

Notes on group-rings and polynomials

Let M be a semigroup (that is M has an operation that is associative and has an identity) and R be a commutative ring. We define $R[M]$ to be the set of functions $f : M \rightarrow R$ such that $\{m \in M \mid f(m) \neq 0\}$ is finite. We represent such a function also as a formal sum

$$\sum_{m \in M} f(m)m \quad (*)$$

and we will define a ring structure on $R[M]$ that will allow us to give sense to (*) and also allow us to manipulate this formula using the distributivity law. So define $(f + g)(m) = f(m) + g(m)$ and

$$(fg)(m) = \sum_{a,b \in M, ab=m} f(a)g(b).$$

Problem 1. *Prove that these actually define operations on $R[M]$ which make it into a ring.*

$R[M]$ with these operations is called the semigroup-ring of M with coefficients in R . If M is a group it is simply called the group-ring.

Problem 2. *If we identify $m \in M$ with the function $M \rightarrow R$ that sends m to 1 and all other elements of M to 0 and we identify $r \in R$ with the function $M \rightarrow R$ that sends e (the identity on M) to r and all other elements of M to 0 prove that any $f \in R[M]$ is equal to its representation (*).*

Let now X be an arbitrary set, M_X the free semigroup on X , F_X the free group on X , $A_X = \langle X \mid [x, y], x, y \in X \rangle$ the free abelian group on X . Then we have a map $F_X \rightarrow A_X$ and we define A_X^+ to be the image of M_X in A_X , and call it the free abelian semigroup on X . Finally we define $R[X] = R[A_X^+]$ (yes the notation is ambiguous but it should be clear from the context). $R[X]$ defined this way is called the polynomial ring on variables X and coefficients in R .

Problem 3. *Prove that if X is a set of one element that $R[X]$ is the usual polynomial ring in one variable and coefficients in R .*

Problem 4. *Prove that if G is the cyclic group in n elements then the group ring $R[G]$ is isomorphic to $R[x]/(x^n - 1)$, where $R[x]$ is the usual polynomial ring in one variable and coefficients in R .*

The brave among you may wish to explore the definition of power series, where we drop the condition that the number of non-zero coefficients is finite. The trick to assure that the sum defining the coefficient of a product is finite, hence makes sense, is to deal only with well-ordered semigroups.