A Deconstruction of the Fundamental Theorem Galois Theory

Sean McLaughlin

May 27, 2007

Abstract

This document breaks down the proof of the Fundamental Theorem of Galois Theory into a sequence of lemmas amenable to formalization in the Coq proof assistant.

This document breaks down the proof of the Fundamental Theorem of Galois Theory into a sequence of lemmas amenable to formalization in the Coq proof assistant. The numbering follows Rotman [1]. When a theorem of Rotman is broken down further for purposes of the formalization process, we give sub-letters to the numbering system of Rotman. Thus, for example, the Fundamental Theorem itself is theorem 63 in Rotman. We will need to prove it in smaller steps. Thus, we will have Lemma 63a, Lemma 63b, ... etc.

1 Rings

Definition (1a) A **commutative ring with 1**, or just a **ring**, is a set R equipped with two binary operations, $a + b, ab$ such that

(i) R is an abelian group under addition

(ii) multiplication is commutation and associative

(iii) $1r = r$

(iv) $r(s + t) = rs + rt$

1.1 Polynomials

Definition (1b) A **polynomial over** R is a sequence

$$f(x) = (r_0, r_1, \ldots, r_n, 0, 0, \ldots)$$

with $r_i \in R$ and $r_i = 0$ for $i > n$. Equality and addition are defined componentwise. The product is defined by the usual polynomial multiplication. Denote the set of such polynomials by $R[x]$.

Theorem (1c) If R is a ring, then so is $R[x]$.

Definition (1d) The **leading coefficient** of a polynomial $(r_0, r_1, \ldots, r_n, 0, 0, \ldots)$ is r_n where n is the largest index with nonzero coefficent.

Definition The largest index of a nonzero coefficient is called the **degree** of the polynomial.

Definition A polynomial is **monic** if its leading coefficient is 1.

Definition A polynomial is **constant** if it is either the 0 polynomial, or has degree 0.

2 Galois Theory

Theorem (63) [ABC]

References

[1] J. Rotman. *Galois Theory.* Springer Verlag, 1990.