Part I

Preliminaries

This part of the book sets the stage for later developments. We start with *Kummer theory*, which is the study of abelian extensions K/F of fields under the crucial assumption that F contain sufficiently many roots of unity. We include "equivariant Kummer theory", which has been part of the folklore around Galois theory for a long time, but does not seem to be treated in any textbook.

While the theory is very satisfying, it is natural to wish to remove the hypothesis about roots of unity. One of the final achievements of the book is the description, in a fashion directly analogous to Kummer theory, of the abelian extensions of *local number fields* (see Part IV). These fields, useful in many areas of mathematics, are introduced in Chapter 2, and their study is continued in Chapter 4. Chapter 3 is an interlude on topological groups and fields.

This may be the place to list the prerequisites for this book. We expect the reader to know a few basic facts from topology/analysis: Cauchy sequences, complete metric spaces, general topological spaces, compactness. We require the basics of linear algebra, and just a few things from commutative algebra: prime ideals, the notion of quotient ring, the Chinese Remainder theorem. We expect the reader to know that a finitely generated abelian group is a direct sum of cyclic groups, and that a subgroup of a finitely generated abelian group is itself finitely generated. In general, the theory of modules over euclidean domains will be required a couple of times (more will be said in due course).

Quite importantly, it is assumed that the reader knows about the Galois theory of finite extensions: separable, normal, and Galois extensions, the primitive element theorem (a separable, finite extension K/F is of the form $K = F(x)$ for some $x \in K$), Dedekind's lemma on the independence of characters, the fundamental theorem of Galois theory giving a bijection between subgroups of the Galois group and intermediate fields in a finite Galois extension. (In Chapter 3, we extend this to infinite Galois extensions.) You should know about cyclotomic extensions and cyclotomic polynomials. Basic facts about finite fields are assumed (you should be able to give a "list" of all the finite fields in the world).

We shall also rely on norms and traces. Most of the time, one can get away by simply knowing this: when K/F is a finite Galois extension, then we define for $a \in K$:

$$\mathrm{N}_{K/F}(a) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(a), \qquad \mathrm{Tr}_{K/F}(a) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(a).$$

These are called the norm and the trace of a, respectively. There are a few occasions (very rare in this book) when we need to talk about the norm or trace in an extension K/F which is not assumed Galois; and in the final chapter of this book, we shall have use for norms and traces when K is not even assumed to be a field. This is not always part of the standard, undergraduate treatment of Galois theory, and so for convenience we include a discussion in the Appendix.

Generally speaking, we point out that the first two chapters of Morandi's book [Mor96] are a great reference for the material which we assume is known.

1 Kummer theory

We begin gently with a warm-up chapter on Kummer theory, which is the study of abelian extensions of fields containing "enough" roots of unity. This will serve as a motivation for the rest of the book, where abelian extensions of *local number fields* are eventually described, in full generality. Besides, Kummer theory should be known to all students of Galois theory (and no doubt many readers will have already seen this).

We take the opportunity to setup some notation that will accompany us throughout the book.

Some basics

We start by recalling some basic material which, in principle, every reader will already know. We do this to fix the notation, and give an idea of where we take off from (in case the list of prerequisites, in the previous pages, left too much to the imagination).

Whenever R is a ring, we write $R^\times$ for the (multiplicative) group of invertible elements of R, also called units. When F is a field, of course $F^\times = F \smallsetminus \{0\}$. Note that the letters of the alphabet used for fields in this book will usually be F, E, K, L, M, sometimes (but rarely) $\mathbb{F}$ or $\mathbb{K}$ (never k).

