Math 250A Lecture 13 Notes

Daniel Raban

October 10, 2017

1 Duality

1.1 Notions of duality for algebraic objects

1.1.1 Duality of vector spaces

Definition 1.1. Let V be a vector space over a field K. Then we have the *dual vector space*, $V^* = \text{Hom}(V, K)$.

Recall from linear algebra that we have a natural map $V \to V^{**}$ taking $v \mapsto (f \mapsto f(v))$ for $f \in Hom(V, k)$. Additionally, V^* is isomorphic to V if $\dim(V) < \infty$, but there is no natural isomorphism. This does not hold in the general case; if $V = \bigoplus_{n=1}^{\infty} K$, then V has countable dimension, but $\dim(V^*)$ is uncountable.

More generally, for objects in a category, we pick a "dualizing object," and let the dual be the set of homomorphisms to that object.

1.1.2 Duality of free modules

For free modules over a ring R, we take the dualizing object to be R. Then $M^* = \text{Hom}(M, R)$, and $M^{**} \cong M$ if $M \cong \mathbb{R}^n$. This also holds if M is projective. We have $M \oplus N$ is free, so $M \oplus N \cong (M \oplus N)^{**}$; then it is not difficult to obtain the property for M.

1.1.3 Duality for finite abelian groups

Since abelian groups are modules over $\mathbb{Z}$, one might think that you should make $\mathbb{Z}$ the dualizing object, but the only homomorphism from $G \to \mathbb{Z}$ is the trivial one. So make the dualizing object $\mathbb{Q}/\mathbb{Z}$.

Proposition 1.1. *Let G be a finite abelian group. Then $G \cong G^*$.*

Proof. G is a direct sum of cyclic groups, so it is enough to check for when is G cyclic. Whe have $G \cong \mathbb{Z}/n\mathbb{Z}$, which means that $G^* = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \{q\mathbb{Z} \in \mathbb{Q}/\mathbb{Z} : n(q\mathbb{Z}) = \mathbb{Z}\} = \{0, 1/n, 2/n, \dots, (n-1)/n\}$. This is cyclic of order n. $\square$

We also get that $G \cong G^{**}$, and this isomorphism is considered natural.

1.2 Applications of duality

1.2.1 Dirichlet characters

Definition 1.2. A *Dirichlet character* is an element of the dual of $(\mathbb{Z}/N\mathbb{Z})^*$, the group of units[1] of the ring $\mathbb{Z}/N\mathbb{Z}$.

Replace $\mathbb{Q}/\mathbb{Z}$ by S^1, unit circle in the complex numbers. We have the map $\mathbb{Q}/\mathbb{Z} \to S^1$ sending $x \mapsto e^{2\pi i x}$, so $\mathbb{Q}/\mathbb{Z} \cong$ elements of finite order in S^1.

Example 1.1. For $N = 8$, $(\mathbb{Z}/N\mathbb{Z})^* = \{1, 3, 5, 7\}$ with $1^2 = 5^2 = 7^2 = 1$. The characters are

	1	3	5	7
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	1	-1	-1
χ_3	1	-1	-1	1

Dirichlet was interested in this because he defined the Dirichlet L-function

$$\sum_{n\geq 1} \frac{\chi(n)}{n^s},$$

where χ is a Dirichlet character. When $N = 1$ and χ is the trivial character, we get the RIemann Zeta function.

Definition 1.3. Let χ_1, χ_2 be Dirichlet characters for the same N. Then the *inner product* of χ_1, χ_2 is

$$(\chi_1, \chi_2) := \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \chi_1(x)\overline{\chi_2(x)}.$$

Proposition 1.2. *Dirichlet characters are orthogonal.*

Proof. Let $\chi_1 \neq \chi_2$, and define the homomorphism $\chi = \chi_1\overline{\chi_2}$. Then $(\chi_1, \chi_2) = (\chi, 1)$, where 1 is the trivial character (sends everything to 1). Since $\chi_1 \neq \chi_2$, $\chi \neq 1$, so let $a \in \mathbb{Z}/N\mathbb{Z}$ with $\chi(a) \neq 1$. Then

$$\sum_{x\in(\mathbb{Z}/N\mathbb{Z})^*} \chi(x) = \sum_{x\in(\mathbb{Z}/N\mathbb{Z})^*} \chi(ax) = \chi(a) \sum_{x\in(\mathbb{Z}/N\mathbb{Z})^*} \chi(x),$$

where multiplying by a just reindexes the elements of $\mathbb{Z}/N\mathbb{Z}$. So we have

$$(\chi_1, \chi_2) = (\chi, 1) = \sum_{x\in(\mathbb{Z}/N\mathbb{Z})^*} \chi(x) = 0.$$ □

