M3P8 LECTURE NOTES 5: FIELD EXTENSIONS

1. Prime Fields

Let K be a field. We have a unique ring homomorphism $\iota : \mathbb{Z} \to K$; its kernel is a prime ideal of $\mathbb{Z}$. Thus the kernel is either the zero ideal (if K has characteristic zero) or the ideal $\langle p \rangle$ for some prime p of $\mathbb{Z}$.

In the latter case we get an injection of the field $\mathbb{Z}/p\mathbb{Z}$ (which we often denote $\mathbb{F}_p$ when we think of it as a field) into K. In the former case, the injection of $\mathbb{Z}$ into K extends to an injection of $\mathbb{Q}$ into K, sending $\frac{a}{b}$ to $\iota a \iota b^{-1}$. Thus the field K contains exactly one of $\mathbb{Q}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, etc. depending on its characteristic. This field is called the "prime field" of K, and it is contained in K in a unique way.

2. Field Extensions

The prime fields are in some sense the smallest possible fields. Once we know they exist, it makes sense to study fields by studying pairs K, L of fields such that $K \subseteq L$. Such a pair is called a *field extension* of L over K, and is often denoted L/K. Note that such an inclusion of fields makes L into a vector space over K.

Definition 2.1. We say that a field extension L/K is *finite* if L is finite-dimensional as a K-vector space. The *degree* of such an extension is the dimension of L as a K-vector space, and is denoted $[L : K]$.

Proposition 2.2. *Let $K \subseteq L \subseteq M$ be fields. Then M/K is finite if, and only if, M/L and L/K are both finite. If this is the case then $[M : K] = [M : L][L : K]$.*

Proof. First suppose that M/K is finite. Then L is a K-subspace of M, so finite dimensional as a K-vector space. Moreover, there exists a finite K-basis for M, and this basis spans M over K and thus also over L. Thus M is finite-dimensional as an L-vector space.

Conversely, let $e_1, \dots e_n$ be a K-basis of L, and let $f_1, \dots, f_m$ be an L-basis for M. Then every element x of M can be expressed uniquely as $c_1 f_1 + \cdots + c_m f_m$, with c_i in L. Each c_i in turn can be expressed as $d_{1,i}e_1 + d_{2,i}e_2 + \cdots + d_{n,i}e_n$ with $d_{j,i} \in K$. Thus we can express x as $d_{1,1}e_1 f_1 + d_{2,1}e_2 f_1 + \cdots + d_{n,m}e_n f_m$. In particular the set $\{e_i f_j\}$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ spans M over K.

In this case the degree of L over K is n and the degree of M over L is m, so it remains to show that $\{e_i f_j\}$ is linearly independent over K. Suppose we have elements $r_{i,j}$ of K such that $\sum r_{i,j} e_i f_j = 0$. Then, regrouping, we find that $\sum_j (\sum_i r_{i,j} e_i) f_j$ is an L-linear combination of the f_j that is zero;

since the f_j are linearly independent we must have $\sum_i r_{i,j} e_i = 0$ for all j. Since the e_i are linearly independent over K we must have $r_{i,j} = 0$ for all i, j. □

3. Extensions generated by one element

Let L/K be a field extension, and let α be an element of L. We let $K(\alpha)$ denote the subfield of L consisting of all elements of L of the form $\frac{P(\alpha)}{Q(\alpha)}$, where P and Q are polynomials with coefficients in K and $Q(\alpha)$ is not zero. This is the smallest subfield of L containing K and α.

We have a map $K[X] \to K(\alpha)$ that takes a polynomial $P(X)$ to $P(\alpha)$; it is a ring homomorphism. Let I_α be the kernel of this homomorphism; we then get an injection of $K[X]/I_\alpha$ into the field $K(\alpha)$. Thus $K[X]/I_\alpha$ is an integral domain, so I_α is a prime ideal of $K[X]$.

Since $K[X]$ is a PID, every nonzero prime ideal is maximal. There are thus two cases. In the first I_α is the zero ideal; that is, there is no nonzero polynomial Q in $K[X]$ such that $Q(\alpha)$ is zero in L. We say that α is *transcendental* over K in this case. In the second I_α is a maximal ideal of $K[X]$; in this case we say α is *algebraic* over K.

