Chapter VII.

§ 1: q_v, ζ_k(cf. § 6).
§ 2: Φ^*, $\prod \Phi_v$, $\prod \alpha_v$.
§ 3: $\Omega(G)$, Ω_1, ω_s.
§ 4: $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$, $\Omega(G_k)$, ω_1, ω_s, G_k^1, Ω_1, M, N, ω_v, $\prod \omega_v$, $Z(\omega, \Phi)$.
§ 6: $G_1(s)$, $G_2(s)$, c_k (cf. Chap. V-4), $G_w(s)$, $\zeta_k(s)$, $Z_k(s)$.
§ 7: $f(v)$, s_v, A, B, N_v, Φ_ω, $\kappa = \prod \kappa_v$, $a = (a_v)$, $b = (b_v)$, G_w, $\lambda(v)$, π_v, $L(s, \omega)$, $\mathfrak{f}, \Lambda(s, \omega)$.
§ 8: $G_{\mathfrak{P}}$, $I(P)$, $D(P)$.

Chapter VIII.

§ 1: K, K', n, q, R, P, π, q', R', P', π', f, e, Tr, N, $\mathfrak{N}$, d, $D(K'/K)$, D, ι'.
§ 2: Δ.
§ 3: $\nu(\lambda)$, $\mathfrak{g}_v$.
§ 4: $\mathfrak{d}$, ι, $\mathfrak{N}_{k'/k}$, $\mathfrak{N}$, $\mathfrak{D}$.

Chapter IX.

§ 1: A_L, $A \otimes B$, A^0.
§ 2: τ, ν.
§ 3: $\mathrm{Cl}(A)$, $B(K)$, $\bar{K}$, K_{sep}, $\mathfrak{G}$, $\mathfrak{H}$, K', $\bar{K}'$, K'_{sep}, $\mathfrak{G}'$, ρ, $H(K)$.
§ 4: $\{\chi, \theta\}$, $[L/K; \chi, \theta]$.
§ 5: $\chi_{n,\xi}$, $\{\xi, \theta\}_n$, $\chi_{p,\xi}$, $\{\xi, \theta\}_p$.

Chapter X.

§ 1: $\mathrm{Hom}(V, W)$, $\mathrm{Hom}(V, L; W, M)$, $\mathrm{End}(V, L)$, $\mathrm{Aut}(V, L)$.
§ 3: $\mathfrak{T}$, $\mathfrak{T}'$, $\mathfrak{T}''$; $\mathfrak{T}$, $\mathfrak{U}$.

Chapter XII.

§ 1: K_{ab}, $\mathfrak{G}^{(1)}$, $\mathfrak{A}$, X_K, ρ, G_K, $(\chi, g)_K$, $\mathfrak{a}$, G_K^1, U_K, X_0, $\mathfrak{A}_0$, K_0.
§ 2: $h(A)$, η, $(\chi, \theta)_K$ (for $K = \mathbf{R}, \mathbf{C}$); $\mathfrak{M}$, K_0, $\mathfrak{H}_0$, K_n, φ_0, X_0, φ, η, $(\chi, \theta)_K$, $\mathfrak{a}$, $h(A)$.
§ 3: U_K, $\mathfrak{A}_0$.

Chapter XIII.

§ 1: $\bar{k}$, K_v, k_{sep}, $k_{v,\mathrm{sep}}$, k_{ab}, $k_{v,\mathrm{ab}}$, $\mathfrak{G}$, $\mathfrak{A}$, $\mathfrak{G}_v$, $\mathfrak{A}_v$, ρ_v, X_k, χ_v, $(\chi_v, z)_v$, $(\chi, z)_k$, $\mathfrak{a}$, $k_{\infty+}^{\times}$, F, q, k_0, $\mathfrak{H}_0$, X_0, k_n, $\mathfrak{A}_0$, φ_0, φ, $\bar{\mathbf{Q}}$, ε, $\mathfrak{H}_m$, $\mathfrak{g}$, $\mathfrak{h}$.
§ 3: $h_v(A)$, U_k.
§ 5: $(x, y)_{n,K}$, $(z, z')_n$, $\Omega(P)$ (cf. Chap. IV-4), $\Omega'(P)$.
§ 7: $(x, z)_{p,K}$, Φ, $\Omega'(m, K)$, $(x, z)_p$, $\Omega'(\mathfrak{m})$.
§ 9: $\mathfrak{B}(L)$, $N(L)$.
§ 10: k', $\mathfrak{g}$, $\mathfrak{h}$, U, $\mathfrak{B}$, U_v, $\mathfrak{B}_v$, γ, γ_v, $\mathfrak{f}(\omega)$, $\mathfrak{D}$.
§ 11: $G_{\mathfrak{P}}$, $G'_{\mathfrak{P}}$, $L_{\mathfrak{P}}$, $l_{\mathfrak{P}}$, pr, $\mathfrak{U}_{\mathfrak{P}}$, $J(U, P)$.

