Galois Theory

Andrew Tran

1 Polynomial Rings

1.1 Adjuctions and their Properties

Definition 1. *Let $\mathscr{C}$ and $\mathscr{D}$ be categories. Then an adjunction from $\mathscr{C}$ to $\mathscr{D}$ is a 4-tuple $(\eta, \epsilon) : F \vdash G$, where $F : \mathscr{C} \to \mathscr{D}$ and $G : \mathscr{D} \to \mathscr{C}$ are functors, $\eta : 1_{\mathscr{C}} \Rightarrow GF$ and $\epsilon : FG \Rightarrow 1_{\mathscr{D}}$ are natural transformations and the following conditions hold:*

1. *For every $X \in Ob\mathscr{C}$, $\epsilon_{FX} \circ F\eta_X = 1_{FX}$*

2. *For every $Y \in Ob\mathscr{D}$, $G\epsilon_Y \circ \eta_{GY} = 1_{GY}$*

1.2 Polynomial Ring Adjoints

Definition 2. *Let $CRing$ be the category of commutative rings and ring homomorphisms and $CRing^*$ be the category of pointed commutative rings and pointed ring homomorphisms. Then the functor*

$$U : CRing^* \to CRing : [\phi : (R, a) \to (S, b)] \mapsto [\phi : R \to S]$$

is called the forgetful functor.

Definition 3. *A polynomial ring adjoint is a triple (Π, η, ϵ) such that*

$$(\eta, \epsilon) : \Pi \vdash U$$

is an adjunction from $CRing$ to $CRing^*$.

For the remainder of these notes, let (Π, η, ϵ) be a fixed polynomial ring adjoint. We define $\pi = U\Pi$.

Definition 4. *Let R be a commutative ring and let X be the distinguished point of the pointed ring ΠR. Then ΠR is referred to as the polynomial ring over R with indeterminate element X. The elements $p \in \Pi R$ are referred to as (formal, univariate) polynomials over R.*

Definition 5. *Let (R, a) be a pointed commutative ring. Then we define $eval_{(R,a)} = U\epsilon_{(R,a)} : \pi R \to R$ and refer to $eval_{(R,a)}$ as the evaluation homomorphism on R at a.*

Definition 6. *Let R be a commutative ring. Then we refer to $\eta_R : R \to \pi R$ as the R embedding homomorphism.*

Theorem 1. *For any pointed commutative ring (R, a), $\eta_R : R \to \pi R$ is injective and $eval_{(R,a)} : \pi R \to R$ is surjective.*

Proof. Let (R, a) be a pointed commutative ring. By definition of adjunctions,

$$eval_{(R,a)} \circ \eta_R = U\epsilon_{(R,a)} \circ \eta_{U(R,a)} = 1_{U(R,a)}$$

In other words, $eval_{(R,a)}$ is a right invertible function and η_R is a left invertible function. This implies that they are surjective and injective, respectively. $\square$

Definition 7. *Let R be a commutative ring. We define the subring of constant polynomials over R, $\overline{R} \subseteq \pi R$, to be the subring of πR given by the image of R under the embedding homomorphism η_R.*

Lemma 1. *For any commutative ring R, $R \cong \overline{R}$.*

Proof. It has already been proven that $\eta_R : R \to \overline{R}$ is injective and is, by construction, surjective on $\overline{R}$. $\square$

Theorem 2. *Let R be a commutative ring. Suppose $X \in \pi R$ is the indeterminate element. Then the following are equivalent:*

1. *$X \in \overline{R}$*
2. *X is a unit in πR*
3. *R is a zero ring*
4. *πR is a zero ring*

Proof. Let R be a commutative ring and $X \in \pi R$ be the indeterminate element.

1. Suppose that $X \in \overline{R}$. Let $x = \eta_R^{-1}(X) \in R$. By properties of adjunctions, the pair $(\eta_R, (\pi R, X))$ is an initial morphism from R to U. Additionally,
$$\eta_R : R \to U(\pi R, 1_{\pi R})$$
So, from the definition of initial morphisms, there is a unique pointed ring homomorphism $\phi : (\pi R, X) \to (\pi R, 1_{\pi R})$ such that
$$U\phi \circ \eta_R = \eta_R$$
Therefore,
$$X = \eta_R(x) = U\phi \circ \eta_R(x) = \phi(X) = 1_{\pi R}$$
So, X is a unit in πR.

2. Suppose that X is a unit in πR. Let $Y \in \pi R$ such that $XY = 1_{\pi R}$. Then
$$\begin{aligned} eval_{(R,0_R)}(XY) &= eval_{(R,0_R)}(1_{\pi R}) \\ eval_{(R,0_R)}(X) \cdot eval_{(R,0_R)}(Y) &= 1_R \\ 0_R \cdot eval_{(R,0_R)}(Y) &= 1_R \\ 0_R &= 1_R \end{aligned}$$
So, R is a zero ring.

3. Suppose that R is a zero ring. Then $1_R = 0_R$. Therefore,
$$\eta_R(1_R) = \eta_R(0_R)$$
Since η_R is a ring homomorphism,
$$1_{\pi R} = \eta_R(1_R) = \eta_R(0_R) = 0_{\pi R}$$
Thus, πR is a zero ring.

4. Suppose πR is a zero ring. Then $X = 0_{\pi R} = \eta_R(0_R) \in \overline{R}$.

Therefore, these conditions are all equivalent. □

Theorem 3. *Let R be a commutative ring. Then the indeterminate element $X \in \pi R$ is not a zero divisor in πR.*