# Math 594. Lemmas for the symmetric function theorem

We wish to prove two lemmas that came up in the proof of the symmetric function theorem. Here is the first lemma, which came up near the end of the proof.

**Lemma 0.1.** *Let $K$ be an infinite field. If $f \in K[T_1, \dots, T_n]$ satisfies $f(t_1, \dots, t_n) = 0$ for all $n$-tuples $(t_1, \dots, t_n) \in K^n$, then $f = 0$.*

Of course, this lemma is always false for finite $K$ by taking $f = T_1^q - T_1$, where $q$ is the size of $K$.

*Proof.* For $n = 1$, the assertion is that a nonzero polynomial in $K[T]$ cannot vanish as a function on $K$. But $K$ is infinite and a nonzero polynomial over a field cannot have more roots than its degree. Thus, the case $n = 1$ is true. In general, we may assume $n > 1$ and by induction we can assume the result is known for $n - 1$. We use the isomorphism

$$K[T_1, \dots, T_{n-1}][T_n] \simeq K[T_1, \dots, T_n]$$

to write $f = \sum a_j T_n^j$ where $a_j \in K[T_1, \dots, T_{n-1}]$. Fix $t_1, \dots, t_{n-1} \in K$ and let $g = \sum a_j(t_1, \dots, t_{n-1}) T_n^j \in K[T]$. For any $t \in K$ we have $g(t) = f(t_1, \dots, t_{n-1}, t) = 0$, so by the one-variable case $g = 0$. Hence, its coefficients $a_j(t_1, \dots, t_{n-1}) \in K$ must all vanish. This holds for any $(n-1)$-tuple of $t_j$'s in $K$, so by the inductive hypothesis we get $a_j = 0$ in $K[T_1, \dots, T_{n-1}]$ for all $j$. Hence, $f = \sum a_j T_n^j = 0$ in $K[T_1, \dots, T_n]$. ∎

The more non-trivial lemma which arose in the proof of the symmetric function theorem is:

**Lemma 0.2.** *Let $F/K$ be an extension of fields. Let $R$ be a subring of $K$. If $a, b \in F$ each satisfy monic polynomial equations with coefficients in $R$, then so do $a + b$ and $ab$.*

Before we prove the lemma, we emphasize that the case $R = K$ is the old assertion that sums and products of algebraic elements over a ground field are again algebraic over the ground field. This was proven by using $K$-dimension of vector spaces, and more specifically the theory of linear algebra over $K$. When working over $R$, one does not have as simple a theory of "vector spaces" (really, modules) over $R$, and hence the old arguments do not trivially carry over to handle assertions involving monic polynomials with $R$ coefficients. The general word used to describe the relation of interest in the lemma is:

**Definition 0.3.** Let $R \to S$ be an extension of commutative rings. We say $s \in S$ is *integral* over $R$ if $s$ satisfies a monic polynomial $f(s) = 0$ where $f \in R[T]$.

The key in this definition is the monicity of $f$. Of course, if $R$ is a field then monicity is not a serious constraint, since a nonzero leading coefficient in a field is a unit and hence may be scaled away by multiplying through by its recirpocal. But in more general rings $R$ not every nonzero polynomial has a unit leading coefficient. It turns out that integrality is the correct notion which generalizes the field-theoretic concept of algebraicity in the study of general commutative rings. For example, $x = (-1+\sqrt{-3})/2$ satisfies $x^2+x+1 = 0$, so it is *integral* over $\mathbf{Z}$, whereas $3/2 \in \mathbf{Q}$ is *not* integral over $\mathbf{Z}$ (as one sees by using the rational root theorem).

The lemma of interest above is a special case of the following (applied to $R \to F$ in the lemma):

**Theorem 0.4.** *Let $R \hookrightarrow S$ be an extension of commutative rings. If $s, s' \in S$ are integral over $R$, then so are $s + s'$ and $ss'$.*

The proof yields some pretty enormous polynomial relations for $s+s'$ and $ss'$ (via monstrous determinants). There is no simple way to "see" these relations just given ones for $s$ and $s'$, as the proof will make clear. This is why the theorem is not obvious.

*Proof.* Let $R' = R[s, s']$ be the $R$-subalgebra of $S$ generated by $s$ and $s'$. That is, $R'$ is the subset of finite sums $\sum r_{ij} s^i s'^j$ with $r_{ij} \in R$. It is easy to check that $R'$ is a subring of $S$ (i.e., stable under addition and multiplication) and also contains $R$. Concretely, $R'$ is the image of the $R$-algebra map $R[X, Y] \to S$ determined by $X \mapsto s$, $Y \mapsto s'$. Note also that $s + s', ss' \in R'$. Thus, we lose no generality by replacing $S$ with $R'$.

