Pontryagin Duality and Kummer Theory

Marco Streng

November 1, 2005

Contents

1 Pontryagin Duality

This lecture consists of two parts. In the first, we state Pontryagin Duality, give some examples and sketch the proof. In the second, we apply Pontryagin duality to the proof of Kummer theory.

1.1 The dual (and other definitions)

Definition 1.1. A *topological group* is a group G together with a topology on G such that both the group law $G \times G \to G$ and the inverse $g \mapsto g^{-1}$ are continuous. In this lecture we further demand the topology to be *Hausdorff*.

In the following, all groups are abelian Hausdorff groups. In particular, finite groups have the discrete topology.

Definition 1.2. A Hausdorff topological space is called *locally compact* if every point has a compact neighborhood.

For a topological group, this is equivalent to the neutral element e having a compact neighborhood, because multiplication by a fixed element is a homeomorphism.

Definition 1.3. Given a locally compact topological group G, we define the *Pontryagin dual* of G to be the set

$$G^\vee = \mathrm{Hom}(G, \mathbf{S}^1)$$

of continuous group homomorphisms from G to $\mathbf{S}^1$.

It is an abelian group, because $\mathbf{S}^1$ is. We can supply it with the *compact-open topology*, which is generated by sets of the form

$$\mathcal{U}_{K,U} = \{\chi \in \mathrm{Hom}(G, \mathbf{S}^1) : \chi(K) \subset U\},$$

where K runs over the compact subsets of G and U runs over the open subsets of Y. One can prove with some work that this makes $G^\vee$ into a topological group. Now $G^\vee$ is also Hausdorff.

Proof. Given $\chi, \chi' \in G^\vee$ with $\chi \neq \chi'$. There is a $g \in G$ with $\chi g \neq \chi' g$. Now as $\mathbf{S}^1$ is Hausdorff, there are disjoint open neighborhoods $U, U' \subset \mathbf{S}^1$ of $\chi g, \chi' g$. This gives us disjoint open neighborhoods $\mathcal{U}_{\{g\},U}, \mathcal{U}_{\{g\},U'}$ of g. $\square$

We define the functor $-^\vee$ to be the well-known functor $\mathrm{Hom}(-, \mathbf{S}^1)$, so $\phi^\vee = - \circ \phi$. We already know that $\mathrm{Hom}(-, \mathbf{S}^1)$ is a functor if we view $\mathrm{Hom}(G, \mathbf{S}^1)$ just as a group (without topology). Therefore, all that needs checking is that $\phi^\vee$ is continuous with respect to the compact-open topology. This is not hard to check:

Proof. Let $\phi : H \to G$ be a continuous group homomorphism and $\mathcal{U}_{K,U}$ a generator for the topology on $G^\vee$. Now $(\phi^\vee)^{-1}(\mathcal{U}_{K,U}) = \mathcal{U}_{\phi(K),U}$ and $\phi(K)$ is compact because K is. $\square$

1.2 The theorem

Theorem 1.4 (Pontryagin Duality)**.** *We have a contravariant equivalence of categories*

$$\begin{array}{rcl} \left\{ \begin{array}{c} \textit{locally compact groups} \\ \textit{(with cont. gp. homs.)} \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \textit{locally compact groups} \\ \textit{(with cont. gp. homs.)} \end{array} \right\} \\ G & \mapsto & G^\vee \\ H^\vee & \leftarrow\!\shortmid & H. \end{array}$$

It restricts to equivalences

$$\begin{array}{rcl} \{\textit{compact groups}\} & \longleftrightarrow & \{\textit{discrete groups}\} \\ \{\textit{profinite groups}\} & \longleftrightarrow & \{\textit{discrete torsion groups}\} \\ \{\textit{finite groups}\} & \longleftrightarrow & \{\textit{finite groups}\} \\ \{\textit{finite cyclic groups}\} & \longleftrightarrow & \{\textit{finite cyclic groups}\}. \end{array}$$

Furthermore: If G and H are dual, then

$$\begin{array}{rcl} \{\textit{closed subgroups of } G\} & \longleftrightarrow & \{\textit{closed subgroups of } H\} \\ U & \mapsto & U^\perp := \{h \in H : \forall g \in U : h(g) = 1\} \\ V^\perp := \{g \in G : \forall h \in V : h(g) = 1\} & \leftarrow\!\shortmid & V \end{array}$$

is an inclusion reversing bijection.

