FEBRUARY 15 NOTES

1. 13.4: Splitting Fields and Algebraic Closures

To end this section, we will construct the *algebraic closure* of a field F, a field in which *every polynomial* in $F[x]$ factors completely.

Definition 1.1. A field $\overline{F}$ is called an **algebraic closure** of F if $\overline{F}$ is algebraic over F and every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$. In other words, $\overline{F}$ contains all of the elements algebraic over F.

A field K is **algebraically closed** if every polynomial with coefficients in K has a root in K. Note that this implies that every polynomial splits completely in K.

Proposition 1.2. *For any field F, there exists an algebraically closed field K containing F.*

Proof. For every nonconstant monic polynomial $f(x) \in F[x]$, let x_f represent a variable. Consider the polynomial ring $R = F[\dots x_f \dots]$ generated over F by all of these variables. Because f is a polynomial, we can plug in the variable x_f. Let I be the ideal generated by all of the polynomials of the form $f(x_f)$.

Claim: I is proper. Why? If not, then $1 \in I$, so we can form 1 as a *finite* R-linear combination of some of these polynomials, i.e.

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n})$$

for $g_i \in R$. For simplicity, denote x_{f_i} by x_i. Because each g_i is a polynomial, there is a finite number of variables appearing in all of the g_i's, so this relation is just

$$1 = g_1(x_1, \dots, x_m) f_1(x_1) + \cdots + g_n(x_1, \dots, x_m) f_n(x_n).$$

Let F' be a finite extension of F containing a root α_i of f_i for each i. Then, in F', we have $1 = 0$, a contradiction. Therefore, I is proper.

Because I is proper, it is contained in some maximal ideal M. Therefore, the quotient $K_1 = R/M$ is a field containing F and each polynomial f in $F[x]$ has a root in K_1 by construction (we quotiented by an ideal containing $f(x_f)$, so the root is the image of x_f). Now, we can repeat this procedure to produce a field K_2 in which every polynomial with coefficients in K_1 has a root, and so on, to obtain a sequence of fields

$$F = K_0 \subset K_1 \subset K_2 \subset \dots$$

where each polynomial in K_j has a root in K_{j+1}.

Define

$$K = \cup_{j \geq 0} K_j$$

so K is a field containing F, and for any polynomial h with coefficients in K, h has only finitely many terms so each term must appear in K_N for some (possibly very large N), i.e. $h(x) \in K_N[x]$. By construction, h has a root in K_{N+1} which is contained in K, so h has a root in K. Therefore, K is algebraically closed. □

Finally, because we now know that algebraically closed fields exist, we can show:

Proposition 1.3. *Let F be a field. The algebraic closure of F exists and is unique up to isomorphism.*

Proof. By the previous proposition, we can find an algebraically closed field containing K containing F. Let $\overline{F}$ be the elements of K that are algebraic over F. By definition, this is an algebraic extension of F. Because any $f(x) \in F[x]$ splits completely in K, every root α of $f(x)$ is contained in K. By definition, α is algebraic over F, so α is contained in $\overline{F}$. Therefore, f splits completely in $\overline{F}[x]$ so $\overline{F}$ is an algebraic closure of F.

The proof of uniqueness is omitted. (Idea: use uniqueness of splitting field of each polynomial.) □

Something we will prove in the future is:

Theorem 1.4. *The field $\mathbb{C}$ is algebraically closed.*

By the proof of the previous proposition, because $\mathbb{Q} \subset \mathbb{C}$, the algebraic closure of $\mathbb{Q}$ therefore exists and is contained in $\mathbb{C}$. So, whenever we do computations with algebraic elements over $\mathbb{Q}$, we may assume that everything is happening in $\mathbb{C}$.

2. 13.5: Separable and Inseparable Extensions

Definition 2.1. If $f(x) \in F[x]$ is a polynomial, over the splitting field for f we can factor f as

$$f(x) = (x - \alpha_1)^{n_1} \dots (x - \alpha_k)^{n_k}$$

where the α_i are the distinct roots of the polynomial and $n_i \geq 1$. The numbers n_i are called the **multiplicities** of the roots α_i. If $n_i = 1$, α_i is called a **simple root** and if $n_i > 1$, α_i is called a multiple root.

Definition 2.2. A polynomial F is called **separable** if it has no multiple roots. It is called **inseparable** if it has multiple roots.

This *depends* on the field.

Example 2.3. The polynomial $x^2 - 2$ is separable over $\mathbb{Q}$ because its two roots are distinct.