Chapter I

Locally compact fields

§ 1. Finite fields. Let F be a finite field (commutative or not) with the unit-element 1. Its characteristic must clearly be a prime $p > 1$, and the prime ring in F is isomorphic to the prime field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, with which we may identify it. Then F may be regarded as a vector-space over $\mathbf{F}_p$; as such, it has an obviously finite dimension f, and the number of its elements is $q = p^f$. If F is a subfield of a field F' with $q' = p^{f'}$ elements, F' may also be regarded e.g. as a left vector-space over F; if its dimension as such is d, we have $f' = df$ and $q' = q^d = p^{df}$.

THEOREM 1. *All finite fields are commutative.*

This theorem is due to Wedderburn, and we will reproduce Witt's modification of Wedderburn's original proof. Let F be a finite field of characteristic p, Z its center, $q = p^f$ the number of elements of Z; if n is the dimension of F as a vector-space over Z, F has q^n elements. The multiplicative group $F^{\times}$ of the non-zero elements of F can be partitioned into classes of "conjugate" elements, two elements x, x' of $F^{\times}$ being called conjugate if there is $y \in F^{\times}$ such that $x' = y^{-1}xy$. For each $x \in F^{\times}$, call $N(x)$ the set of the elements of F which commute with x; this is a subfield of F containing Z; if $\delta(x)$ is its dimension over Z, it has $q^{\delta(x)}$ elements. As we have seen above, n is a multiple of $\delta(x)$, and we have $\delta(x) < n$ unless $x \in Z$. As the number of elements of $F^{\times}$ conjugate to x is clearly the index of $N(x)^{\times}$ in $F^{\times}$, i.e. $(q^n - 1)/(q^{\delta(x)} - 1)$, we have

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{\delta(x)} - 1}, \tag{1}$$

where the sum is taken over a full set of representatives of the classes of non-central conjugate elements of $F^{\times}$. Now assume that $n > 1$, and call P the "cyclotomic" polynomial $\prod (T - \zeta)$, where the product is taken over all the primitive n-th roots of 1 in the field $\mathbf{C}$ of complex numbers. By a well-known elementary theorem (easily proved by induction on n), this has integral rational coefficients; clearly it divides $(T^n - 1)/(T^\delta - 1)$ whenever δ is a divisor of n other than n. Therefore, in (1), all the terms except $q - 1$ are multiples of $P(q)$, so that $P(q)$ must divide $q - 1$. On the other hand, each factor in the product $P(q) = \prod (q - \zeta)$ has an absolute value $> q - 1$. This is a contradiction, so that we must have $n = 1$ and $F = Z$.

We can now apply to every finite field the following elementary result:

LEMMA 1. *If K is a commutative field, every finite subgroup of $K^\times$ is cyclic.*

In fact, let Γ be such a group, or, what amounts to the same, a finite subgroup of the group of all roots of 1 in K. For every $n \geqslant 1$, there are at most n roots of $X^n=1$ in K, hence in Γ; we will show that every finite commutative group with that property is cyclic. Let α be an element of Γ of maximal order N. Let β be any element of Γ, and call n its order. If n does not divide N, there is a prime p and a power $q=p^\nu$ of p such that q divides n and not N. Then one verifies at once that the order of $\alpha\beta^{n/q}$ is the l.c.m. of N and q, so that it is $>N$, which contradicts the definition of N. Therefore n divides N. Now $X^n=1$ has the n distinct roots $\alpha^{iN/n}$ in Γ, with $0 \leqslant i < n$; as β is a root of $X^n=1$, it must be one of these. This shows that α generates Γ.

THEOREM 2. *Let K be an algebraically closed field of characteristic $p>1$. Then, for every $f \geqslant 1$, K contains one and only one field $F=\mathbf{F}_q$ with $q=p^f$ elements; F consists of the roots of $X^q=X$ in K; $F^\times$ consists of the roots of $X^{q-1}=1$ in K and is a cyclic group of order $q-1$.*

If F is any field with q elements, lemma 1 shows that $F^\times$ is a cyclic group of order $q-1$. Thus, if K contains such a field F, $F^\times$ must consist of the roots of $X^{q-1}=1$, hence F of the roots of $X^q-X=0$, so that both are uniquely determined. Conversely, if $q=p^f$, $x \to x^q$ is an automorphism of K, so that the elements of K which are fixed under it make up a field F consisting of the roots of $X^q-X=0$; as it is clear that X^q-X has only simple roots in K, F is a field with q elements.