Example. 1. If C_n is a cyclic group of n elements, then $C_n^\vee \cong C_n$, because a character is completely determined by where it sends a generator, and such a generator must be sent to an n-th root of unity.

2. If A is a finite group, then $A = \prod C_{n_j} = \bigoplus C_{n_j}$, so by the universal property of the sum, $A^\vee = \mathrm{Hom}(\bigoplus C_{n_j}, \mathbf{S}^1) = \prod \mathrm{Hom}(C_{n_j}, \mathbf{S}^1) \cong \prod C_{n_j} = A$.

3. $\mathbb{Z}^\vee = \mathbf{S}^1$, because a character of $\mathbb{Z}$ is completely determined by where it sends 1.

   A character of $\mathbf{S}^1$ wraps the circle around itself a number of times continuously. This must happen linearly, so a character is detemined by the number of times to wrap the circle around itself. Indeed, the theorem says $(\mathbf{S}^1)^\vee = \mathbb{Z}^{\vee\vee} \cong \mathbb{Z}$.

The subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ and we have

$$\begin{array}{rcl} \mathbb{Z}^{\perp} & = & \{1\} \\ n\mathbb{Z}^{\perp} & = & \{n\text{-th roots of unity}\} \quad \text{if } n > 0 \\ \{0\}^{\perp} & = & \mathbf{S}^1 \end{array}$$

4. Let $\mathbb{R}$ be the additive group of real numbers. Then a character of $\mathbb{R}$ wraps $\mathbb{R}$ around the circle with a fixed speed, so $\mathbb{R}^{\vee} \cong \mathbb{R}$.

5. If $(A_j)_{j\in J}$ is any family of finite sets, then $(\bigoplus A_j)^{\vee} = \prod A_j^{\vee}$. This is true as an identity of sets by the universal property of the sum. The group law on both sides are the same and it is not hard to check that so are the topologies. Now $A_j^{\vee} \cong A_j$, so we get $(\bigoplus A_j)^{\vee} \cong \prod A_j$ and dually $(\prod A_j)^{\vee} \cong \bigoplus A_j$.

Exercise 1. Let $\mathbb{Z}_p$ be the ring of p-adic integers with the topology induced by the p-adic valuation. Prove that $\mathbb{Z}_p^{\vee}$ is, as a group, isomorphic to the group of points on $\mathbf{S}^1$, that have order a power of p. What is the topology on $\mathbb{Z}_p^{\vee}$?

The proof of the theorem works from the bottom up. The examples show how it works for finite groups. Then we can use this result for profinite groups and discrete torsion groups. There we can stop, because this is enough for the application in the second part of the lecture.

2 Kummer Theory

Now that we have seen Pontryagin Duality, we will apply it to Kummer Theory. Kummer Theory could also be proved with only duality for finite groups and with only finite Galois theory (see for example [Lan02] for a proof of only two pages). However, when we use Pontryagin duality, the reductions to the finite case are already done implicitly in the duality. Also, as a bonus, we will get direct information about the Galois group of the extensions and the proof will be more suitable for replacing parts of it with group cohomology.

2.1 Kummer extensions

Definition 2.1. We call a group G *of exponent* m if $g^m = e$ for every $g \in G$. We say that a field extension L/K is *of exponent* m if it is Galois and the Galois group is of exponent m.

Definition 2.2. A Kummer extension is an abelian extension of exponent m.

The following theorem forms the basis for the study of Kummer extensions.

