Fundamental theorem of symmetric polynomials

math center

Let k be a field, and let $K = k(X_1, X_2, \cdots, X_n)$ be the field of rational functions in n variables. S_n naturally acts on K by permuting the indeterminates. We then view S_n as a subset of $\mathrm{Aut}(K)$.

Lemma 0.1. The extension $K|K^{S_n}$ is Galois.

Proof. This extension is the splitting field of the polynomial

$$f(X) = (X - X_1)(X - X_2)\cdots(X - X_n) \in K^{S_n}[X], \tag{1}$$

which clearly has no repeated roots. □

We could easily check that $S_n = \mathrm{Gal}(K|K^{S_n})$. But for an obvious generalization of this, we actually need to take a slightly tricky path.

Theorem 0.2. Let K be a field and let $G \leq \mathrm{Aut}(K)$ be a finite subgroup. Then $K|K^G$ is Galois, and $\mathrm{Gal}(K|K^G) = G$.

Proof. Mimicking (1), for every $x \in K$, we wish to write

$$g_x(X) \stackrel{?}{=} \prod_{h \in G} (X - h(x)) \in (K[X])^G = K^G[X].$$

But this doesn't work, because $g_x(X)$ might has repeated roots. The correct solution is to use the G-orbit of x:

$$g_x(X) = \prod_{y \in Gx} (X - y) \in (K[X])^G = K^G[X].$$

This time, we see that any simple subextension $K^G(x)|K^G$ is the splitting field of $g_x(X)$, and thus is Galois. We have an upper bound $[K^G(x) : K^G] \leq |G|$. Clearly, every finite subextension of $K|K^G$ is separable, so the primitive element theorem always applies. Combining with the above, we see that every finite subextension has degree $\leq |G|$. This means that $K|K^G$ is itself finite (hence Galois), and $[K : K^G] = |\mathrm{Gal}(K|K^G)| \leq |G|$. As $G \subset \mathrm{Gal}(K|K^G)$, the result follows. □

The coeffients of f are called the *elementary symmetric polynomials* in $X_1, X_2, \cdots, X_n$, and are denoted by $\sigma_1, \sigma_2, \cdots, \sigma_n$, the subscripts indicating their degree. We should be aware of what this means:

Proposition 0.3. K^{S_n} is generated by the elementary symmetric polynomials $\sigma_1, \sigma_2, \cdots, \sigma_n$.

Proof. Let $L = k(\sigma_1, \sigma_2, \cdots, \sigma_n) \subset K^{S_n}$. Then K is the splitting field of $f(X)$ over L as well. We obtain a bound

$$[K : K^{S_n}] \leq [K : L] \leq n!.$$

By Theorem 0.2, $[K : K^{S_n}] = |S_n| = n!$. Therefore $L = K^{S_n}$. □

Recall that an integral domain R is *integrally closed* if any element of the field $\mathrm{Frac}(R)$ which is a root of a monic polynomial in $R[X]$ must lie in R.

Lemma 0.4. Let $R = k[X_1, X_2, \cdots, X_n]$ be the polynomial ring. Then R is integrally closed.

Proof. Brings back the bittersweet middle school memories! □

Remark 0.5. For the same reason, any GCD domain is integrally closed. The lemma is a special case of this.

Theorem 0.6 (Fundamental theorem of symmetric polynomials)**.** We have an equation of subalgebras of L and K^{S_n}:

$$k[\sigma_1, \sigma_2, \cdots, \sigma_n] = K^{S_n} \cap k[X_1, X_2, \cdots, X_n].$$

Proof. Since $n = \mathrm{tr.deg}(K|k) = \mathrm{tr.deg}(K^{S_n}|k)$, the n generators $\sigma_1, \sigma_2, \cdots, \sigma_n$ of K^{S_n} must be algebraically independent. Therefore $R := k[\sigma_1, \sigma_2, \cdots, \sigma_n]$ is a polynomial ring, with K^{S_n} as its field of fraction. By (1), the X_i's are integral over R. It follows that $k[X_1, X_2, \cdots, X_n]$ is integral over R for it's a commutative ring. This completes the proof. □

The End

Final remark: I don't know any commutative algebra. Very inconvenient.

Compiled on 2025/07/15.
Home page