[1] We are being sloppy here by using $*$ to both mean dual and the group of units. In the case of $((\mathbb{Z}/N\mathbb{Z})^*)^*$, we mean $\mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^*, S^1)$.

1.2.2 The Fourier transform

Definition 1.4. Suppose f is a complex function on a finite group G. The Fourier transform $\tilde{f}$ is a function on G^*

$$\tilde{f}(\chi) = (\chi, f) = \sum_{x \in G} \chi(x) f(x).$$

Duality for infinite abelian groups (with a topology) follows a few rules:

1. The dualizing object is S^1.
2. Groups should be locally compact
3. Homomorphisms should be continuous.

Example 1.2. Let $G = \mathbb{Z}$. Then $G^* = \mathrm{Hom}(\mathbb{Z}, S^1) \cong S^1$. Let $H = S^1$. Then H^* is the continuous homomorphisms from $S^1 \to S^1$ ($z \mapsto z^n$ for $n \in Z$). These two groups are dual to each other.

The fourier transform takes function on S^1 to a fourier series (a function on $\mathbb{Z}$) by sending

$$f \mapsto \sum_n c_n e^{2\pi i n z}, \qquad c_n = \int_{z \in S^1} e^{-2\pi i n z} f(z)\, dz.$$

If $G = \mathbb{R}$, then $G^* = \mathrm{Hom}(\mathbb{R}, S^1) \cong \mathbb{R}$. This gives the fourier transform on $\mathbb{R}$.

1.2.3 Existence of "enough" injective modules

Def of injective module

Definition 1.5. An *injective module* I is a module with the following property. If the sequence $0 \to B \to A$ is exact, then any map $B \to I$ induces a homomorphism $A \to I$.

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r] \arrow[d] & C \arrow[dl, dashed] \\ & I & \end{tikzcd}$$

It is not immediately clear how we can find injective modules. The first step is to find a divisible abelian group.

We want to say that every module is a submodule of an injective module.

Definition 1.6. A group G is *divisible* if given $g \in G$ and $n \in \mathbb{Z}^+$, there exists some $h \in G$ with $nh = g$.

Example 1.3. $\mathbb{Q}/\mathbb{Z}$ is a divisible abelian group.

Finitely generated abelian groups are never divisible, except for the trivial group.

Proposition 1.3. *Let I be a module. If it is divisible as an abelian group, it is injective as a module.*

Proof. Pick $a \in A$ with $a \notin B$. We want to extend f to a. Pick the smallest $n > 0$ so that $na \in B$ if n exists. Extend f to a by putting $f(a) = g$, where $g \in I$ satisfies $ng = f(x)$. If n does not exist, then put $f(a)$ equals anything (it doesn't matter what we put here). Now extend f to all of A using Zorn's lemma (choose the maximal extension from submodules of A to I). □

Proposition 1.4. *Every abelian group is contained in an injective module.*

Proof. By the previous proposition, $\mathbb{Q}/\mathbb{Z}$ is injective, and given an abelian group G with an element $a \neq 0$ in G, we can find a homomorphism $f : G \to \mathbb{Q}/\mathbb{Z}$ such that $f(a) \neq 0$. So any abelian group G is a subset of a (possibly infinite) product of $\mathbb{Q}/\mathbb{Z}$s. □

Proposition 1.5. *Let R be a ring. Then the dual R^* is an injective R-module*

Proof. The key point is that $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ is an injective R-module. This is the dual of R as a $\mathbb{Z}$-module. Be careful; $\mathbb{Q}/\mathbb{Z}$ is a $\mathbb{Z}$-module but not necessarily an $\mathbb{R}$-module. If $f \in \mathrm{Hom}(R, \mathbb{Z})$ and $r, s \in R$, define fr by $fr(x) = f(rs)$ This makes $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ a right R-module.