Theorem 2.3. *Let K be a field, m an integer which is not divisible by the characteristic of K and assume that there is a primitive m-th root of unity ζ in K. Then*

1. *Let $a \in K$. Then $K(\sqrt[m]{a}\,)/K$ is a cyclic extension of degree $d|m$.*

2. *Conversely, let L/K be a cyclic extension of degree m. Then there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^m = a$ for some $a \in K$.*

Proof. We will only prove 1. For the converse statement, see for example [Lan02] Thm 6.2.

Let $a \in K$. If α is a root of $X^m - a$, then so is $\zeta^i\alpha$ for $i = 1, \dots, m$. Hence $K(\sqrt[m]{a}\,)$ is the splitting field of $X^m - 1$, which is a separable polynomial, because its derivative mX^{m-1} has only 0 as a root. Now let G be the Galois group of $K(\sqrt[m]{a}\,)/K$, then for any $g \in G$, $g(\alpha)$ is another root of $X^m - a$, so $g(\alpha)/\alpha$ is an m-th root of unity. As g is completely determined by $g(\alpha)$, this gives an injection of G into the cyclic group of m-th roots of unity. Hence G is cyclic of order dividing m. □

The extension $K(\sqrt[m]{a}\,)/K$ is cyclic and has degree dividing m. In particular it is a Kummer extension. The following lemmas show that all subextensions and composites of Kummer extensions are also Kummer extensions.

Lemma 2.4. Any subextension of a Kummer extension is a Kummer extension.

Proof. Any subextension L/K of an abelian extension M/K is abelian and the Galois group of L/K is a quotient of the Galois group of M/K. The quotient of a group of exponent m is of exponent m. □

Lemma 2.5. Let $\{L_i\}_{i \in I}$ be a family of Kummer subextensions of any field extension M/K. Let L be the composite. Then L is a Kummer extension.

Proof. We know that a composite of Galois extensions is a Galois extension. We can look at the group homomorphism

$$\begin{array}{rcl} \mathrm{Gal}(L/K) & \to & \prod_{i \in I} \mathrm{Gal}(L_i/K) \\ g & \mapsto & (g|_{L_i}). \end{array}$$

This map is injective, because the action of g on L is completely determined by the action on each of the L_i. Therefore, L/K is abelian and of exponent m. □

Together, these lemmas imply

Proposition 2.6. There is a unique Kummer subextension K_m/K of $\overline{K}/K$, which contains all other Kummer subextensions of $\overline{K}/K$. All subextensions of K_m/K are Kummer extensions.

2.2 Notation

Before we continue, let us fix some notation.

m	A positive integer.
K	A field which contains a primitive m-th root of unity. We assume that the characteristic of K does not divide m (i.e. $\mathrm{char}(K)$ is zero or coprime to m).
$K^{*m} \subset K^*$	The subgroup of all m-th powers of elements of K^*
$\mu_m \subset K^*$	The subgroup of m-th roots of unity. It is a cyclic group of order m, because $\mathrm{char}(K)$ does not divide m. We fix an embedding of μ_m inside the unit circle $\mathbf{S}^1$.
K_m/K	The maximal Kummer extension from the previous section.
G	The Galois group of K_m/K.

2.3 The pairing

Let $G = \mathrm{Gal}(K_m/K)$ and $H = K^*/K^{*m}$. We will define a bilinear map ψ by

$$\begin{array}{rcl} \psi : G \times H & \to & \mathbf{S}^1 \\ (g, a) & \mapsto & \dfrac{g(\alpha)}{\alpha}, \end{array}$$

where $\alpha^m = a$.

Let $a \in K^*$ be any element and let $\alpha \in K_m$ be an m-th root of a (we know that $\alpha \in K_m$, because $K(\sqrt[m]{a}\,)$ is a Kummer extension). Given $g \in G$, we know that $g(\alpha)$ is another m-th root of a, so it is of the form $\omega\alpha$ for some $\omega \in \mu_m$. In other words, we have $g(\alpha)/\alpha \in \mu_m$, which is inside $\mathbf{S}^1$, because of the agreed fixed embedding.

