Some review of Galois theory

Dedekind's lemma (Bourbaki's Algebra; French version; Ch V, p.27, Cor 2)

The set Maps(G,K), where G is a gp & K a field, of all maps from G to K is a vector space over K (pointwise addition & scalar multiplication). Any set of maps from G to $K^\times$ is naturally considered as a subset of Maps(G,K). With this understanding, any set of distinct gp hom from G to $K^\times$ is K-linearly independent.

COROLLARY $E \subseteq F$ field extension. Then $\mathrm{Gal}(F|E) \leq [F:E]$.

Proof: $\mathrm{Gal}(F|E) \subseteq \mathrm{Hom}_{Gps}(F^\times, F^\times)$ and so elts of $\mathrm{Gal}(F|E)$ are F-linearly independent in Maps$(F^\times, F)$. ~~But~~ Now, the space $\mathrm{Hom}_E(F,F)$ of E-endomorphisms of the E-vector space F is a linear F-subspace of dimension $[F:E]$ of the ~~E~~ F-vector space Maps$(F^\times,F)$ & $\mathrm{Gal}(F|E) \subseteq \mathrm{Hom}_E(F,F)$. ∎

Artin's lemma (Bourbaki's Algebra; French version; Ch V. p.63)

Γ a gp of field automorphisms of a field K. Let V be a f.d. K^Γ-subspace of K. Any K^Γ-linear map from V to K is a K-linear combination of the restrictions of elements of Γ to V.

COROLLARY: G finite group of automorphisms of a field K. $K^G \subseteq K$ normal separable extension. $[K:K^G] = |G|$ & $\mathrm{Gal}(K|K^G) = G$.

EASY PROBLEM: Suppose M is a f.g. module, and $\{m_\alpha\}_{\alpha\in I}$ be a set of generators of M. Then there exists a finite subset J of I such that $\{m_\alpha\}_{\alpha\in J}$ generates M.

EXERCISE: For indeterminates $x_1,\dots,x_n$, prove $\boxed{n!\,x_1\cdots x_n = (-1)^n \sum_{I\subseteq\{1,\dots,n\}} (-1)^{|I|}\left(\sum_{i\in I} x_i\right)^n}$

THEOREM: $G=\mathfrak{S}_n$ symmetric group, acting as permutations on a basis $v_1,\dots,v_n$ of V. If $x_1,\dots,x_n$ is the dual basis of V^*, then $K[V]^G = K[x_1,\dots,x_n]^G = K[e_1,\dots,e_n]$, where $e_1,\dots,e_n$ are the elementary symmetric functions.

Proof: First show $K(e_1,\dots,e_n)\subseteq K(x_1,\dots,x_n)$ is Galois. This is so because the larger field is the splitting field of the separable polynomial $(t-x_1)\cdots(t-x_n) = \sum(-1)^i e_i t^{n-i}$. This last equation also shows that $K[e_1,\dots,e_n]\subseteq K[x_1,\dots,x_n]$ is integral. Any $K(e_1,\dots,e_n)$-automorphism of $K(x_1,\dots,x_n)$ must permute the x_i, so $\mathrm{Gal}(K(x_1,\dots,x_n)\mid K(e_1,\dots,e_n)) = \mathfrak{S}_n$ and $K(x_1,\dots,x_n)^{\mathfrak{S}_n} = K(e_1,\dots,e_n)$. Now we have:

$$\begin{tikzcd}
K[e_1,\dots,e_n] \arrow[r, phantom, "\subseteq"] \arrow[d, dash, "q.f."] & K[x_1,\dots,x_n]^{\mathfrak{S}_n} \arrow[rr, hook] \arrow[d, dash, "q.f.\ (\text{see problem below})"] & & K[x_1,\dots,x_n] \arrow[d, phantom, "\cap\ q.f."] \\
K(e_1,\dots,e_n) \arrow[r, dash] & K(e_1,\dots,e_n) = K(x_1,\dots,x_n)^{\mathfrak{S}_n} \arrow[rr, dash] & & K(x_1,\dots,x_n)
\end{tikzcd}$$

Since $K[e_1,\dots,e_n]\subseteq K[x_1,\dots,x_n]^{\mathfrak{S}_n}$ is integral and $K[e_1,\dots,e_n]$ is integrally closed (in its q.f.), we conclude that $K[e_1,\dots,e_n] = K[x_1,\dots,x_n]^{\mathfrak{S}_n}$. QED

EXERCISE: R domain, G finite $\circlearrowright R$ by ring auts. $K=$ q.f. of R. Then G acts on K by field auts, and K^G is the q.f. of R^G.