The second key point is that $\mathrm{Hom}_R(M, \mathrm{Hom}(R, \mathbb{Q}/\mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$; this is easy but confusing to actually write out, so we leave it as an exercise. So finding an induced homomorphism from $A \to \mathrm{Hom}(R, \mathbb{Q}/\mathbb{Z})$ is the same problem as finding an induced homomorphism from $A \to \mathbb{Q}/\mathbb{Z}$, which is possible because $\mathbb{Q}/\mathbb{Z}$ is injective.

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r] \arrow[d] & C \arrow[dl, dashed] \\ & \mathrm{Hom}(R, \mathbb{Q}/\mathbb{Z}) & \end{tikzcd} = \begin{tikzcd} 0 \arrow[r] & B \arrow[r] \arrow[d] & C \arrow[dl, dashed] \\ & \mathbb{Q}/\mathbb{Z} & \end{tikzcd}$$

So $R^* = \mathrm{Hom}(R, \mathbb{Q}/\mathbb{Z})$ is injective, as claimed. □

2 Limits and Colimits

Recall from the lecture on category theory that a limit of a family $\{G_\alpha\}$ is a universal object with morphisms from $G \to G_\alpha$ for each α.

2.1 Colimits

Definition 2.1. A *colimit* G of the family $\{G_\alpha\}$ is universal object with morphisms from $G_\alpha \to G$ for each α. In other words, a colimit is the same concept as a limit, but the arrows (morphisms) go the other way.

$$\begin{tikzcd}
& Y & \\
& G \arrow[u, dashed, "\varphi"'] & \\
G_1 \arrow[uur] \arrow[ur, "f_1"'] \arrow[r, "g_{1,2}"'] & G_2 \arrow[u, "f_2"'] \arrow[uu, bend left] \arrow[r, "g_{2,3}"'] & G_3 \arrow[uul] \arrow[ul, "f_3"] \arrow[ll, bend left, "g_{3,1}"]
\end{tikzcd}$$

A special case is that if $G_i \to G_{i+1}$ is injective for all i, then the colimit, G, is more or less the union of the G_i.

$$\begin{tikzcd}
G_0 \arrow[r] \arrow[drr] & G_1 \arrow[r] \arrow[dr] & G_2 \arrow[r] \arrow[d] & G_3 \arrow[r] \arrow[dl] & \cdots \arrow[dll] \\
& & G & &
\end{tikzcd}$$

Example 2.1. $\mathbb{Q}/\mathbb{Z}$ is the union of $\mathbb{Z}/\mathbb{Z} \subseteq (\frac{1}{2}\mathbb{Z})/\mathbb{Z} \subseteq (\frac{1}{6}\mathbb{Z})/\mathbb{Z} \subseteq (\frac{1}{24}\mathbb{Z})/\mathbb{Z} \subseteq \cdots$.

2.1.1 Examples of colimits

Recall that the kernel $f : A \to B$, where A, B are groups is the equalizer of f and $\mathbb{1}$, the trivial map from $A \to B$; this is the limit of A, B with the morphisms $f, \mathbb{1}$.

Definition 2.2. The *cokernel* X of A and B is the colimit of A, B with morphisms $f, \mathbb{1}$.

$$\begin{tikzcd}
A \arrow[r, shift left, "f"] \arrow[r, shift right, "\mathbb{1}"'] \arrow[drr, bend right] & B \arrow[r] \arrow[dr] & Y \arrow[d, dashed] \\
& & X
\end{tikzcd}$$

This can also be thought of as the coequalizer of $f, \mathbb{1}$, where the coequalizer has the same definition as the equalizer but with the arrows reversed.

Definition 2.3. The *push-out* X is the colimit of A and B with morphisms $f : A \to C$ and $g : B \to C$.

$$\begin{tikzcd}
 & Y & \\
 & X \arrow[u, dashed, "\varphi"'] & \\
A \arrow[uur] \arrow[ur, "p_1"'] \arrow[dr, "f"] & & B \arrow[uul] \arrow[ul, "p_2"] \arrow[dl, "g"'] \\
 & C &
\end{tikzcd}$$

2.2 Exact sequences of colimits

When do colimits preserve exactlness? Say we have the following diagram with rows exact:

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & A_i \arrow[r] \arrow[d] & B_i \arrow[r] \arrow[d] & C_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_{i+1} \arrow[r] \arrow[d] & B_{i+1} \arrow[r] \arrow[d] & C_{i+1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Then

$$\cancel{0 \to} \operatorname{colim} A_i \to \operatorname{colim} B_i \to \operatorname{colim} C_i \to 0$$

is right exact but not left exact.