We will now show that it is welldefined. Note that ω only depends on a and g, not on α. Indeed, if α' is another m-th root of a, then $\alpha' = \zeta\alpha$ for some $\zeta \in \mu_m \subset K^*$, hence $g(\alpha')/\alpha' = \zeta g(\alpha)/(\zeta\alpha) = g(\alpha)/\alpha$. Notice also that $g(\alpha')/\alpha$ doesn't change if we multiply a by an element of K^{*m}, because then α gets multiplied with an element of K^*.

It is easy to see that the map is bilinear (i.e., $\psi(-,a)$ is a homomorphism for every a and $\psi(g,-)$ is a homomorphism for every g). This concludes the proof that we indeed have defined a map ψ.

Now ψ induces a group homomorphism (we do not speak about a topology on H for now)

$$\begin{array}{rcl} H & \to & G^\vee \\ a & \mapsto & \psi(-,a). \end{array}$$

First, we need to see that $\psi(-,a)$ is indeed inside $G^\vee$. We have already noted that it is a group homomorphism, but we need to see that $\psi(-,a) : G \to \mathbf{S}^1$ is continuous as well. To see this, note that $\psi(-,a)$ factors as

$$\begin{tikzcd} G \arrow[r, "\psi(-,a)"] \arrow[d, two heads] & \mathbf{S}^1 \\ G/\ker(\psi(-,a)) \arrow[ur] & \end{tikzcd}$$

The kernel of $\psi(-,a)$ consists of those g that leave α fixed, i.e. $\mathrm{Gal}(K_m/K(\sqrt[m]{a}\,))$, so the quotient at the bottom is the finite group $\mathrm{Gal}(K(\sqrt[m]{a}\,)/K)$. Now the leftmost map is continuous by definition of the topology on G and the rightmost map is continuous because finite groups are discrete. Therefore, $\psi(-,a)$ is continous.

Now, we will show that the map $H \to G^\vee$ is both injective and surjective, hence a group isomorphism. For *injectivity*, take any $a \in K^*$ which is not in K^{*m}, i.e. $\alpha \notin K^*$. Then there is a $g \in G$ such that $g(\alpha) \neq \alpha$, so $\psi(g,a) \neq 1$.

Finally, we will prove *surjectivity*. Given any character $\chi \in G^\vee$, we need to find $a \in H$ such that $\chi = \psi(-,a)$. Let's look at

$$\begin{tikzcd} G \arrow[r, "\chi"] \arrow[d, two heads] & \mathbf{S}^1 \\ G' = G/\ker(\chi) \arrow[ur] & \end{tikzcd}$$

The kernel $\ker(\chi)$ is $\mathrm{Gal}(K_m/L)$ for some field L and $G' = \mathrm{Gal}(L/K)$ for that field. Note that G' is isomorphic to the image in $\mathbf{S}^1$, but it is of exponent m, so it is cyclic of order $d|m$. Therefore, L/K is a *cyclic* subextension, hence (by theorem 2.3) L is of the form $K(\sqrt[d]{b}\,)$ for some $b \in K^*$. Let $a = b^{m/d}$, then $L = K(\sqrt[m]{a}\,)$. Let's compare χ and $\psi(-,a)$. They are both trivial on $\ker(\chi) = \mathrm{Gal}(K_m, L)$, so we will look at what they do with the quotient G'. Let $g \in G'$ be a generator, then $\psi(g,a) = \psi(g, b^{m/d})$ is some primitive d-th root of unity ζ and $\chi(g)$ is another, say ζ^k for some k coprime to d. If we replace b by b^k, then we get the same field $K(\sqrt[d]{b}\,)$, because $b^{kl} = b$ for some l. Meanwhile, $\psi(g,a)$ is taken to the power k, so $\psi(g,a) = \chi(g)$. This holds for the generator g of G', hence for all of G.