A very important fact about the group $F^\times$ is:

Lemma 1.1 *Let F be a field. Then every finite subgroup of $F^\times$ is cyclic.*

Proof. Let G be such a finite subgroup. By the classification of finite abelian groups, there is an isomorphism

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}$$

with $a_i > 1$ an integer dividing a_{i+1}. So the order of G is $a_1 a_2, \dots a_k$, while every $g \in G$ satisfies $g^{a_k} = 1$. However, the equation $X^{a_k} - 1$ has at most a_k solutions in the field F, and the order of G must be $\leq a_k$. From $a_1 \dots a_k \leq a_k$ we draw $k = 1$. □

A crucial subgroup of $F^\times$, in this chapter and elsewhere, is

$$\mu_n(F) = \{x \in F : x^n = 1\},$$

for any $n \geq 1$, the group of nth *roots of unity*. Thus $\mu_n(F)$ is a cyclic group of order $\leq n$; this order may well be strictly less than n, even if we try to enlarge F, as follows from:

Lemma 1.2 *Suppose the characteristic of F is the prime number p, and that $n = p^r m$. Then $\mu_n(F) = \mu_m(F)$, and the order of this group is thus $\leq m$. If n is a power of p, then $\mu_n(F)$ is trivial.*

Proof. Indeed, we simply write

$$X^n - 1 = (X^m - 1)^{p^r},$$

from which the result is clear. □

If, on the other hand, the integer n is prime to the characteristic of F, then the roots of $X^n - 1$ (in an algebraic closure of F) are distinct. If K is the splitting field of $X^n - 1$ over F, then $\mu_n(K)$ has order n, as does $\mu_n(L)$ for any field containing K. (In other words, unless the characteristic gets in the way, we can enlarge any field to have the "right" number of roots of unity.) The extension K/F is called a cyclotomic extension.

Remark 1.3 Many people write informally μ_n instead of $\mu_n(\overline{F})$, where $\overline{F}$ is an algebraic closure of F. With this notation, the field K just mentioned is $F(\mu_n)$. We shall refrain from employing this shorthand in this chapter (but we will have some use for it later). ■

A *primitive nth root of unity* is an element $\omega \in F^\times$ of order n (in the sense of group theory, that is, n is the smallest positive integer such that $\omega^n = 1$). It is important to keep in mind that the existence of such an element implies in particular that $\mu_n(F)$ has order n, and so the characteristic of F does not divide n. Conversely, if $\mu_n(F)$ has order n, then primitive nth roots of unity exist by Lemma 1.1.

In this chapter we will frequently refer to the subgroup

$$F^{\times n} = \{f^n : f \in F\} \subset F^\times.$$

More precisely, we shall encounter quite often the quotient $F^\times/F^{\times n}$. The image of $x \in F^\times$ in $F^\times/F^{\times n}$ will be denoted $[x]$ or $[x]_F$ if there is any ambiguity. (Note that n does not appear in the notation.)

Example 1.4 Take $F = \mathbb{Q}$. It takes some time to get used to the following example. We have

$$\mathbb{Q}^\times = \{\pm 1\} \times A,$$

where A is a free abelian group, with a basis consisting of the set of prime numbers. Indeed, any element of $\mathbb{Q}^\times$ can be written uniquely $\pm p_1^{n_1} p_2^{n_2} \cdots$ where $n_i \in \mathbb{Z}$ and $p_1, p_2, \ldots$, is an enumeration of the primes. Now

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \{\pm 1\} \times (A/2A)\,,$$

a vector space over $\mathbb{Z}/2\mathbb{Z}$, with basis given by the elements $[\ell]$ where ℓ is a prime number, together with $[-1]$. On the other hand, when p is an odd prime we have

$$\mathbb{Q}^\times/\mathbb{Q}^{\times p} = A/pA\,,$$

since $-1 = (-1)^p$. ∎

Cyclic extensions

cyclic extension

Definition 1.5 An extension of fields K/F will be called **cyclic extension** when it is finite and Galois, with $\mathrm{Gal}(K/F)$ cyclic. ∎

When F has enough roots of unity, we will be able to characterize cyclic extensions completely. The main ingredient for this is the next lemma, which is a first version of Hilbert's Theorem 90. Later in the book, we shall discover more sophisticated versions of the same result.

Lemma 1.6 (Hilbert 90) *Let F be a field containing a primitive nth root of unity ω, for some $n \geq 1$, and let K/F be a cyclic extension of degree n. If σ is a generator for $\mathrm{Gal}(K/F)$, then there exists $x \in K^\times$ such that*

$$\omega = \frac{\sigma(x)}{x}\,.$$

Proof. We want to find $x \neq 0$ with $\sigma(x) = \omega x$, so what we want is to show that ω is an eigenvalue of the F-linear endomorphism σ (the given form is here for "historical" reasons; it will come up naturally when we generalize this result).

Since σ^n is the identity, the minimal polynomial P of σ (in the sense of linear algebra) divides $X^n - 1$. However, this minimal polynomial must have degree n, for the distinct automorphisms $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent, by Dedekind's lemma. So $P = X^n - 1$. On the other hand, the characteristic polynomial χ of σ is a multiple of P, which also has degree n, and we conclude that $\chi = P = X^n - 1$. Thus, ω is indeed a root of χ. □

Proposition 1.7 *Let F be a field containing a primitive nth root of unity ω.*

1. *For $a \in F^\times$, consider $K = F(\sqrt[n]{a})$, where we write $\sqrt[n]{a}$ for some root of $X^n - a$ in an algebraic closure of F. Then K/F is a cyclic extension. Its degree $m = [K : F]$ is the order of $[a]_F$ in $F^\times/F^{\times n}$, which divides n.*
2. *Let K/F be a cyclic extension of degree n. Then $K = F(\sqrt[n]{a})$ for some $a \in F^\times$. The order of $[a]_F$ in $F^\times/F^{\times n}$ is n.*

Remark 1.8 (on notation) When K/F is a field extension and $\alpha \in K$, the (completely standard) notation $F[\alpha]$ is for the smallest subring containing F and α, while $F(\alpha)$ is the smallest subfield containing F and α; when α is algebraic over F, we have $F[\alpha] = F(\alpha)$, so that one has to choose. The author admits his agnosticism in the matter, implying that $F[\alpha]$ and $F(\alpha)$ alternate in this book. In absolutely all examples, the element α will be algebraic, so that no confusion can possibly arise (a field is always meant); the only exception is when we form a polynomial ring, always clearly identified by the use of capital letters, such as $F[X]$ or $F[Y]$. ■

Proof of the proposition. (1) The roots of $X^n - a$ are $\omega^k \sqrt[n]{a}$ for $0 \leq k < n$, so if $\sigma \in \mathrm{Gal}(K/F)$, we must have $\sigma(\sqrt[n]{a}) = \omega^{k(\sigma)} \sqrt[n]{a}$ for some integer $k(\sigma)$ whose class in $\mathbb{Z}/n\mathbb{Z}$ is well defined. The map $\mathrm{Gal}(K/F) \to \mathbb{Z}/n\mathbb{Z}$ taking σ to $k(\sigma)$ is readily seen to be a group homomorphism, which is injective since K is generated by $\sqrt[n]{a}$. Thus, $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$, and we see that it is cyclic, of order m dividing n. We turn to the alternative description of m.

We allow ourselves to write $a^{r/n}$ instead of $(\sqrt[n]{a})^r$, when r is an integer. We first claim that

$$a^{r/n} \in F^\times \iff a^r \in F^{\times n}. \tag{*}$$

The implication $\implies$ is trivial. If $a^r = (a^{r/n})^n = f^n$ with $f \in F^\times$, then $a^{r/n} f^{-1}$ is an nth root of unity, and so belongs to F, showing the converse. Next, let σ be a generator for $\mathrm{Gal}(K/F)$, and let $k = k(\sigma)$. We have

$$\sigma(a^{1/n}) = \omega^k a^{1/n},$$

so that

$$\sigma(a^{r/n}) = \omega^{kr} a^{r/n}.$$

An element of K lies in F if and only if it is fixed by σ, so

$$a^{r/n} \in F^\times \iff n \text{ divides } kr. \tag{**}$$

Comparing (*) and (**) shows that m, defined above to be the smallest integer such that n divides km, is also the smallest integer such that $a^m \in F^{\times n}$, as we wanted to show.

(2) This is where we use Lemma 1.6 ("Hilbert 90"), giving us the existence of $x \in K^\times$ with $\sigma(x) = \omega x$, where σ is a generator for K/F. It follows that $\sigma(x^n) = x^n$, so the element $a := x^n$ belongs to F, and we may write $x = \sqrt[n]{a} = a^{1/n}$. We have $F \subset F(a^{1/n}) \subset K$ and it is enough to prove that $[F(a^{1/n}) : F] = n$. By part (1), we must show that the order of $[a]$ in $F^\times/F^{\times n}$ is n, and by (*), we must show that the smallest integer r so that $x^r \in F$ is $r = n$. Examining the relation $\sigma(x^r) = \omega^r x^r$, this appears clearly true. □

The two parts of the proposition are almost converses for one another, but not quite. In the important case when n is a prime number at least, we obtain a clean-cut result:

Corollary 1.9 *Let p be a prime, and let F be a field containing a root of unity of order p^2. Then the Galois extensions of F of degree p (which are automatically cyclic) are precisely those of the form $F(\sqrt[p]{a})/F$ where $a \in F^\times \smallsetminus F^{\times p}$.* □

Some classical applications

The field $\mathbb{R}$ has a *finite* extension which is algebraically closed, namely $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$. We could alternatively emphasize that the algebraically closed field $\mathbb{C}$ has an automorphism of finite order. Do algebraically closed fields possess automorphisms of arbitrary finite order, and do they admit complicated finite groups of automorphisms? Using the material on cyclic extensions just obtained, we shall see that the answer is, in a precise sense, "no". The case of $\mathbb{C}/\mathbb{R}$ is as complicated as can be.

Lemma 1.10 *Let p be a prime number, and let F be a field containing a primitive p^2th root of unity. Then for any Galois extension K/F with $[K : F] = p$, there exists a field L containing K such that L/F is cyclic of degree p^2.*

Proof. The extension K/F is cyclic of degree p, so by Proposition 1.7 we must have $K = F[a^{1/p}]$ for some $a \in F^\times$. Let $L = F[a^{1/p^2}]$, so L/F is cyclic, $K \subset L$, and $[L : F]$ is the order of $[a]$ in F^*/F^{*p^2}. Suppose this order were to divide p. Then we would have $a^p = f^{p^2}$ for some $f \in F^\times$, so $(a/f^p)^p = 1$ and $a = f^p\omega^k$, where ω is a primitive pth root of unity and k is some integer. Using that ω has a pth root in F, we see that a has a pth root: this is a contradiction, however, as the order of $[a]$ in $F^\times/F^{\times p}$ is $[K : F] = p$. So the only possibility is that $[L : F] = p^2$. □

Lemma 1.11 *Let p be a prime number, and let F be a field of characteristic $\neq p$. Suppose K/F is a Galois extension of degree p with K algebraically closed. Then $p = 2$ and $K = F[\sqrt{-1}]$.*

Proof. The field K, being algebraically closed and of characteristic $\neq p$, contains a primitive pth root of unity ω. However, ω is a root of

$$1 + X + \cdots + X^{p-1} \in F[X],$$

so $F(\omega)/F$ has degree prime to p, and from $F(\omega) \subset K$ we deduce $F(\omega) = F$, that is, $\omega \in F$.

On the other hand, we claim that F does not have a primitive p^2th root of unity: if it did, then Lemma 1.10 would give us the existence of an extension of K of degree p, which is absurd. Let us write $\omega^{1/p}$ for such a root, which lives in $K \smallsetminus F$. Clearly, we must have $K = F(\omega^{1/p})$.

Let σ be a generator of the group $\mathrm{Gal}(K/F)$. There is an integer k such that $\sigma(\omega^{1/p}) = \omega^k\omega^{1/p}$, and for clarity let us put $\zeta = \omega^k$, another (primitive) pth root of unity.

Now suppose p is odd. The following computation is classical:

$$\mathrm{N}_{K/F}(\omega^{1/p}) = (\omega^{1/p}) \cdot (\zeta\omega^{1/p}) \cdot (\zeta^2\omega^{1/p}) \cdots (\zeta^{p-1}\omega^{1/p}) = \zeta^{p(p-1)/2}\omega = \omega,$$

using that p divides $p(p-1)/2$ when p is odd. This leads to a contradiction. Indeed, as K is algebraically closed, every element of K has a pth root in K, including $\omega^{1/p}$; taking norms down to F, we see that ω has a pth root in F, contrary to what we have shown.

Thus $p = 2$, and $\omega = -1$. We have seen that $K = F[\omega^{1/p}] = F[\sqrt{-1}]$. □

Theorem 1.12 *Let F be a field of characteristic 0, and suppose that K/F is a finite Galois extension with K algebraically closed. Then either $K = F$, or $K = F[\sqrt{-1}]$.*

Equivalently, if G is a finite group of automorphisms of a field K, which is algebraically closed and of characteristic 0, then either $G = \{1\}$ or G has order 2; in the latter case, the fixed field F of G is such that $K = F[\sqrt{-1}]$.

Proof. That the two statements are equivalent follows from Artin's theorem (which asserts that, when F is the fixed field of G, then $G = \mathrm{Gal}(K/F)$). We work with the first formulation.

Let σ be an element of $\mathrm{Gal}(K/F)$ of prime order p. Consider the fixed field F_σ of σ; the extension K/F_σ has degree p, so by Lemma 1.11 we have $p = 2$. It follows that the order of $\mathrm{Gal}(K/F)$ is a power of 2, as this group does not have elements of odd prime order.

Next, consider the element $\sqrt{-1} \in K$, and the field $F[\sqrt{-1}]$. Let σ be an element of $\mathrm{Gal}(K/F[\sqrt{-1}])$ of order 2, if there is one, and let F_σ be its fixed field. Then $[K : F_\sigma] = 2$ while $\sqrt{-1} \in F_\sigma$, and this contradicts Lemma 1.11. So no such element σ exists. Since the group $\mathrm{Gal}(K/F[\sqrt{-1}])$ has an order which is a power of 2, but does not have elements of order 2, we are compelled to conclude that it is trivial, and that $K = F[\sqrt{-1}]$. □

Remark 1.13 (1) The hypothesis on the characteristic of F is here for simplicity. In fact, one can prove that, if K/F is finite and Galois, with K algebraically closed, and $K \neq F$, then F (and K) are automatically of characteristic 0. See [Lan02, VI, corollary 9.3]. The argument raises subtle points about separability which we do not want to review, as they are not particularly relevant for the rest of the book.

(2) The group $\mathrm{Aut}(K)$ may have several elements of order 2, of course. However, the theorem asserts that if σ and τ are two such elements with $\sigma \neq \tau$, then the group they generate in $\mathrm{Aut}(K)$ is infinite. ■

Kummer extensions

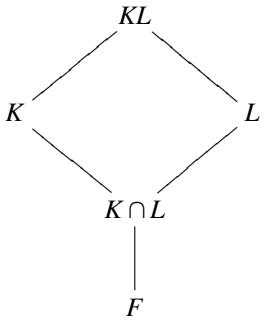
n-Kummer extension

Definition 1.14 A finite Galois extension K/F is said to be an ***n*-Kummer extension** when F contains an nth primitive root of unity, and $\mathrm{Gal}(K/F)$ is abelian of exponent dividing n. (In other words, $g^n = 1$ for all $g \in \mathrm{Gal}(K/F)$.) ■

It is an important fact that there is an alternative definition of n-Kummer extensions: they are the extensions which can be obtained by adjoining to F finitely many elements of the form $\sqrt[n]{a}$ for $a \in F^\times$. Before we turn to this, let us give a useful

proposition about the Galois group of a compositum of two fields. It is more general than is immediately needed.

Proposition 1.15 *Let F be a field, and let K and L be two finite extensions of F contained in a common algebraic closure, as the following diagram indicates.*



1. *If K/F is Galois, then so is KL/L, and moreover*

$$\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)\,.$$

2. *If K/F and L/F are both Galois, then so is KL/F, and*

$$\mathrm{Gal}(KL/F) \cong \{(\sigma,\tau) \in \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F) : \sigma|_{K\cap L} = \tau|_{K\cap L}\}\,.$$

The group appearing in (2) is sometimes called the *fiber product* of $\mathrm{Gal}(K/F)$ and $\mathrm{Gal}(L/F)$ "above" $\mathrm{Gal}(K \cap L/F)$.