The key point of monicity is that since we have relations

$$s^n = r_{n-1} s^{n-1} + \dots + r_0, \;\; s'^m = r'_{m-1} s'^{m-1} + \dots + r'_0$$

with $r_i, r'_j \in R$, we can recursively feed such relations back into themselves to see that for any $e > n$ (resp. $e' > m$), $s^e$ (resp. ${s'}^{e'}$) can be expressed as an $R$-linear combination of $1, s, \dots, s^{n-1}$ (resp. $1, s', \dots, {s'}^{m-1}$). In other words, $S = R[s, s']$ is spanned over $R$ by the *finitely many* monomials $s^i {s'}^j$ with $i < n$ and $j < m$. Hence, $S$ is *finite* over $R$ in the sense that all elements of $S$ may be expressed as $R$-linear combinations on a fixed *finite* set of elements. We will use this condition to prove that *all* elements of $S$ (in particular, the elements $s + s'$ and $ss'$) are integral over $R$. If $R$ were a field, we could say that $S$ is a finite-dimensional $R$-vector space, and this was the key to using linear algebra in our earlier proofs that sums and products of quantities algebraic over a field are again algebraic over that field (ultimately using that a subspace of a finite-dimensional vector space is finite-dimensional). But since $R$ is not a field, we do not have linear algebra available and so must proceed differently.

The general result we aim to prove is the following: if $R \to S$ is an extension of rings and $S$ is *finite* over $R$ (in the sense that there exist $s_1, \dots, s_N \in S$ such that all elements of $S$ can be written as $\sum r_i s_i$ with $r_i \in R$), then every $s \in S$ is integral over $R$. Let's write $ss_i = \sum_{j=1}^N r_{ij} s_j$ for (not necessarily unique!) $r_{ij} \in R$. Let $M = (r_{ij})$. This is an $N \times N$ matrix. The Cayley-Hamilton theorem asserts that any square matrix $A = (a_{ij})$ over a field satisfies its characteristic polynomial; that is, $\sum c_j A^j$ is the zero matrix if $\sum c_j T^j$ is the characteristic polynomial of $A$. In fact, this identity applies to a square matrix over any commutative ring whatsoever. Indeed, since there is a ring map $\mathbf{Z}[X_{ij}] \to R$ satisfying $X_{ij} \mapsto r_{ij}$, the validity of the "Cayley-Hamilton" identity for $(r_{ij})$ as a matrix over $R$ would follows from the corresponding identity for the "universal matrix" $(X_{ij})$ over the ring $\mathbf{Z}[X_{ij}]$, but this latter ring is a *domain* and hence Cayley-Hamilton identities over this ring may be checked by working in its fraction field (where the old linear algebra results apply!).

If we let $P_M = \det(T \cdot \mathrm{id} - M) = \sum \rho_j T^j \in R[T]$ denote the *monic* characteristic polynomial of the matrix $M = (r_{ij})$ (with determinants over a commutative ring defined in the evident manner), then Cayley-Hamilton as discussed above says $\sum \rho_j M^j = 0$ in $\mathrm{Mat}_{N \times N}(R)$. From the definition of the $r_{ij}$'s, we have

$$\begin{pmatrix} ss_1 \\ \vdots \\ ss_n \end{pmatrix} = M \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix},$$

from which it readily follows by induction (check!) that

$$\begin{pmatrix} s^j s_1 \\ \vdots \\ s^j s_n \end{pmatrix} = M^j \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$$

for all $j \geq 0$. Thus, adding up such identities with $\rho_j$ multipliers thrown in yields

$$\begin{pmatrix} (\sum \rho_j s^j) s_1 \\ \vdots \\ (\sum \rho_j s^j) s_n \end{pmatrix} = P_M(M) \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

since $P_M(M)$ is the zero matrix (by Cayley-Hamilton). Entry-wise, this says $P_M(s) s_j = 0$ in $R$ for all $j$. But *every* element $\sigma \in S$ is an $R$-linear combination $\sigma = \sum r_j s_j$, so $P_M(s) \cdot \sigma = \sum r_j P_M(s) s_j = \sum r_j \cdot 0 = 0$. Taking $\sigma = 1 \in S$, we get $0 = P_M(s) \cdot 1 = P_M(s)$. Hence, $P_M \in R[T]$ is a *monic* polynomial for which $P_M(s) = 0$ (recall that $M$ "came" from $s$ in the sense that the entries $r_{ij}$ of $M$ were provided by describing how multiplication by $s$ looks in terms of the choice of elements $s_j \in S$ which $R$-linearly span $S$). ■