Math 615, Winter 2020: Lecture of Wednesday, March 25

We continue the study of subrings of polynomial and Laurent polynomial rings generated by monomials. We do this by studying the vectors of exponents in $\mathbb{Z}^n$ (if there are n variables): the set of vectors is an additive subsemigroup of $\mathbb{Z}^n$. Such a semigroup H determines a subring of $S = K[x_1, 1/x_1, \ldots, x_n, 1/x_n]$ for every field K, namely $K[x^H] = K[x_1^{a_1} \cdots x_n^{a_n} : (a_1, \ldots, a_n) \in H]$. It turns out that this ring is integrally closed in its fraction field (also called normal) if and only if H is *normal* in the sense defined below (the definition and theorem are given in the third and fourth paragraphs of the next page). Note that the condition for normality depends only on the semigroup H, and not on its embedding in $\mathbb{Z}^n$. The condition for normality of the algebra depends only on the semigroup, not on the field. Also note that the algebra one gets need not be Noetherian: see the Example at the top of the third page of the notes for this lecture.

The notion of a *full* subsemgroup of $\mathbb{N}^n$ is also introduced, in the middle of the third page of the notes for this lecture, following the example. Observe that in this case, negative exponents are not allowed. Moreover, whether $H \subseteq \mathbb{N}^n$ is full depends on the embedding in $\mathbb{N}^n$, not just on the semggroup H. The importance of this notion is that when H is full, the ring $K[x^H]$ is a direct summand, as a module over itself, of the polynomial ring $K[x_1, \ldots, x_n]$. Hence, for full semigroups, $K[x^H]$ is Cohen-Macaulay.

Another major result is that a finitely generated normal subsemigroup is isomorphic with the direct sum of a group $\mathbb{Z}^K$ and a full subsemigroup of some $\mathbb{Z}^s$. From this one sees that given a finitely generated normal subring R of the Laurent polynomials S or of the usual polynomial ring, R is Cohen-Macaulay! A key point in the proof of this is that if a subsemigroup of Z^n does not contain a nonzero element u and its inverse $-u$, then it is isomorphic with a full subsemgroup of some $\mathbb{N}^s$. The proof of this fact depends on studying convex geometry over the rational numbers $\mathbb{Q}$. I am designating this material optional.

We next want to consider when a K-subalgebra of $S = K[x_1, 1/x_1, \ldots, x_n, 1/x_n]$ generated by monomials is normal. This is entirely a property of the semigroup of monomials involved, and does not depend on the base field.

We shall typically work with the additive semigroup of exponent vectors, which is a subsemigroup H of $\mathbb{Z}^n$. If $\alpha = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, we write x^α for $x_1^{a_1} \cdots x_n^{a_n}$. Then the K-subalgebras of S generated by monomials correspond bijectively to the subsemigroups H of $\mathbb{Z}^n$: given H, the corresponding subalgebra is the K-span of $\{x^\alpha : \alpha \in H\}$.

If H is an additive (which we intend to imply commutative) f semigroup such that cancellation holds, i.e., if $\alpha, \alpha', \beta \in H$ and $\alpha + \beta = \alpha' + \beta$ then $\alpha = \alpha'$, then there is an essentially unique way to enlarge H to group that is generated by H. Define an equivalence relation on $H \times H$ by the rule $(\alpha, \beta) \sim (\alpha', \beta')$ precisely when $\alpha + \beta' = \alpha' + \beta$. The equivalence classes form a semigroup such that

$$[(\alpha_1, \beta_1) + [(\alpha_2, \beta_2)] = [(\alpha_1 + \alpha_2, \beta_1 + \beta_2)].$$

H embeds in this new semigroup by sending $\alpha \mapsto [(\alpha, 0)]$. The 0 element is represented by $(0, 0)$ and also by those elements of the form (α, α). There are now inverses since $[(\alpha, \beta)] + [(\beta, \alpha)] = [(\alpha + \beta, \alpha + \beta)] = [(0, 0)]$. In particular, $[(\beta, 0)]$ has additive inverse $[(0, \beta)]$. Thus, the new semigroup is a group, and if we identify $\alpha \in H$ with its image, then every element of this group has the form $\alpha - \beta$ for choices of α, $\beta \in H$. We denote this group $H - H$. If we have any other injection of H into a semigroup G that is a group, then the subgroup of G generated by H is isomorphic with $H - H$.