We now have an isomorphism $H \cong G^\vee$ and from Pontryagin duality, we know that $G^\vee$ is discrete. Therefore, we give H the discrete topology.

Example. Let $m = 2$, $K = \mathbb{Q}$. Then K satisfies the conditions, hence $G^\vee = K^*/K^{*2}$. Now $\mathbb{Q}^* = \{\pm 1\} \times \bigoplus \mathbb{Z}$ and $\mathbb{Q}^{2*} = \bigoplus 2\mathbb{Z}$, where the sum ranges over all positive primes. Therefore, $\mathbb{Q}^*/\mathbb{Q}^{*2} = \bigoplus \mathbb{Z}/2\mathbb{Z}$, where the sum ranges over all positive primes and -1.

The duality now tells us $G = (\bigoplus \mathbb{Z}/2\mathbb{Z})^\perp = \prod (\mathbb{Z}/2\mathbb{Z})^\perp = \prod \mathbb{Z}/2\mathbb{Z}$, where the product ranges over all positive primes and -1.

Exercise 2. Generalize this example to the case where m is any positive integer and K is a number field of class number 1, containing a primitive m-th root of unity.

Example. Let $\mathbb{F}_q$ be a finite field, let $m = q-1$ and let $K = \mathbb{F}_q(T)$ be the field of rational functions over $\mathbb{F}_q$. Then K contains $\mathbb{F}_q^*$, so it contains a primitive $q-1$-st root of unity. Also, because $\mathbb{F}_q(T)$ is the field of fractions of the PID $\mathbb{F}_q[T]$, we get

$$\begin{aligned} \mathbb{F}_q(T)^* &= \mathbb{F}_q^* \times \bigoplus \mathbb{Z}, \\ G^\vee = \mathbb{F}_q(T)^*/(\mathbb{F}_q(T)^*)^{q-1} &= C_{q-1} \times \bigoplus C_{q-1}, \end{aligned}$$

where the sum ranges over all monic irreducible polynomials in $\mathbb{F}_q[T]$.

2.4 Kummer Theory

Theorem 2.7 (Kummer Theory)**.** *Let K be a field and m a positive integer which is not divisible by the characteristic of K. Assume that K contains a primitive m-th root of unity. Then there is an inclusion preserving bijection*

$$\begin{array}{rcl} \{\textit{subgroups of } K^*/K^{*m}\} & \longleftrightarrow & \{\textit{abelian extensions of } K \textit{ of exponent } m\} \\ B & \mapsto & K(\sqrt[m]{B}\ ) \\ L^m \cap K^* & \leftarrow\!\shortmid & L. \end{array}$$

Proof. We have the following commutative diagram

$$\begin{tikzcd} \{\text{subext. of } K_m\} \arrow[r, shift left, "L \mapsto \mathrm{Gal}(K_m/L)"] \arrow[d, equal] & \{\text{cl. subgr. of } G\} \arrow[l, shift left, "K_m^A \leftarrow\!\shortmid A"] \arrow[d, leftrightarrow, "\perp"] \\ \{\text{Kummer subext. of } \overline{K}\} \arrow[r, leftrightarrow, dashed] & \{\text{subgr. of } K^*/K^{*m}\}, \end{tikzcd}$$

where the above bijection comes from Galois theory and the one on the right from Pontryagin duality and $G^\vee \cong K^*/K^{*m}$. The maps compose into a bijection at the bottom. So we will now find out what it does.

