$  be the roots of  $f$ . Then

$$\begin{aligned} A'((\exists X)[f(X) = 0]) &= \{\mathfrak{p} \in P(K) \mid \left(\frac{L/K}{\mathfrak{p}}\right) \subseteq \bigcup_{i=1}^n \text{Gal}(L/K(x_i))\} \\ &\approx \{\mathfrak{p} \in P(K) \mid \bar{K}_{\mathfrak{p}} \models (\exists X)[f(X) = 0]\}. \quad \blacksquare \end{aligned}$$

## References

- [Ax] J. Ax, *Solving diophantine problems modulo every prime*, Annals of Mathematics **85** (1967), 161–183.
- [BoS] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
- [FrJ] M.D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.
- [FrV] M. D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Mathematische Annalen **290** (1991), 771–800.
- [Ja1] M. Jarden, *Elementary statements over large algebraic fields*, Transactions of AMS **164** (1972), 67–91.
- [Lan] S. Lang, *Introduction to algebraic geometry*, Interscience Publishers, New York, 1958.
- [Mum] D. Mumford, *The Red Book of Varieties and Schemes*, Lecture Notes in Mathematics **1358**, Springer, Berlin, 1988.

4 November, 2007