Proof. (1) Since K is obtained by adjoining to F the roots of a collection of separable polynomials, the field KL can be obtained from L by adding the same roots, so KL/L is Galois, by a standard criterion. An element $\sigma \in \mathrm{Gal}(KL/L) \subset \mathrm{Gal}(KL/F)$ must map K to itself, since K/F is normal by assumption, so the restriction $\sigma \mapsto \sigma|_K$ defines a homomorphism $r\colon \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/K \cap L)$. The latter is visibly injective.

Let E be the intermediate field such that $\mathrm{Im}(r) = \mathrm{Gal}(K/E)$. Certainly $K \cap L \subset E \subset K$, so it remains to prove $E \subset L$ to obtain $E = K \cap L$. However, E is a subfield of KL which is fixed by $\mathrm{Gal}(KL/L)$, so $E \subset L$ as desired.

(2) That KL/F is Galois is obvious. An element $\gamma \in \mathrm{Gal}(KL/F)$ must preserve K and L, and is determined by $\sigma = \gamma|_K$ and $\tau = \gamma|_L$. Hence, we have an injective homomorphism

$$\mathrm{Gal}(KL/L) \longrightarrow \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$$

whose image is contained in the group Γ described in the proposition. It suffices to establish that the order of Γ is $[KL : F]$. However, the second projection $\Gamma \longrightarrow \mathrm{Gal}(L/F)$ is surjective, and its kernel is

$$\{(\sigma,1) \in \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F) : \sigma|_{K\cap L} = 1\} \cong \mathrm{Gal}(K/K \cap L)\,,$$

so

$$|\Gamma| = [K : K \cap L][L : F] = [KL : L][L : F] = [KL : F],$$

using (1). □

Proposition 1.16 *Let F be a field containing a primitive nth root of unity, and let K/F be an extension. The following properties are equivalent.*

1. *K/F is n-Kummer.*
2. *There are elements $a_1, \dots, a_k \in F^\times$ such that $K = F[\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}]$.*

Proof. (2) $\implies$ (1). Each extension $F[\sqrt[n]{a_i}]/F$ is cyclic of order dividing n by Proposition 1.7, so it is n-Kummer. The field K is the compositum of all the $F[\sqrt[n]{a_i}]/F$ as i varies; so by (2) of the last proposition, applied repeatedly, we see that K/F is Galois and that $\mathrm{Gal}(K/F)$ is a subgroup of a product of cyclic groups, each of order dividing n. Clearly, K/F is then itself n-Kummer.

(1) $\implies$ (2). Write

$$\mathrm{Gal}(K/F) = C_1 \times C_2 \times \cdots \times C_k,$$

where each C_i is cyclic, of order dividing n. Also, let

$$H_i = \prod_{j \neq i} C_j \subset \mathrm{Gal}(K/F),$$

and let E_i be the fixed field of H_i. Then $\mathrm{Gal}(E_i/F) \cong C_i$, so E_i/F is cyclic, and it follows from Proposition 1.7 that $E_i = F[\sqrt[n]{a_i}]$ for some $a_i \in F^\times$. There remains only to prove that K is the compositum of the fields E_i. This compositum L, being the smallest field containing all the E_i, is associated in the Galois correspondence with the largest subgroup contained in all the H_i, that is, the intersection $\cap_i H_i$. This intersection is trivial, so $L = K$. □

The Kummer pairing

When studying cyclic extensions above, we have come across a certain computational remark several times. Namely, if K/F is a Galois extension, $\sigma \in \mathrm{Gal}(K/F)$, and $\sqrt[n]{a} \in K$ is an n-th root for $a \in F$, then $\sigma(\sqrt[n]{a})/\sqrt[n]{a}$ is an n-th root of unity. In this section we shall study the association

$$\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}},$$

seen as a homomorphism $\mathrm{Gal}(K/F) \to \mu_n(F)$. This requires some preparation.

Pontryagin dual

Definition 1.17 Let G be a finite abelian group. Its **Pontryagin dual** is

$$G' = \mathrm{Hom}(G, \mathbb{C}^\times),$$

the (finite abelian) group of homomorphisms $G \to \mathbb{C}^\times$, often called (linear) characters. (The notation $\widehat{G}$ is also common.)