COROLLARY 1. *Up to isomorphisms, there is one and only one field with $q=p^f$ elements.*

This follows at once from theorem 2 and the fact that all algebraic closures of the prime field $\mathbf{F}_p$ are isomorphic. It justifies the notation $\mathbf{F}_q$ for the field in question.

COROLLARY 2. *Put $q=p^f$, $q'=p^{f'}$, with $f \geqslant 1$, $f' \geqslant 1$. Then $\mathbf{F}_{q'}$ contains a field $\mathbf{F}_q$ with q elements if and only if f divides f'; when that is so, $\mathbf{F}_{q'}$ is a cyclic extension of $\mathbf{F}_q$ of degree f'/f, and its Galois group over $\mathbf{F}_q$ is generated by the automorphism $x \to x^q$.*

We have already said that, if $\mathbf{F}_{q'}$ contains $\mathbf{F}_q$, it must have a finite degree d over $\mathbf{F}_q$, and then $q'=q^d$ and $f'=df$. Conversely, assume that $f'=df$, hence $q'=q^d$, and call K an algebraic closure of $\mathbf{F}_{q'}$; by theorem 2, the fields $\mathbf{F}_q$, $\mathbf{F}_{q'}$, contained in K, consist of the elements of K respectively

invariant under the automorphisms α, β of K given by $x \to x^q$, $x \to x^{q'}$; as $\beta=\alpha^d$, $\mathbf{F}_{q'}$ contains $\mathbf{F}_q$. Clearly α maps $\mathbf{F}_{q'}$ onto itself; if φ is the automorphism of $\mathbf{F}_{q'}$ induced by α, $\mathbf{F}_q$ consists of the elements of $\mathbf{F}_{q'}$ invariant under φ, hence under the group of automorphisms of $\mathbf{F}_{q'}$ generated by φ; this group is finite, since φ^d is the identity; therefore, by Galois theory, it is the Galois group of $\mathbf{F}_{q'}$ over $\mathbf{F}_q$ and is of order d.

COROLLARY 3. *Notations being as in corollary 2, assume that $f'=df$. Then, for every $n \geqslant 1$, the elements of $\mathbf{F}_{q'}$, invariant under $x \to x^{q^n}$, make up the subfield of $\mathbf{F}_{q'}$ with q^r elements, where $r=(d,n)$.*

Let K be as in the proof of corollary 2; the elements of K, invariant under $x \to x^{q^n}$, make up the subfield F' of K with q^n elements; then $F' \cap \mathbf{F}_{q'}$ is the largest field contained both in F' and $\mathbf{F}_{q'}$; as it contains $\mathbf{F}_q$, the number of its elements must be of the form q^r, and corollary 2 shows that r must be (d,n).

§ 2. The module in a locally compact field. An arbitrary field, provided with the discrete topology, becomes locally compact; thus the question of determining and studying locally compact fields becomes significant only if one adds the condition that the field should not be discrete.

We recall the definition of the "module" of an automorphism, which is basic in what follows. For our purposes, it will be enough to consider automorphisms of locally compact commutative groups. Let G be such a group (written additively), λ an automorphism of G, and α a Haar measure on G. As the Haar measure is unique up to a constant factor, λ transforms α into $c\alpha$, with $c \in \mathbf{R}_+^\times$; the constant factor c, which is clearly independent of the choice of α, is called the *module* of λ and is denoted by $\mathrm{mod}_G(\lambda)$. In other words, this is defined by one of the equivalent formulas

$$(2)\quad \alpha(\lambda(X))=\mathrm{mod}_G(\lambda)\alpha(X), \quad \int f(\lambda^{-1}(x))\,d\alpha(x)=\mathrm{mod}_G(\lambda)\int f(x)\,d\alpha(x),$$

where X is any measurable set, f any integrable function, and $0<\alpha(X)<+\infty$, $\int f\,d\alpha \neq 0$; the second formula may be written symbolically as $d\alpha(\lambda(x))=\mathrm{mod}_G(\lambda)\,d\alpha(x)$. If G is discrete or compact, the first formula (applied to $X=\{0\}$, $X=G$, respectively) shows that the module is 1. Obviously, if λ, λ' are two automorphisms of G, the module of $\lambda \circ \lambda'$ is the product of those of λ and λ'. We shall need the following lemma:

LEMMA 2. *Let G' be a closed subgroup of G, and λ an automorphism of G which induces on G' an automorphism λ' of G'. Put $G''=G/G'$, and call λ'' the automorphism of G'' determined by λ modulo G'. Then:*

$$\mathrm{mod}_G(\lambda)=\mathrm{mod}_{G'}(\lambda')\mathrm{mod}_{G''}(\lambda'').$$

In fact, it is well-known that one can choose Haar measures $\alpha, \alpha', \alpha''$ on G, G', G'' so as to have, for every continuous function f with compact support on G: