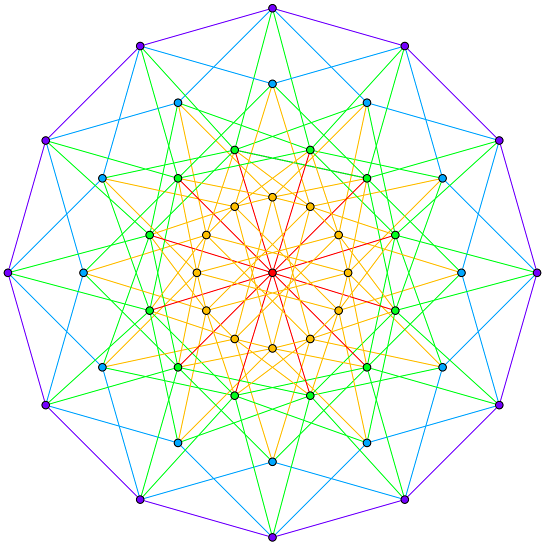
Algebra (II)

Fields, Modules, and Galois Theory

Braden Hoagland



Contents

Definition 1. *A field K is a **(field) extension** of F if F is a subfield of K. Denote this by $K \nwarrow F$.*

Definition 2. *If K is an extension of F, then the **degree** $[K : F]$ of K over F is the dimension of K as an F-vector space. An extension is **finite** if its degree is finite, and its **infinite** otherwise.*

Example 1. $[\mathbb{C} : \mathbb{R}] = 2$ *because $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.*

Many field extensions arise from trying to solve polynomial equations, so we gotta review that.

Theorem 1. *Let F be a field, then $F[x]$ is a Euclidean Domain.*

This means that any polynomial ring over a field has a division algorithm, i.e. for all $f(x)$ and nonzero $g(x)$, there exist *unique* $q(x), r(x)$ such that

$$f(x) = q(x)g(x) + r(x),$$

where $\deg r(x) < \deg g(x)$. Here, we take the degree of the zero polynomial to be 0. It should also be clear that degree is the norm of $F[x]$.

Corollary 1. *$F[x]$ is also a principal ideal domain (PID) and a unique factorization domain (UFD).*

If $E \nwarrow F$ and $f(x), 0 \neq g(x) \in F[x]$, then the result of the division algorithm in $F[x]$ is the same in $E[x]$ by the uniqueness bit. paragraph at end of sec 9.2.

Often, even if R is not a field (but *is* a UFD), then we can say something about factorization in R by looking at its field of fractions (the smallest field containing R, see sec 7.5, think $\mathbb{Z}$ to $\mathbb{Q}$).

Lemma 1 (Gauss' Lemma)**.** *Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$ have coefficients with $\gcd$ 1, then $p(x)$ is irreducible in $R[x]$ if and only if it's irreducible in $F[x]$.*

Note that this works for all monic polynomials.

Proposition 1. *Let $p(x) \in F[x]$, where F is a field. Then $p(x)$ has a root $a \in F$ if and only if $(x - a)$ divides $p(x)$.*

Proof. Do this. □

Corollary 2. *Any $p(x) \in F[x]$ has at most $\deg p$ roots in F (including with multiplicity).*

Proof. Use induction on the proposition above. □

Corollary 3. *If $p(x) \in F[x]$ has degree 2 or 3, then it's reducible if and only if it has a root in F.*

The above corollary should be relatively obvious, but note that it doesn't hold in 4 dimensions or higher because a reducible polynomial could reduce into two other polynomials that have dimension 2+.

Example 2. *We claim that $p(x) = x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Using Corollary 3, we check that $p(0)$ and $p(1)$ are nonzero, so p has no roots in $\mathbb{F}_2$.*

Proposition 2. *Let R be a UFD and let $p(x) = \sum_i a_i x^i \in R[x]$. If c and d are relatively prime with d nonzero and $p(c/d) = 0$, then $c \mid a_0$ and $d \mid a_n$.*

This is very useful in limiting the candidates for the roots of a particular polynomial.

Example 3. *We claim that $p(x) = x^3 - x - 1$ is irreducible in $\mathbb{Z}[x]$. By Gauss' Lemma and Corollary 3, it suffices to show that p has no rational roots. By the above proposition, the only possibilities of rational roots are ± 1. But $p(1)$ and $p(-1)$ are both nonzero, so p is irreducible.*

Theorem 2 (Eisenstein's Criterion)**.** *Let R be a UFD with field of fractions F and let $f(x) = \sum_i a_i x^i \in R[x]$ with $n \geq 1$ (i.e. non-constant) and $a_n \neq 0$. If there is some irreducible $p \in R$ such that*

1. *p does not divide a_n,*
2. *p divides a_i for all $i < n$, and*
3. *p^2 does not divide a_0,*

then $f(x)$ is irreducible in $F[x]$.

This is usually used when $R = \mathbb{Z}$ (so the field of fractions is $\mathbb{Q}$) and p is prime.

Example 4. *$x^{12} - 10x^4 + 4x - 6$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion for $p = 2$.*

Theorem 3. *The multiplicative group of any finite field is cyclic.*

Proof. Let F be a finite field, then $F^\times = F - \{0\}$. Since F is a field, it's a commutative ring, so $F^\times$ is an abelian group under multiplication. Finish this. □