Polynomial Rings and Group Rings for Abelian Groups

E. L. Lady

(June 16, 2009)

A lifetime or so ago, when I was teaching at the University of Kansas, Jim Brewer and I wrote a paper on group rings for finite rank torsion free abelian groups. (J.W. Brewer, D.L. Costa, and E.L. Lady, Prime ideals and localization in commutative group rings, J. Algebra 34(1975), pp. 300 - 308.) This paper was fairly popular, apparently because many people felt that it would be fairly easy to write follow-up papers to it. However I was not completely happy with it, and each time since then that I have occasion to think about it again, I am even more unhappy. Because it seems to me that we completely missed the main point and that most of the theorems could have been proved much more easily using a different approach.

(For a later paper which includes exploration of some of the ideas in our paper far more seriously than I will do here, see "Robert Gilmer's Work on Semi-group Rings" by David F. Anderson, published in the volume *Multiplicative Ideal Theory in Commutative Algebra: A Tribute to the Work of Robert Gilmer,* edited by James W. Brewer, Sarah Glaz, William J. Heinzer, and Bruce M. Olberding (Springer, 2006).)

The way I think of it recently is to see a group ring for an abelian group as simply a polynomial ring but with generalized exponents.

To start with, think of what is meant by a polynomial ring $k[X]$, where k is a base ring, most often a field. Many textbooks on algebra give a fairly rigorous set-theoretic definition of $k[X]$, but I want to think of it more informally. The ring $k[X]$ consists of linear combinations of elements of the form X^r, where r is a non-negative integer. People often refer to X as a "variable," and some books call it an "indeterminate." What this word means is, as far as I know, that X is basically... nothing! It's just a symbol. And if this is true, then what do we mean by X^r? It is also just a symbol then, but one that operates according to the familiar rules for exponents.

Now of course in algebraic geometry, and even more so in differential geometry and complex analysis, this is not the way people actually think of X^r. There X^r is a function and X is a variable in the sense of calculus. I.e. X is something that takes on a value, and this value varies. For a contemporary mathematician, it's taboo to actually say this, because it's contrary to the prevailing orthodoxy that all mathematics consists of constructions in set theory. Nonetheless, this is the way we all think (as far as I know), and I need to mention it because this way of thinking gets in the way (at least it gets in *my* way) when we begin to develop a generalization of polynomials.

But more to the point, in the expression X^r what is r? It is a non-negative integer, of course. And for us in this context, the important thing about the set of non-negative integers is that they can be added (subject, of course, to the usual rules).

Now there are other possible exponents besides non-negative integers. It is certainly permissible to consider the possibility that r can also be negative, and this presents no challenge to us. And it also works to allow r to be any rational number. Certainly we are familiar with $X^{\frac{1}{2}}$. In calculus and related subjects, $X^{\frac{1}{2}}$ denotes $\sqrt{X}$. In abstract algebra, this doesn't work so well, because it is not always very clear what we mean by $\sqrt{X}$. So we need to forget that and think of X^r as being just a symbol, which may or may not have an intuitive meaning, depending on the context. For us algebraists, that's not the point.

However algebra, especially the parts of commutative ring theory related to algebraic geometry, does offer us another way of understanding X and even $X^{1/r}$ on a somewhat intuitive level, at least in the case when the base ring k is a field. Namely, we can treat X as an element in some field extension of k which is transcendental over k. And it turns out that this is in fact something that we need to do in at least a part of our investigation of the group ring for a finite-rank torsion free abelian group.

Beyond this, though, what we now need do is admit the possibility of monomials of the form X^g, where g is an element of a fixed additive (and commutative) semi-group G. Understanding such monomials on an intuitive basis is now quite a challenge, especially if g is a torsion element of G. Fortunately, interpreting X^g as a purely formal entity usually does not usually pose a serious problem, and it is in fact the way that Brewer and I thought while writing our original paper. . Taking the set of all generalized polynomials based on these monomials, we get the semi-group ring $k[G]$, a typical element of which looks like $c_1X^{g_1} + \cdots + c_kX^{g_k}$, with the c_i being elements ofthe base ring k. In the case of greatest interest, G will actually be an abelian group.