Example 2.2. Here is an example where the colimit is not left exact.

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r] \arrow[u, "\times 2"] \arrow[d, "\times 2"] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[u] \arrow[d, "\times 2"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[u] \arrow[d, "\times 2"] & 0 \\
 & \mathbb{Z} \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

The colimit $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not injective.

When do colimits preserve exactness, then?

Definition 2.4. A *directed set* S is a partially ordered set such that if $a, b \in S$, there exists a c with $a \leq c$ and $b \leq c$.

Example 2.3. The set $\mathbb{N}$ is directed under the usual ordering $\leq$.

Definition 2.5. A *direct limit* is a colimit of a family indexed by a directed set.

Proposition 2.1. *Direct limits preserve exactness.*

Proof. Suppose S is a directed set and we are taking the colimit over a family indexed by S. We have modules A_i for $i \in S$ with $A_i \to A_j$ with $i < j$. Every element of the colimit is representaed by some $a \in A_i$ for some i. This is because any element of the colimit is represented by some sum of elements $a_k \in A_j$ for various $j \in S$; then we can pick $c \geq$ all these j, and take the sum of the images of a_j in A_c.

Now suppose we have exact sequences $0 \to A_i \to B_i \to C_i \to 0$ for $i \in S$. We want to show that $\operatorname{colim} A_i \to \operatorname{colim} B_i$ is injective. Pick $a \in \operatorname{colim} A_i$. Then a is represented by some $a_i \in A_i$ for some $i \in S$. Now suppose that a_i has image 0 in $\operatorname{colim} B_i$. If b_i is the image of s_i, then $b_i = 0$ in the colimit. So for some j, the image of b_i in B_j is 0. So if a_j is the image of a_i in A_j, then a_j has image 0. Then $a_j = 0$, which makes $A_j \to B_j = 0$, and so $s_j = 0$ in the colimit. □

2.3 Inverse limits and the p-adic integers

Look at $G = \mathbb{Z}[1/p]/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$. This is the colimit of $\mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{Z}/p^2\mathbb{Z} \subseteq \mathbb{Z}/p^3\mathbb{Z} \subseteq \cdots$. What is G^*? We get

$$\operatorname{Hom}(\mathbb{Z}/p\mathbb{Z}, S^1) \leftarrow \operatorname{Hom}(\mathbb{Z}/p^2\mathbb{Z}, S^1) \leftarrow \operatorname{Hom}(\mathbb{Z}/p^3\mathbb{Z}, S^1) \leftarrow \cdots$$

Definition 2.6. The *inverse limit* is the limit of a directed family $\{A_\alpha\}$.

So the dual of a direct limit is the inverse limit of the duals. The dual for our example above is the p-adic integers $\mathbb{Z}_p$. Look at

$$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots$$

Then the p-adic integers is the inverse limit of this. We get the set of sequences of base p expansions going to the left an infinite distance. For example, if $p = 3$, such a sequence would look like $(\ldots, 2, 1, 2, 2, 0, 1, 2)$. Addition and multiplication are indeed well-defined componentwise.

Does taking inverse limits preserve exactness? The answer is no, even if the set is directed.

Example 2.4. Take the following diagram, where the rows are exact:

$$
\begin{tikzcd}
 & {} \arrow[d] & {} \arrow[d] & & \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "\times 3"] & \mathbb{Z} \arrow[r] \arrow[d, "\times 3"] & \mathbb{Z}/2\mathbb{Z} & \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "\times 3"] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "\times 3"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[u] \arrow[d, "\times 2"] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd}
$$

The inverse limits give us $0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0$, but this is not exact.

However, there is hope! Taking inverse limits preserve exactness if the A_i preserve the Mittag-Leffler[2] condition.

[2] This sounds like two people, but it is actually just one.