In particular, when H is a subsemigroup of $\mathbb{Z}^n$, the group $H - H$ depends only on H, not on its embedding in $\mathbb{Z}^n$.

We define $H \subseteq \mathbb{Z}^n$ to be *normal* if whenever α, $\alpha' \in H$ and there is a positive integer k such that $k(h - h') \in H$, then $h - h' \in H$.

Theorem. *For every field K, $R = K[x^\alpha : \alpha \in H]$ is normal if and only if H is normal.*

Proof. First suppose that the subalgebra R is normal, and that $k(\alpha - \alpha') \in H$, where k is a positive integer. Then x^α, $x^{\alpha'} \in R$, and $f = x^\alpha / x^{\alpha'} = x^{\alpha - \alpha'}$ is an element of the fraction field integral over R, since $f^k \in R$. Hence, $f \in R$, and so $\alpha - \alpha' \in H$.

We next show that the condition that H be normal is sufficient for R to be normal. Suppose that we can solve the problem when K is an infinite field, e.g., an algebraically closed field. If K is finite, let L be an infinite field containing K. Then

$$R = K[x_1, 1/x_1, \ldots, x_n, 1/x_n] \cap L[x^\alpha : \alpha \in H],$$

and since both the rings being intersected are normal, R is normal as well.

Therefore we may assume that K is infinite. The group of invertible diagonal matrices $\mathcal{D}_n$ acts on S, and R is stable. One can then show thiat that the integral closure of R will be spanned by monomials. Consider the ring obtained by adjoining the inverses of all monomials in R. This ring R_1 corresponds to $H - H$, which is isomorphic with a free abelian group $\mathbb{Z}^h$, and so R_1 is isomorphic with a localized polynomial ring obtained by adjoining h algebraically independent elements and their inverses to K. Thus, R_1 is normal, and so any monomial in the normalization of R is in R_1.

It follows that if R is not normal, then there is a monomial $\mu = x^\alpha / x^{\alpha'}$, where $\alpha, \alpha' \in H$, that is integral over R and not in R. Choose a monic polynomial $F(Z)$ with coefficients in R of degree k satisfied by μ. Assign Z the same monomial degree as μ. Then the sum of the terms whose monomial degree is μ^k must also vanish when we substitute $Z = \mu$, and so we have an equation of integral dependence that is monomially graded. Since R is a domain, there is no loss of generality in assuming that the constant term is nonzero: if necessary, we may factor out a power of Z. We continue to call the degree k. Then μ^k has the same monomial degree ν as the constant term $c\nu$, where $c \in K - \{0\}$, and ν is a monomial in R. This shows that $k(\alpha - \alpha') \in H$, and so $\alpha - \alpha' \in H$ and $\mu \in R$ after all. $\square$

Example. Let K be any field, let $\lambda \geq 0$ be a real number, and let

$$H_\lambda = \{(a,\, b) \in \mathbb{N}^2 : a/b > \lambda\}.$$

It is easy to see that if $0 \leq \lambda < \lambda'$ then H_λ is strictly larger than $H_{\lambda'}$. Morever, every H_λ is a normal semigroup. Let $R_\lambda = K[x^\alpha : \alpha \in H_\lambda]$. This gives an uncountable chain $\{R_\lambda\}_{\lambda \geq 0}$ of normal subrings of $K[x_1,\, x_2]$. None of the rings R_λ is Noetherian: if R_λ were Noetherian, the fact that it is $\mathbb{N}$-graded over K would imply that it is finitely generated by elements

$$x_1^{a_1}x_2^{b_1},\, \ldots,\, x_1^{a_n}x_2^{b_n}$$

with every $a_j/b_j > \lambda$. Let $s > \lambda$ be the minimum of the rational numbers $a_1/b_1,\, \ldots,\, a_n/b_n$. Then

$$K[x_1^{a_1}x_2^{b_1},\, \ldots,\, x_1^{a_n}x_2^{b_n}]$$

does not contain any monomial $x^a y^b$ with $a/b < s$, and so cannot be equal to R_λ. $\square$

The Example above shows that the condition of being normal is too weak to imply that a semigroup is finitely generated. We next want to consider a much stronger condition on subsemigroups of $\mathbb{N}^n$ which implies *both* normality and finite generation.

We say that a subsemigroup $H \subseteq \mathbb{N}^n$ is *full* if whenever $\alpha, \alpha' \in H$ and $\alpha - \alpha' \in \mathbb{N}^n$ then $\alpha - \alpha' \in \mathbb{N}$. We observed at the end of the previous lecture that the subsemigroups obtained from rings of invariants of torus actions on polynomial rings are full.

It is obvious that full subsemigroups are normal, for if $k(\alpha - \alpha') \in H$, then $k(\alpha - \alpha') \in \mathbb{N}^n$, and since $k > 0$, this implies that $\alpha - \alpha' \in H$. Something much stronger is true.

Theorem. *Let H be a full subsemigroup of $\mathbb{N}^n$. Let $R = K[x^\alpha : \alpha \in H]$, where K is any field. Then $R \hookrightarrow K[x_1,\, \ldots\, , x_n]$ is split. Hence:*

(a) *R is a finitely generated K-algebra, and so H is a finitely generated semigroup.*

(b) *R is Cohen-Macaulay.*

Proof. Let W be the K-span of the monomials x^β for $\beta \in \mathbb{N}^n - H$. Evidently, $K[x_1,\, \ldots\, , x_n] = R \oplus W$ as K-vector spaces. To complete the proof that we have a splitting, it suffices to show that W is an R-module. This comes down to the assertion that if $\alpha' \in H$, so that $x^{\alpha'} \in R$, and $\beta \in \mathbb{N}^n - H$, so that $x^\beta \in W$, then $x^{\alpha'}x^\beta \in W$. Suppose not. Then $x^{\alpha' + \beta} = x^\alpha$, where $\alpha \in H$. But thihs means that $\beta = \alpha - \alpha' \in \mathbb{N}^n$. By the definition of full subsemigroup, $\beta \in H$, a contradiction.

The first statement in part (a) follows from the Lemma at the top of p. 2 of the Lecture Notes of March 11, and the second statement in part (a) is an Immediate consequence. Part (b) the follows from the Theorem at the top of p. 4 of the Lecture Notes of March 11. $\square$

We shall complete the proof that finitely generated normal K-subalgebras of S are Cohen-Macaulay by proving the following

Theorem. *Let H be a finitely generated normal subsemigroup of $\mathbb{Z}^n$. Then $H \cong \mathbb{Z}^k \oplus H'$, where H' is isomorphic to a full subsemigroup of $\mathbb{N}^n$.*

It will then follow that $K[x^\alpha : \alpha \in H]$ is the polynomial ring in k variables with the inverses of the variables adjoined over $K[x^\alpha : \alpha \in H']$. Thus, the remaining work is in the proof of the Theorem just above, most of which we postpone for a bit. However, we can immediately give the part of the argument in which we split off $\mathbb{Z}^k$.

First part of the proof of the Theorem. First, replace $\mathbb{Z}^n$ by $H - H \subseteq \mathbb{Z}^n$. Since a subgroup of $\mathbb{Z}^n$ will also be a finitely generated free abelian group, we may assume that $H - H = \mathbb{Z}^n$ (the property of being a normal semigroup is not affected). Let G be the set of all elements of H with additive inverses in H. Then G contains 0 and is closed under addition. It follows that G is a subgroup of $\mathbb{Z}^n$, and so $G \cong \mathbb{Z}^k$ for some $k \in \mathbb{N}$. We next claim that $\mathbb{Z}^n/G$ is torsion-free. Suppose $\beta \in \mathbb{Z}^n = H - H$ and $k\beta \in G$. Then $k(-\beta) \in G$ as well, and both β and $-\beta$ are in $\mathbb{Z}^n = H - H$. It follows that β and $-\beta$ are both in H, and so $\beta \in G$, as required.

Thus, $\mathbb{Z}^n/G$ is a finitely generated torsion-free abelian group, and it follows that it is free. Thus,

$$0 \to G \to \mathbb{Z}^n \to \mathbb{Z}^n/G \to 0$$

splits. Let $G' \cong \mathbb{Z}^h \cong \mathbb{Z}^n/G$ be a free complement for G in H. Every element $\beta \in H$ can be expressed uniquely as $\alpha + \alpha'$ where $\alpha \in G$ and $\alpha' \in G'$. But $-\alpha \in H$, and so $\alpha' \in H$. Thus, $H = G \oplus H'$, where $H' = H \cap G'$, and may also be viewed as the image of H under the projection $\mathbb{Z}^n = G \oplus G' \cong G \times G' \twoheadrightarrow G'$. It follows that H' is a finitely generated subsemigroup of G'. Evidently, H' does not contain the additive inverse of any of its nonzero elements, since $G \cap H' = 0$. Moreover, H' is normal: if $\beta \in H - H'$ and $\kappa\beta \in H'$, then $\beta \in H$, and may be written uniquely as $\alpha + \alpha'$ with $\alpha \in G$ and $\alpha' \in H'$. Then $k\alpha + k\alpha' \in H'$, and so $k\alpha = 0$. It follows that $\alpha = 0$, and $\beta = \alpha' \in H'$, as required. The proof of the Theorem above therefore reduces to establishing the following

Lemma. *Let H be a finitely generated normal subsemigroup of $\mathbb{Z}^n$ such that there is no nonzero element with an additive inverse in H. Then H is isomorphic with a full subsemigroup of $\mathbb{N}^s$ for some nonnegative integer s.*

The proof of this Lemma will be carried through by studying a class of semigroups in $\mathbb{Q}^n$ that are closed under multiplication by elements of $\mathbb{Q}^+$, the positive rational numbers. What we need is an understanding of convex geometry over $\mathbb{Q}$.

Optional material

Geometry in vector spaces over the rational numbers

The results in this section are proved over $\mathbb{Q}$: the statements and proofs are valid with no changes whatsoever if $\mathbb{Q}$ is replaced by any field between $\mathbb{Q}$ and $\mathbb{R}$, including $\mathbb{R}$, or any ordered field. The results are, in fact, more "standard" over $\mathbb{R}$.

Let V be a vector space over $\mathbb{Q}$. By a *$\mathbb{Q}^+$-subsemigroup C* of V we mean a subsemigroup that is closed under multiplication by elements of $\mathbb{Q}^+$. (It would also be natural to refer to C as a *convex cone*: it will be closed under taking all linear combinations with nonnegative coefficients, and will be a union of "rays" emanating from the origin.) Henceforth, V will be assumed finite-dimensional. We say that C is *finitely generated over* $\mathbb{Q}^+$ if it has finitely many elements $\alpha_1, \ldots, \alpha_h$ such that every element of C is a $\mathbb{Q}^+$-linear combination of the elements $\alpha_1, \ldots, \alpha_h$. We write V^* for the $\mathbb{Q}$-vector space $\mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$, which is finite-dimensional of the same dimension as V. Its elements will be called *linear functionals* on V.

If L is a nonzero linear functional on V, the set $\{\alpha \in V : L(\alpha) \geq 0\}$ is called a *half-space*. The set $\{\alpha \in V : L(\alpha) \leq 0\}$ is also a half-space, since we may replace L by $-L$. We can always choose a basis for V consisting of $n-1$ vectors $e_1, \ldots, e_{n-1}$ in the kernel of V and a vector e_n on which L has the value 1. If we identify V with $\mathbb{Q}^n$ using this basis, the half-space determined by L is is identified with $\{(q_1, \ldots, q_n) \in \mathbb{Q}^n : q_n \geq 0\}$: we refer to this as the *standard example* of a half-space. A half-space is a $\mathbb{Q}^+$-subsemigroup that is finitely generated: it suffices to see this for the standard example. Then generators are the vectors $e_1, \ldots, e_{n-1}$, $-e_1, \ldots, -e_{n-1}$, and e_n.

We shall say that a $\mathbb{Q}^+$-subsemigroup C *has no line* or is a $\mathbb{Q}^+$-subsemigroup *with no line* if there is no nonzero vector in C whose additive inverse is in C: it is equivalent that C does not contain a one-dimensional vector subspace of the ambient space.

If C is a finitely generated $\mathbb{Q}^+$-subsemigroup we may take any set of generators, and choose a minimal subset with the property of generating C over $\mathbb{Q}^+$. We shall call these elements *a minimal set of generators of C*.

Lemma. *Let V be a finite-dimensional $\mathbb{Q}$-vector space.*

(a) *Every finite intersection of half-spaces in V is a finitely generated $\mathbb{Q}^+$-subsemigroup.*

(b) *Let C be be any $\mathbb{Q}^+$-subsemigroup in V. Let W be the subset of C consisting of elements with an additive inverse in C. Then W is a vector subspace of V, and if W' is a vector space complement for W in V, then $C = W \oplus C'$, where $C' = C \cap W'$ is also the projection of C on W'. C' is a finitely generated $\mathbb{Q}^+$-subsemigroup with no line.*

(c) *If C is a $\mathbb{Q}^+$-subsemigroup with no line, $\alpha_1, \ldots, \alpha_h \in C$, $c_1, \ldots, c_h \in \mathbb{Q}^+$, and $c_1\alpha_1 + \cdots + c_h\alpha_h = 0$, then $\alpha_1 = \cdots = \alpha_h = 0$.*

(d) *Let C be a finitely generated $\mathbb{Q}^+$-subsemigroup with no line and let α, β be part of a minimal set of generators for C. Then $C_1 = C + \mathbb{Q}\alpha$, which is the $\mathbb{Q}^+$-subsemigroup generated by C and $-\alpha$, does not contain $-\beta$.*

Proof. For part (a) we use induction on the number of half-spaces. We have already proved the result in the discussion above if there is just one half-space. Thus, we may assume that the intersection of all but one of the half-spaces is a finitely generated $\mathbb{Q}^+$-subsemigroup C, and it suffices to show that the intersection of C with remaining half-space is finitely generated. After a change of basis, we may assume that the last half-space D is the standard example. Let $\alpha_1, \ldots, \alpha_h$ generate C, and let c_j be the last coordinate of α_j, $1 \leq j \leq h$. We may multiply each α_j by $1/|c_j|$ if $c_j \neq 0$ and so assume that every nonzero c_j is 1 or -1. Then

$$C \cap D = \{q_1\alpha_1 + \cdots + q_h\alpha_h : q_j \in \mathbb{Q}_j^+ \text{ for all } j \text{ and } \sum_{j=1}^{h} q_j c_j \geq 0\}.$$

It therefore suffices to show that

$$E = \{(q_1, \ldots, q_h) \in (\mathbb{Q}^+)^h : \sum_{j=1}^{h} q_j c_j \geq 0\}$$

is finitely generated as a $\mathbb{Q}^+$-subsemigroup, because we have a surjective map $E \twoheadrightarrow C \cap D$ sending

$$(q_1, \ldots, q_h) \mapsto q_1\alpha_1 + \cdots + q_h\alpha_h.$$

This map will carry a finite set of generators for E to a finite set of generators for $C \cap D$. We may assume that coordinates have been permuted so that we have $c_1 = \cdots = c_a = 1$, $c_{a+1} = \cdots = c_{a+b} = -1$, and the remaining c_j are 0. It is easy to verify that the e_i for $1 \leq i \leq a$, the $e_i + e_j$ for $1 \leq i \leq a$ and $a+1 \leq j \leq b$, and the e_k for $a+b+1 \leq k \leq h$ generate E over $\mathbb{Q}^+$.

Part (b) is entirely similar to the construction of the splitting $H = G \oplus H'$ except that it is much simpler in the present context, and the proof is left as an exercise.

For part (c), if some c_j is not 0, say c_h, then

$$-\alpha_h = \frac{c_1}{c_h}\alpha_1 + \cdots + \frac{c_{h-1}}{c_h}\alpha_{h-1},$$

contradicting the assumption that C has no line.