This notation for elements of a group ring $k[G]$ for an abelian group G is due to Northcott, and Brewer and I used it in our paper. But we were stupid enough not to notice the real insight hidden in this notation: namely that group rings are actually not very different from polynomial rings; it's just a matter of using a different sort of exponents. And thus it should be very easy to address the question of which standard theorems for polynomial rings also work for group rings of abelian groups. It should have been easy, but for us it wasn't.

Brewer and I were specifically interested in the case where G is a finite-rank torsion free abelian group. And such a group, as I was well aware, can be thought of as simply a subgroup of Q^n, where Q is the group of rational numbers and n is a positive integer. For practical purposes, in most cases n will be the rank of G. Thus an element of G has the form $g = (r_1, ..., r_n)$ where the r_i are rational numbers. If we now introduce new variables $X_1, ..., X_n$, then we get a simple isomorphism between $k[G]$ and a ring containing $k[X_1, .., X_n]$ by mapping the monomial X^g to $X_1^{r_1}, ..., X_n^{r_n}$. Thus $k[G]$ is more or less a polynomial ring in n variables, except that negative exponents are allowed, and some exponents may also be fractional. (In fact, this must be the case in order to get anything at all interesting.)

In order for an example to be interesting, there must be at least some elements in G with denominators. In most cases, there will be elements having denominators divisible by arbitrarily high powers of some prime, or perhaps divisible by arbitrarily many primes chosen from a designated set.

Actually, saying that $k[G]$ is a polynomial ring in n variables is slightly simplistic, even allowing the possibility that some exponents may be fractional. An example may by enlightening. We might let G be the subgroup of Q^2 (where Q is the group of rational numbers) generated by all elements $(1/3^k,\, 0)$, $(0, 1/5^k)$, and $(1/11^k,\, 1/11^k)$, with $k = 0,\, 1,\, 2,\, \ldots$. The corresponding group ring $k[G]$ would consist of all linear combinations of the "monomials" $X_1^{1/3^k}$, $X_2^{1/5^k}$, and $X_1^{1/11^k} X_2^{1/11^k}$, $k = 0,\, 1,\, 2, \ldots$. (It is essential here that in the third set of monomials, the exponents on X_1 and X_2 be equal.

There do exist interesting torsion-free abelian groups G, however, such that no element has an unbounded set of denominators of the sort shown above. The most well known example is the Pontryagin group, which must at this point be about a hundred years old. But to give more detail would take us into the realm of abelian group theory rather than commutative ring theory. The main point is that the difference between $k[G]$ and $k[X_1, ..., X_n]$ is not just a matter of allowing a few denominators in the exponents.

The fact that $k[G]$ is only a slight variation of the polynomial ring in n variables over k in and of itself doesn't actually prove any theorems. But consider that G will always contain a free subgroup F of rank n, and the ring $k[F]$ will be isomorphic to the polynomial ring $k[X_1, ..., X_n]$, except that negative exponents are allowed, so that $k[F]$ is the localization of $k[X_1, ..., X_n]$ with respect to the multiplicative set consisting of all products of powers of the variables X_i. (The fact that $k[F]$ involves this localization seemed at the time to have no real importance. In fact though, I now see that it plays a crucial role in the development.) We may choose F so that all elements of Q^n with integer coefficients are contained in F, and thus for every element g in G, then is a positive integer r so that $rg \in F$. And thus $(X^g)^r \in k[F]$. Thus $k[G]$ is an integral extension of $k[F]$, and the latter is just a localization of an ordinary polynomial ring.

It then follows immediately that the Krull dimension of $k[G]$ equals the rank of G, and that $k[G]$ satisfies many properties which are known to be true for polynomial rings, such as the saturated chain condition for prime ideals. The proofs that Brewer and I originally gave for these results were considerably more cumbersome.

$k[G]$ Is (Usually) Locally Noetherian.

Brewer was especially interested in the fact that although the group ring $k[G]$ is not noetherian (except in the uninteresting case where G is finitely generated), its localization at at least some prime ideals will be noetherian (at least in characteristic 0). Brewer told me that examples of rings which are not noetherian but have noetherian localizations are fairly rare. Or at least that was the case at the time when we were writing the paper.

It seems to me now though that the same mechanism at work in these group rings can be used much more generally. So it seems worthwhile to give the essential idea of the proof that this is the case for $k[G]$, with full details for the case where rank $G = 1$

Making a change of coordinates, one can see that there is no loss of generality in supposing that G contains a free group F which contains a basis for the divisible hull of G (i.e. the vector space over the rationals generated by G).

