Mathematics 4340

Root adjunction

Ken Brown, Cornell University, March 2009

All rings in this handout are assumed to be commutative. Recall that if $R \leq S$ and α is an element of S, then we can adjoin α to R to obtain a ring $R[\alpha] \leq S$ containing R and α. If α satisfies an equation $f(\alpha) = 0$ where $f \in R[x]$ is a monic polynomial of degree n, then every element of $R[\alpha]$ can be expressed in the form

$$\sum_{0 \leq i < n} r_i \alpha^i$$

with $r_i \in R$. [The equation $f(\alpha) = 0$ allows one to express α^n in this form, and higher powers can be obtained by repeatedly multiplying by α.] A familiar example is $\mathbb{C} = \mathbb{R}[i]$, in which $n = 2$ and $f(x) = x^2 + 1$.

But what if we just start with R and f, with no bigger ring S under discussion. It turns out that there is a universal way of adjoining to R a root α of f, thereby obtaining the "largest possible" instance of $R[\alpha]$. Intuitively, this universal $R[\alpha]$ is generated by R and α, subject to the relation $f(\alpha) = 0$. Nothing should be true about this ring other than what's forced by the axioms of ring theory and the given relation. Note the analogy here with groups defined by generators and relations.

Proposition. *Let R be a ring and $f \in R[x]$ a monic polynomial of degree $n > 0$. There is a ring $R[\alpha] \geq R$ containing an element α with the following properties:*

(1) $f(\alpha) = 0$.

(2) Every element of $R[\alpha]$ is uniquely expressible in the form

$$\sum_{0 \leq i < n} r_i \alpha^i$$

with $r_i \in R$.

(3) Given any ring $S \geq R$ and any element $\beta \in S$ such that $f(\beta) = 0$, there is a unique homomorphism $\phi\colon R[\alpha] \to S$ such that ϕ is the identity on R and $\phi(\alpha) = \beta$.

Thus every ring obtained from R by adjoining a root of f is a quotient of this universal $R[\alpha]$.

Example. Let $R = \mathbb{R}$ and let $f(x) = x^3 - 1$. Then the universal $\mathbb{R}[\alpha]$ is a 3-dimensional $\mathbb{R}$-algebra with a vector-space basis $1, \alpha, \alpha^2$. The multiplication table is completely determined by the equation $\alpha^3 = 1$. (This implies $\alpha^4 = \alpha$, and there is no need to consider higher powers of α.) On the other hand, since f has three roots $\beta \in \mathbb{C}$ (one of which is in $\mathbb{R}$), we can form subrings $\mathbb{R}[\beta] \leq \mathbb{C}$ in three different ways. One of these is $\mathbb{R}$, and the other two are $\mathbb{C}$. The UMP in (3) therefore gives us three $\mathbb{R}$-algebra surjections

$$R[\alpha] \twoheadrightarrow \mathbb{R}, \quad R[\alpha] \twoheadrightarrow \mathbb{C}, \quad R[\alpha] \twoheadrightarrow \mathbb{C},$$

each taking α to one of the cube roots of unity in $\mathbb{C}$. The second and third maps are complex conjugates of one another.

You'll see further examples in class and in the homework.

Proof of the proposition. This is analogous to the theory of group presentations, in which we start with a free group and form a quotient to force the relations to hold. Here we start by "freely" adjoining an element to R, i.e., we form the polynomial ring $R[x]$. Let I be the ideal $\langle f \rangle$ generated by f, and consider the quotient ring $S := R[x]/I$. Let α be the image of x in S. The quotient map $R[x] \twoheadrightarrow S$ is injective on R, since no nonzero constant polynomial can be divisible by f. So we may identify R with its image and view R as a subring of S. We will show that S is the desired $R[\alpha]$.

By construction, $f(\alpha) = 0$ and every element of S can be written in the form $\sum_i r_i \alpha^i$; moreover, we can take this expression to have degree less than n as in the first paragraph of this handout. To see that the expression is then unique, it suffices to show that $g(\alpha) \neq 0$ in S if $g \in R[x]$ is nonzero and has degree less than n. But this is the same as saying that $g \notin I$, i.e., that g is not divisible by f, which is obvious. Thus S and α satisfy (1) and(2). Finally, (3) is obtained by combining the UMP for $R[x]$ and the UMP for the quotient $R[x]/I$. $\square$