Finally, for part (d), suppose

$$-\beta = \eta - c\alpha,$$

where we may assume $c > 0$ or else $-\beta \in H$. The element η can be written as a nonnegative linear combination of α, β, and the other minimal generators, say

$$\eta = q\alpha + r\beta + \eta',$$

where η' does not involve α or β. Then

$$-\beta = q\alpha + r\beta + \eta' - c\alpha,$$

and so

$$(q-c)\alpha + (r+1)\beta + \eta' = 0.$$

If $q \geq c$ this contradicts part (c). If $q < c$, then

$$\alpha = \frac{r+1}{c-q}\beta + \frac{1}{c-q}\eta',$$

which means that α is not needed as a generator, a contradiction. $\square$

Proposition. *Let V be a finite-dimensional vector space over $\mathbb{Q}$ and let $C \subseteq V$ be a finitely generated $\mathbb{Q}^+$-subsemigroup. If C is proper, then C is contained in a half-space, i.e., there is a nonzero linear functional that is nonnegative on C. If $\alpha \in C$ and $-\alpha \notin C$ then one can choose L nonnegative on C so that $L(\alpha) > 0$. If C contains no line, one can choose L so that it is positive on all nonzero elements of C.*

Proof. We use induction on $\dim_{\mathbb{Q}}(V)$, and assume that all of the statements are true for vector spaces of smaller dimension. We may replace V by $C - C$, and so assume that C spans V. If $\dim(V) = 1$ then C is either $\{0\}$, a half-line, or all of V, and the result is trivial.

In general, we have a decomposition $C = W + C'$ where W is a vector space as in part (b) of the Lemma, and $C' \subseteq W'$, a complement for W. If $W \neq 0$ then all of the statements can now be deduced from the induction hypothesis applied to $C' \subseteq W'$: one extends the functional on W' by letting it be 0 on W. Note that if $\alpha \in C$ and $-\alpha \notin C$ then $\alpha = \beta + \alpha'$ where $\beta \in W$ and $\alpha' \in C' - \{0\}$, and has no additive inverse in C'.

This means that we can assume without loss of generality that C has no line, and we may choose minimal generators $\alpha_1, \ldots, \alpha_h$. We must have $h \geq 2$, or else $\dim_{\mathbb{Q}}(V) \leq 1$, since C spans V. It will suffice to construct a linear functional L_i that is positive on α_i and nonnegative on C for every i. The sum of these linear functionals will be positive on all of $C - \{0\}$, since every element is nonnegative linear combination of the α_i. Thus, it suffices to construct such a functional that is nonnegative on, say, α_1. Let $\alpha = \alpha_2$ and $\beta = \alpha_1$. We apply part (d) of the Lemma above, and replace C by $C_1 = C + \mathbb{Q}\alpha$. Then β does not have an inverse, but C_1 contains a line, and so we can construct a linear functional nonnegative on C_1 and positive on $\beta = \alpha_1$ by reducing to a lower-dimensional case, as in the preceding paragraph. $\square$

Theorem. *Let V be a finite-dimensional vector space over $\mathbb{Q}$. Then $C \subseteq V$ is a finitely generated $\mathbb{Q}^+$-subsemigroup if and only if C is a finite-intersection of half-spaces.*

Proof. The "if" part is part (a) of the Lemma. It remains to see that every $\mathbb{Q}^+$-subsemigroup is a finite intersection of half-spaces. Let $\alpha_1, \ldots, \alpha_h$ be a finite set of generators. The set

of linear functionals nonnegative on α_i is a half-space H_i in the dual vector space V^*, and so the intersection of the H_i is a finitely generated $\mathbb{Q}^+$-subsemigroup in V^*. Let $L_1, \ldots, L_s$ be generators. It suffices to show that C is the intersection of the half-spaces determined by the L_j. Let β be any vector not in C. It will suffice to show that there exists a linear functional that is nonnegative on C and negative on β, for this functional is a nonnegative linear combination of the L_j, and so at least one of the L_j will have the same property. Consider

$$C_1 = C + \mathbb{Q}^+(-\beta),$$

the $\mathbb{Q}^+$-subsemigroup generated by C and $-\beta$. If $\beta \in C_1$ we have

$$\beta = \alpha - c\beta$$

with $\alpha \in C$ and $c > 0$ and then

$$\beta = \frac{1}{1+c}\alpha \in C,$$

a contradiction. Since $\beta \notin C_1$, by the Proposition above there is a linear functional that is positive on $-\beta$ and nonnegative on C_1, and this has the required property. $\square$