BLUEPRINT FOR GORDAN'S LEMMA

ABSTRACT. A blueprint for Gordan's Lemma.

What we are going for is the following. Let Λ be a finite free $\mathbb{Z}$-module, and let $\Lambda^* := \mathrm{Hom}(\Lambda, \mathbb{Z})$ be its dual. If S is a subset of Λ^* (always finite, in practice, I think) then its *dual* $\mathbb{Z}$*-cone* $S^\vee$ consists of the $t \in \Lambda$ such that $\langle s, t\rangle \geq 0$ for all $s \in S$.

Note that the dual $\mathbb{Z}$-cone is an additive submonoid of Λ, but it need not be a $\mathbb{Z}$-module: multiplying by negative integers will reverse all the inequalities implied by being in the dual $\mathbb{Z}$-cone! For instance $\mathbb{N} \subset \mathbb{Z}$ is the dual $\mathbb{Z}$-cone of $\{1\} \subset \mathbb{Z}$, viewing $\mathbb{Z}$ as its own dual, via multiplication.

Our goal is to prove the following result.

Theorem 1 (Gordan's Lemma). *If $S \subset \Lambda^*$ is finite, then $S^\vee \subset \Lambda$ is a finitely-generated additive monoid.*

1. Algebraic proof

We follow the algebraic proof in Wikipedia.

Theorem 2. *If M is an additive abelian monoid and R is a nonzero commutative ring, then M is finitely-generated as a monoid iff the monoid algebra $R[M]$ is finitely-generated as an R-algebra.*

Proof. Because R is nonzero, we can think of M as a subset of $R[M]$: even more, we can think of M as a multiplicative submonoid of $R[M]$.

First, say M is finitely generated by $S \subseteq M$. The R-subalgebra of $R[M]$ generated by S contains all of M, and is an R-module so it's all of $R[M]$.

Conversely, say $R[M]$ is finitely-generated. If $f \in R[M]$ then it has a support, which is a finite subset of M. Now f is in the R-submodule generated by its support, and hence is in the R-subalgebra generated by the support. So if we have finitely many f's which generate $R[M]$ as an R-algebra then we can replace each f by its support and get a finite subset of M which generates a subalgebra of $R[M]$ which contains all the f's and hence is all of $R[M]$. We deduce that a finite subset S of M generates $R[M]$ as an R-algebra. We claim that S generates M as an additive monoid. This follows because the R-algebra generated by S is the R-module generated by the monoid generated by S, and the monoid generated by S is a subset of M. □

We prove Gordan's Lemma by two layers of induction. First, proceed by induction on the rank of Λ.

First induction on $\mathrm{rk}\,\Lambda$**: base case.** The result is clear in the case in which the rank of Λ is 0: in this case, $\Lambda = 0$ and the empty set generates the unique additive submodule of $\Lambda = 0$.

First induction on $\mathrm{rk}\,\Lambda$**: inductive step.** Assume that the rank of Λ is strictly positive and that, for every free, finitely generated $\mathbb{Z}$-module Λ' of rank strictly smaller than the rank of Λ, the dual set of every finite subset of $(\Lambda')^*$ is a finitely generated additive monoid.

Note for formalization. We really only need the case of rank one less. In fact, we are going to apply the inductive hypothesis to a submodule of Λ obtained as the kernel of a non-zero linear map $\Lambda \to \mathbb{Z}$.

Proceed by induction on (the size of) S (within the inductive step of the first induction on $\operatorname{rk}\Lambda$).

Note for formalization. In the second induction we play around with S. Note that the set $S^\vee$ coincides with the dual $\mathbb{Z}$-cone on the set of points of the $\mathbb{N}$-submodule spanned by S (or even its saturation). I, DT, do not know whether or not this observation makes the formalization simpler.