For a moment, though, by way of contrast, let us consider the *semi*-group ring consisting of all monomials X^s, where s is a positive rational number from some additive semi-group $S \subseteq Q$. By making a change of coordinates, we may also assume that S contains the set of positive integers. It then follows that S is generated by elements of the form $\frac{1}{m}$, for various positive integers m. (If t/m is an element of S, written in lowest terms, then t has an inverse u modulo m, and thus $\frac{tu}{m} = \frac{1}{m} + k$, where k is an integer.)

For the ring to be at all interesting, S should be infinite. In this case, we can see clearly that the ideal $\mathfrak{P}$ generated in the semi-group ring by all elements $X^{1/m}$ for $\frac{1}{m} \in S$ is not finitely generated and that the localized ring $R_{\mathfrak{P}}$ is not noetherian.

For the *group* ring $k[G]$, on the other hand, things will be less obvious, because in the group ring the requirement to include negative exponents means that these elements X^g for $g \in G$. are all invertible, so the corresponding ideal is the whole ring. The distinction between the group ring and semi-group ring turns out to have more significance than one might expect.

In the case of the *group* ring $k[G]$, we need only look at “augmentation ideal” $\mathfrak{P}$, i.e. the set of elements of the form $X^g - 1$, for all $g \in G$. This is the kernal of the ring morphism

$k[G] \to k$ determined by mapping all elements X^g to 1, and thus is a prime ideal (in fact maximal if k is a field) and can be quickly seen to be not finitely generated unless G is a finitely generated group. (There is a homomorphism from G onto $\mathfrak{P}/\mathfrak{P}^2$ mapping $g \in G$ to the image of $X^g - 1$.)

Accepting the convention that G consists of vectors of rational numbers, for given $g \in G$, let m be a common multiple of the denominators occuring in g. Writing for convenience, $X_1^g = Y$, then $Y^m = X_1^{mg} \in S^{-1}k[X_1, \cdots, X_n]$, where n is the rank of G. and S is multiplicative set generated by the variables $X_1, \ldots, X_n$, used to cover the possibility that some exponents may be negative. (Or if one prefers the group-theoretic notation, then there exists a positive integer m such that $mg \in F$ and $Y^m \in k[F] \approx S^{-1}k[X_1, \ldots, X_n]$.)

From this point on we need to assume that the characteristic of k is 0, or at least not p for any prime number p such that $pG_1 = G_1$ for some non-trivial subgroup of G. Now

$$Y^m - 1 = (Y-1)(Y^{m-1} + \cdots + Y + 1) \in S^{-1}k[X_1, \ldots, X_n].$$

But the expression in the second parenthesis does not belong to $\mathfrak{P}$, as can be seen by substituting $Y = X^g = 1$, and hence it is invertible in the localized ring $k[G]_{\mathfrak{P}}$. Thus in the localized ring, $Y - 1$ is a multiple of the polynomial $Y^m - 1 \in k[X_1, \ldots, X_n]$, and the latter is of course a noetherian ring. Thus $\mathfrak{P}k[G]_{\mathfrak{P}}$ is finitely generated when $\mathfrak{P}$ is the augmentation ideal.

And in the case where G has rank 1, it turns out, rather astonishingly, that that the localized augmentation ideal $\mathfrak{P}k[G]_{\mathfrak{P}}$ is principal, generated by $X_1 - 1$.

Now let's look at the general principle here in the case that $\mathfrak{P}$ is any prime ideal in the group ring $k[G]$ for a rank-one group G.

What we will see can be applied in quite general situations to get rings whose localizations at prime ideals are all noetherian.

Setting aside the specific computations here, consider prime element f in a principal ideal domain R (the ring $k[X]$ in our example), and consider a finite integral extension R' of R. R' will be a dedekind domain, and just to keep the example clean, we will assume that it is a principal ideal domain, although this is only a minor simplification. In R', $f = f_1 \cdots f_r$, where the f_i are prime elements in R'. Now the crucial issue here turns out to be whether the f_i are all distinct, or whether there are repetitions. In the latter case, classical dedekind domain language says that the prime ideal generated by f in R "ramifies" in the ring extension. It is known that ramification is rare, and occurs only when f is belongs to the discriminant ideal of the field extension.