If we start with a subextension L/K of K_m/K and go through the diagram, then we end up at

$$\mathrm{Gal}(K_m/L)^\perp = \{a \in K^*/K^{*m} : \forall g \in \mathrm{Gal}(K_m/L) : \psi(g,a) = 1\}.$$

The condition $\psi(g,a) = 1$ is equivalent to $g(\alpha) = \alpha$ for an α with $\alpha^m = a$. But $g(\alpha) = \alpha$ for all $g \in \mathrm{Gal}(K_m/L)$ is equivalent to $\alpha \in L$, i.e. $a \in L^m$. Therefore,

$$L \mapsto \mathrm{Gal}(K_m/L)^\perp = L^m \cap K^*.$$

If we start with a subgroup B of K^* containing K^{*m}, then we will end up with some Kummer extension L. Let us compare L with another Kummer extension,

$K(\sqrt[m]{B}\,)$. Indeed, $K(\sqrt[m]{B}\,)$ is a Kummer extension, as it is the composite of the Kummer extensions $K(\sqrt[m]{a}\,)$ with $a \in B$.

The main thing we know about L is that $L^m \cap K^* = B$, so L contains an m-th root of every $a \in B$, hence $L \supset K(\sqrt[m]{B}\,)$. This implies

$$L^m \cap K^* \supset (K(\sqrt[m]{B}\,)^m \cap K^*) \supset B = L^m \cap K^*,$$

so $L^m \cap K^* = (K(\sqrt[m]{B}\,)^m \cap K^*)$, which implies $L = K(\sqrt[m]{B}\,)$ (because of the bijection). □

Example. Let's look at the example $K = \mathbb{Q}, m = 2$ again. Let $L = \mathbb{Q}(\sqrt{p} : p \text{ prime})$. Then $L = K(\sqrt[m]{B}\,)$, where B is the group of positive rational numbers. Now B corresponds to $\bigoplus_{p \text{ prime}} \mathbb{Z}/2\mathbb{Z}$ inside $\mathbb{Q}^*/\mathbb{Q}^{2*}$, so $\mathrm{Gal}(K_m/L) = B^\perp$ is only the part $\{\pm 1\}$ of $G = \{\pm 1\} \times \prod \mathbb{Z}/2\mathbb{Z}$. Therefore $\mathrm{Gal}(L/K) = G/\mathrm{Gal}(K_m/L) = \prod_{p \text{ prime}} \mathbb{Z}/2\mathbb{Z}$. This solves one of the exercises from last week.

2.5 Artin-Schreier Theory

So far, we only considered the case where m does not divide the characteristic of K. The theory where m equals the characteristic of K is called Artin-Schreier Theory.

Instead of polynomials $X^m - a$, we could have considered polynomials $X^p - X - a$. And instead of our basic theorem 2.3, we could have started out with

Theorem 2.8 (Artin-Schreier)**.** *Let K be a field of characteristic p.*

1. *Given $a \in K$, the polynomial $f(X) = X^p - X - a$ either has one root in K, in which case all roots are in K, or it is irreducible. In this latter case, if α is a root, then $K(\alpha)/K$ is cyclic of degree p.*
2. *Conversely, let L/K be a cyclic extension of degree p. Then there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^p - \alpha = a$ for some $a \in K$.*

Proof. [Lan02] Thm 6.4. □

We could then have considered the additive group $K = (K, +)$ instead of K^* and the operation $\wp(x) = x^p - x$ on that. Then we could have looked at $K/\wp(K)$ instead of K^*/K^{*m} and defined a pairing between G and $K/\wp(K)$ by $\psi(g, a) = g\alpha - \alpha$ where $\wp(\alpha) = a$. This would have resulted (with a similar proof) in

Theorem 2.9. *Let K be a field of characteristic $p > 0$. Then there is an inclusion preserving bijection*

$$\begin{array}{ccc} \{\textit{subgroups of } K/\wp(K)\} & \longleftrightarrow & \{\textit{abelian extensions of } K \textit{ of exponent } p\} \\ B & \mapsto & K(\wp^{-1}B), \end{array}$$

where $\wp^{-1}(a)$ means a root of $X^p - X - a$.

If one uses so called Witt vectors one could ([Lan02], exers. 46-51) prove a similar statement for $m = p^k$.

For remarks or questions about the text or if you want hints for the exercises: m.streng@math.uu.nl

References

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, revised third edition, 2002.

[NSW00] Jurgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften*. Springer, 2000.