Example 2.4. The polynomial $x^2 - t$ over the field $F = \mathbb{F}_2(t)$ (rational functions over $\mathbb{F}_2$) is irreducible but inseparable. The root $\sqrt{t} \notin F$ but because $\mathrm{char} F = 2$, and $1 = -1$ in $\mathbb{F}_2$,

$$(x - \sqrt{t})^2 = x^2 - 2x\sqrt{t} + t = x^2 - t$$

so $\sqrt{t}$ is a multiple root.

Definition 2.5. If $f(x) = a_n x^n + \dots + a_0 \in F[x]$ is a polynomial, the **derivative** of f is defined as

$$D_x f(x) = n a_n x^{n-1} + \dots + a_1 \in F[x].$$

This is the usual formula for the derivative, but keep in mind that it does not have a geometric meaning at this point (has nothing to do with the usual calculus construction involving limits). But, from the definition, one can show that the usual 'rules' in calculus (e.g. the product rule) still hold.

Definition 2.6. A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$, i.e. $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial of α. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative.

Proof. Suppose α is a multiple root, so in some splitting field, $f(x) = (x - \alpha)^n g(x)$ for some $n \geq 2$. Then, $D_x f(x) = n(x - a)^{n-1} g(x) + (x - a)^n D_x g(x)$ has α as a root.

Conversely, if α is a root of both $f(x)$ and $D_x f(x)$, then we know $f(x) = (x - a)h(x)$, and taking the derivative yields $D_x f(x) = h(x) + (x - \alpha) D_x h(x)$, or equivalently $h(x) = D_x f(x) - (x - \alpha) D_x h(x)$. Because α is a root of the right hand side, it is also a root of $h(x)$ and hence $h(x) = (x - \alpha) g(x)$, i.e. $f(x) = (x - \alpha)^2 g(x)$ so α is a multiple root. □

Example 2.7. The polynomial $x^n - 1$ has derivative nx^{n-1}. Over any field of characteristic not dividing n, the only root of the derivative is 0, which is not a root of $x^n - 1$, so $x^n - 1$ is separable.

If the characteristic divides n, then the derivative is 0, so *every* element of the field is a root of the derivative, and hence every root of $x^n - 1$ is a multiple root and $x^n - 1$ is inseparable.

Example 2.8. The polynomial $x^{p^n} - x$ over $\mathbb{F}_p$ has derivative $p^n x^{p^n - 1} - 1 = -1 \neq 9$, so the derivative has no roots. This implies that $x^{p^n} - x$ is separable.

Separability is most interesting over fields of characteristic p, because:

Corollary 2.9. Every irreducible polynomial over a field of characteristic 0 is separable. A general polynomial over a field of characteristic 0 is separable if and only if it is the product of distinct (up to multiplication by a unit) irreducible polynomials.

Proof. Suppose $\mathrm{char} F = 0$ and $p(x) \in F[x]$ is irreducible of degree n. Because $p(x)$ is irreducible, its only factors (up to multiplication by a unit) are 1 and $p(x)$, and $D_x p(x)$ has degree $n-1$ so is not divisible by $p(x)$. Hence, $p(x)$ and $D_x p(x)$ are relatively prime and therefore have no common root.

The second statement follows because distinct irreducible polynomials never have roots in common: if $p(x)$ is irreducible, it is (up to multiplication by a unit) the minimal polynomial of any of its roots, and if $q(x)$ is any other irreducible polynomial with a common root, then it must also be divisible by the minimal polynomial and hence equal to $p(x)$ (up to a unit). □

Remark 2.10. Even in characteristic p, if $D_x p(x)$ is *non-zero*, the same proof applies to show irreducible polynomials are separable. So, the only way to find inseparable irreducible polynomials is to have those whose derivative is identically 0.

We can actually say more: suppose $p(x) \in F[x]$ is an inseparable irreducible polynomial over a field F of characteristic p. To be inseparable, the derivative must be identically 0, i.e. $D_x p(x) = 0$, which is possible if and only if each exponent in the polynomial $p(x)$ is a multiple of p. In other words,

$$p(x) = a_m x^{mp} + a_{m-1} x^{(m-1)p} + \cdots + a_1 x^p + a_0$$

so $p(x) = q(x^p)$ for the polynomial $q(x)$ given by

$$q(x) = a_m x^m + a_{m-1} x^{(m-1)} + \cdots + a_1 x + a_0.$$