Second induction on $\#S$: base case. For S empty the result is clear: the dual of the empty set is the whole Λ and if $\lambda \subset \Lambda$ generates Λ as a $\mathbb{Z}$-module, then $\lambda \cup \{-\ell : \ell \in \lambda\}$ generates Λ as an additive monoid.

Second induction on $\#S$: induction step. For the inductive (in the size of $\#S$) step, it suffices to check that if $S^\vee$ is finitely-generated then so is $(S \cup \varphi)^\vee$. We use the equality

$$(S \cup \varphi)^\vee = S^\vee \cap \{v \in \Lambda : \varphi(v) \geq 0\},$$

which follows from the definitions.

The result is clear if $\varphi = 0$: in this case φ imposes no extra condition on $S^\vee$, the equality

$$(S \cup \{0\})^\vee = S^\vee$$

holds, and we know the result for $S^\vee$.

Thus, assume that φ is non-zero. Choose any non-zero, commutative ring with identity R. Set $M = S^\vee$ and write $A = R[M]$; this is finitely-generated as an R-algebra by Theorem 2. Define

$$\deg_\varphi \colon M \to \mathbb{Z}$$

by $\deg_\varphi(v) = \varphi(v)$. Define A_n to be the R-module generated by the $v \in M$ with $\deg_\varphi(v) = n$; this determines a $\mathbb{Z}$-grading on A. By Theorem 2, it suffices to prove that the subring $A_{\geq 0} := \oplus_{n \geq 0} A_n$ is finitely-generated as an R-algebra.

First note that $A_0 = R[T]$ where $T = \{v \in M : \deg(v) = 0\}$ is a subalgebra, so it suffices to prove that

- A_0 is a finitely-generated R-algebra, and that
- $A_{\geq 0}$ is a finitely-generated A_0-algebra.

Lemma 3. *The R-algebra $A_0 = R[T]$ is finitely generated.*

Proof. We use the equivalence of Theorem 2: it suffices to show that T is finitely generated as a monoid. Recall that, by definition, T is the submonoid of Λ satisfying

$$T = \{v \in M : \deg(v) = \varphi(v) = 0\} \subset \ker\varphi.$$

Since we reduced to the case in which φ is non-zero, we know that $\ker\varphi$ is a free, finitely-generated $\mathbb{Z}$-module of rank equal to $\operatorname{rk}\Lambda - 1$.

To apply the induction hypothesis, we check that $T \subset \ker\varphi$ is the dual of a finite subset of $(\ker\varphi)^*$. Observe that the dual of $\ker\varphi$ is the quotient of Λ^* by the saturation of the additive subgroup generated by φ. By construction, T is therefore the dual set of the image of S under the projection

$$\Lambda^* \to \left(\Lambda^*/\langle\varphi\rangle^{\mathrm{sat}}\right) \simeq (\ker\varphi)^*.$$

By the induction step of the first induction (on the number of generators of Λ), we know that T is finitely generated, as needed. $\square$

> **Note for formalization.** The saturation can be avoided by working, more generally, not with the dual of Λ, but with a $\mathbb{Z}$-module of linear functionals on Λ that surjects onto the dual of Λ. Alternatively, it can also be avoided by replacing φ by $\varphi' \in \Lambda^*$, where $\varphi = a\varphi'$, with $a \in \mathbb{N}$ chosen as the largest it can be for such an identity to hold.

To prove the second, and final, step, we show the following more general result.

Lemma 4. *Let A be a Noetherian $\mathbb{Z}$-graded ring. Denote by $A_{\geq 0} = \oplus_{n \geq 0} A_n$ the sub-algebra of A consisting of the elements of A of non-negative degree. The ring $A_{\geq 0}$ is finitely generated as an A_0-algebra.*

Proof. Let I be the ideal of A that is generated by all the homogeneous elements of strictly positive degree. (Note that, since A might have elements of negative degree, the ideal I might contain elements of negative degree as well.)