In the example where $R = k[X]$ and R' is a semi-group ring $k[S]$ for some finite semi-group $S \subseteq Q$, given the assumption that the characteristic of k is not a prime p such that S is p-divisible, what one sees is that the only prime polynomial in R which ramifies is X. (In fact, for any m, $X = Y^m$, where $Y = X^{1/m}$ for some $\frac{1}{m} \in S$.)

But for group rings $k[G]$, we see that no ramification can occur. I am skipping past some standard theory involving the discriminant here. The reader can take my claim on faith, or else consult texts on commutative ring theory such as Zariski-Samuels or Bourbaki, among others.

Or one can simply skip the ramification theory altogether, and notice that with the assumption that the characteristic of k is 0 or a prime p for which G is not p-divisible, the fact that all the irreducible factors in the factorization $f = f_1 \cdots f_r$ have multiplicity 1 can be seen simply from the standard results on separable polynomials in the theory of field extensions. (A minor adjustment needs to be made for the fact that the "polynomial" f in our example involves fractional exponents rather than the usual positive-integer exponents.)

(The reason we need the assumption on the characteristic is that if k has characteristic p and G contains elements $g_k = 1/p^k$ for all k, then $1 - X = (1 - X^{g_k})^{p^k}$, so we have ramification for the augmentation ideal. The augmentation ideal is in fact not locally finitely generated in this case.)

What we gain by excluding ramification is the opportunity to apply the following extremely simple lemma.

Lemma. Let f be a prime element in a principal ideal domain R. Let R' be a ring containing R and let $\mathfrak{P}'$ be a prime ideal in R' containing f. If f factors into distinct prime factors in R', then f generates the localized ideal $\mathfrak{P}'R'_{\mathfrak{P}'}$.

PROOF: Suppose that the prime element $f \in R$ factors in R' as $f = f_1 \cdots f_r$, where the f_i are distinct prime elements in R'. The prime ideal $\mathfrak{P}'$ in R' must contain one of the f_i, say f_1, and cannot contain two of them, since they are relatively prime elements. Thus all but one of the f_i become invertible in $R'_{\mathfrak{P}'}$. So we see that f and f_1 are multiples of each other in $R'_{\mathfrak{P}'}$. In particular, f is a prime element in $R'_{\mathfrak{P}'}$. Since $R'_{\mathfrak{P}'}$ is a principal ideal domain and $f \in \mathfrak{P}'R'_{\mathfrak{P}'}$, we see that $\mathfrak{P}'R'_{\mathfrak{P}'}$ is generated by f. $\boxed{\checkmark}$

Now let's see how this applies to a group ring $k[G]$.

For convenience (mine!), we will look only at the case where the rank of G is 1. Thus we may assume that G is a subgroup of the group Q of all rational numbers. We need to assume that and k is a field of characteristic 0 or characteristic p such that G is not p-divisible. We let F be a subgroup of G isomorphic to the integers, and in the paragraphs above we take $R = k[F]$, which is a principal ideal domain. Let $\mathfrak{P}$ be a prime ideal in $k[G]$.

What we would like to do is to apply the lemma above with $R' = k[G]$. Unfortunately, this won't work because $k[G]$ is an infinite dimensional extension of R and is not noetherian and elements in $k[G]$ don't always factor into a finite product of primes.

But consider a prime ideal $\mathfrak{P}$ in $k[G]$. Then $\mathfrak{P} \cap k[F]$ is a principal prime ideal in $k[F]$, generated by an irreducible element which we will call f. We claim that f generates $\mathfrak{P}k[G]_{\mathfrak{P}}$. Now an element in $f_1 \in \mathfrak{P}$ is a linear combination elements X^g for finitely many $g \in G$, and thus belongs to $\mathfrak{P} \cap k[F_1]$ for some finitely generated subgroup F_1 of G. By the Lemma, $\mathfrak{P} \cap k[F_1]$ is generated by f so that f_1 is a multiple of f. Since this is true for every $f_1 \in \mathfrak{P}$, we see that f generates $\mathfrak{P}$.

Thus in this case of a rank-one group G, not only is the localization of $k[G]$ at every prime ideal noetherian, but the localized prime ideals are all principal.

As far as I can recall, the proof when G has rank larger than 1 follows the same general lines. But for specific details, I have to refer readers to the original paper.