Assume first that α is transcendental over K. In this case the map taking $P(X)$ to $P(\alpha)$ is an *injection* of $K[X]$ into L; in particular every nonzero element of $K[X]$ gets sent to a nonzero (hence invertible) element of L. Thus the map from $K[X]$ to L extends to a map from the field of fractions of $K[X]$ (which we denote $K(X)$) to L. This map takes $\frac{P(X)}{Q(X)}$ to $\frac{P(\alpha)}{Q(\alpha)}$. The image of this map is $K(\alpha)$; in particular $K(X)$ and $K(\alpha)$ are isomorphic. We call $K(X)$ the *field of rational functions in* X. Note that in this case $K(\alpha)$ is infinite dimensional as a K-vector space (it contains a subspace isomorphic to $K[X]$, for instance.)

If α is algebraic over K, then I_α is a nonzero maximal ideal of the PID $K[X]$, so it is generated by a single polynomial $Q(X)$. Since the units in $K[X]$ are just the constant polynomials, the polynomial $Q(X)$ is well-defined up to a constant factor; it is called the *minimal polynomial* of α. By definition, it divides every polynomial $P(X)$ such that $P(\alpha) = 0$. The ring $K[X]/\langle Q(X)\rangle$ is a field, whose dimension as a K-vector space is equal to the degree of $Q(X)$. The map $K[X] \to K(\alpha)$ descends to an injection of $K[X]/\langle Q(X)\rangle$ into $K(\alpha)$; since its image is a subfield of $K(\alpha)$ containing K and α, this map is an *isomorphism* of $K(\alpha)$ with $K[X]/\langle Q(X)\rangle$. Thus in this case the extension $K(\alpha)/K$ is a finite extension, of degree equal to the degree of $Q(X)$.

4. Algebraic Extensions

Definition 4.1. An extension L/K is *algebraic* if every element of L is algebraic over K.

Proposition 4.2. *If L/K is finite, then L/K is algebraic.*

Proof. Let L/K be finite, and suppose $\alpha \in L$ is transcendental over K. Then we have an injection of $K[X]$ into L taking X to α. Since $K[X]$ is an infinite-dimensional K vector space, L cannot be finite over K.

(More explicitly, there is also the following argument: let d be the dimension of L over K. Then for any α, the set $1, \alpha, \dots, \alpha^d$ must be linearly dependent over K; this gives a nonzero polynomial P such that $P(\alpha) = 0$.) □

Corollary 4.3. *Let L/K be a field extension, and suppose α, β are elements of L algebraic over K. Then $\alpha + \beta$ and $\alpha\beta$ are algebraic over K. Moreover, if α is nonzero then α^{-1} is algebraic over K.*

Proof. Consider the chain of extensions:

$$K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$$

where we write $K(\alpha, \beta)$ for $(K(\alpha))(\beta)$. Since α is algebraic over K, $K(\alpha)$ is finite over K. Since β is algebraic over K, it is also algebraic over $K(\alpha)$, so $K(\alpha, \beta)$ is finite over $K(\alpha)$. Thus $K(\alpha, \beta)$ is algebraic over K. On the other hand, we also have a chain of extensions:

$$K \subseteq K(\alpha + \beta) \subseteq K(\alpha, \beta),$$

so $K(\alpha + \beta)$ is finite over K. Hence $\alpha + \beta$ is finite over K. The proofs for $\alpha\beta$ and α^{-1} are similar. □

Corollary 4.4. *For any extension L/K, let L' be the subset of L consisting of all elements that are algebraic over K. Then L' is a field.*

Proof. We have seen that L' is closed under addition, multiplication, and taking inverses. □

In particular, the set $\overline{\mathbb{Q}}$ of complex numbers that are algebraic over $\mathbb{Q}$ is a field, called the field of algebraic numbers.

5. Example

Consider the polynomial $X^2 + X + 1$ in $\mathbb{F}_2[X]$. It has no roots in $\mathbb{F}_2$, so it is irreducible (as a polnyomial of degree 2 any nontrivial factor would be linear). Thus the quotient $\mathbb{F}_2[X]/\langle X^2 + X + 1\rangle$ is a field extension of degree 2 of $\mathbb{F}_2$, which is denoted $\mathbb{F}_4$. Its four elements are $0, 1, X, X + 1$ (or more precisely, their classes modulo $\langle X^2 + X + 1\rangle$.) Note that $X^2 = X + 1$, $(X + 1)^2 = X$, and $X^3 = X(X + 1) = 1$; in particular the multiplicative group of $\mathbb{F}_4$ is cyclic of order 3. (This is not particularly surprising, as all groups of order 3 are cyclic. We will see later, though, that the multiplicative group of any finite field is cyclic.)