Since A is Noetherian, the ideal I admits a finite generating set: choose one and denote its elements by $f_1, \ldots, f_n$. Since each element of I is an A-linear combination of homogeneous elements of strictly positive degree, we can replace each chosen generator by the collection of all the elements of I that appear in such linear combinations. Thus, we further assume that the chosen generators are

- homogeneous, and
- have strictly positive degree.

Let $N_0 \in \mathbb{N}$ be the maximum of the degrees of the generators $f_1, \ldots, f_r$:

$$N_0 = \max\{\deg f_1, \ldots, \deg f_r\}.$$

Let $A_{0 \leq N} \subset A_{\geq 0}$ be the subset consisting all the homogeneous elements of degree at most N. Note that, in particular, all the chosen generators $f_1, \ldots, f_r$ are contained in $A_{0 \leq N}$. We show that $A_{0 \leq N}$ generates $A_{\geq 0}$ as an A_0-algebra.

More precisely, we show that, for all $n \in \mathbb{N}$, every element $f \in A_{\geq 0}$ of degree n in the A_0-algebra $A_{\geq 0}$ is generated by $A_{0 \leq N}$ as an A_0-algebra. (If this is any help, this step is entirely analogous to the proof that the Weak Mordell-Weil Theorem implies the Mordell-Weil Theorem: it is a relatively standard "Noetherian induction" argument.)

Proceed by induction on n, starting the induction at $n = N$. For the base case there is nothing to prove: the result is true if $n = N$, by definition of $A_{0 \leq N}$.

Suppose that $A_{0 \leq N}$ generates every element of $A_{\geq 0}$ of degree at most n, for some natural number n satisfying $N \leq n$. Let f be an element of $A_{\geq 0}$ of degree $n + 1$. By homogeneity of the ideal, we can assume that f is homogeneous of degree $n + 1$.

Since $f_1, \ldots, f_r$ generate I, the homogeneous element f admits a decomposition

$$f = \sum_{i=1}^{r} g_i f_i$$

with $g_1, \ldots, g_r$ homogeneous elements. Since the degrees of the generators $f_1, \ldots, f_r$ are strictly positive, the inequalities

$$\deg g_1 < \deg f, \ldots, \deg g_r < \deg f$$

hold. Since the degree of f is $n+1$ and n satisfies $N = \max\{\deg f_1, \ldots, \deg f_r\} \leq n$, the degrees of $g_1, \ldots, g_r$ satisfy

$$0 \leq \deg g_1 < \deg f, \ldots, 0 \leq \deg g_r < \deg f.$$

By the inductive hypothesis, each one of the elements $g_1, \ldots, g_r$ is in the A_0-algebra generated by $A_{0 \leq N}$, as stated.

Thus, it suffices to show that $A_{0 \leq N}$ is finitely generated as an A_0-module. For this, we show that, for each natural number n, the homogeneous degree piece A_n is finitely generated as an A_0-module.

Note for formalization. For the given proof, it seems important that we work with a *unique* graded piece: I do not see right away how to make the argument work with $A_{0 \leq N}$ directly.

This is again a consequence of Noetherianity of A. Suppose that

$$N_1 \subset N_2 \subset \cdots \subset N_i \subset \cdots$$

is an increasing chain of A_0-submodules of A_n, such that $\cup_i N_i = A_n$. The chain of ideals

$$N_1 A \subset N_2 A \subset \cdots \subset N_i A \subset \cdots$$

stabilizes, since A is Noetherian. Intersecting with A_n, we find that the sequence

$$N_1 A \cap A_n \subset N_2 A \subset \cap A_n \cdots \subset N_i A \cap A_n \subset \cdots$$

also stabilizes. Finally, we observe that, for all indices i, the equality $N_i A \cap A_n = N_i$ holds: since all the elements of N_i are homogeneous of degree n, the only A-multiples of the elements of N_i that have degree n are the multiples by homogeneous elements of degree 0. Since N_i is an A_0-module, we are done. $\square$