Math 361 lecture for Friday, Week 1

Field extensions

In the first lecture, in order to think about Pythagorean triples, we extended the field of rational numbers by adding i to get the field $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$. We then considered the Gaussian integers sitting inside of that field,

$$\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\} \subset \mathbb{Q}(i).$$

We picture the situation as follows, with lines representing the superset/subset relation:

$$\begin{array}{ccc} \mathbb{Q}(i) & \text{——} & \mathbb{Z}[i] \\ \Big| & & \Big| \\ \mathbb{Q} & \text{———} & \mathbb{Z}. \end{array}$$

To understand Pythagorean triples, we then considered factorization of elements in $\mathbb{Z}[i]$. Our goal is to generalize this construction: extend a field by adding some elements not in the field, and then consider a subset that plays the role of the integers inside that field. Of special interest with be factorization properties of these new integers.

Extension fields

A *field extension* is a pair of fields $K \subseteq L$. In that case, L is automatically a vector space over K. It's dimension is denoted

$$[L : K] := \dim_K L,$$

and we might display this like so:

$$\begin{array}{c} L \\ \Big|{\scriptstyle [L:K]} \\ K. \end{array}$$

If $[L : K] < \infty$, we say that L is a *finite field extension of* K. For example, a basis for $\mathbb{Q}(i)$ over $\mathbb{Q}$ is $\{1, i\}$, and we have

$$\begin{array}{c} \mathbb{Q}(i) \\ \Big|{\scriptstyle 2} \\ \mathbb{Q}. \end{array}$$

We usually denote a field extension $K \subseteq L$ by L/K.

Proposition 1. Suppose K, H and L are fields with $K \subseteq H \subseteq L$, and suppose that $[L : K] < \infty$. Then $[L : H] < \infty$ and $[H : K] < \infty$, and

$$[L : K] = [L : H][H : K].$$

Proof. Homework. □

Algebraic elements of a field extension

Definition 2. Let L/K be a field extension. Then $\alpha \in L$ is *algebraic* over K if there exists a nonzero polynomial $f \in K[x]$ such that $f(\alpha) = 0$.

Example 3. The numbers $\sqrt{2}, i \in \mathbb{C}$ are algebraic over $\mathbb{Q}$ since they are zeros of $x^2 - 2$ and $x^2 - 1$, respectively. The numbers $e, \pi \in \mathbb{R}$ are not algebraic over $\mathbb{Q}$ (although this is not easy to prove). If $Q(t)$ denotes the field of rational functions in t (whose elements have the form f/g with $f, g \in \mathbb{Q}[t]$ and $g \neq 0$), then t is not algebraic over $\mathbb{Q}$. However, t is algebraic over $\mathbb{Q}(t)$ since is it satisfies the polynomial $x - t$ having coefficients in $\mathbb{Q}(t)$. It is also algebraic over $\mathbb{Q}(t^2)$ (the field of rational functions in t with coefficients in $\mathbb{Q}$) since it satisfies the polynomial $x^2 - t \in \mathbb{Q}(t^2)[x]$.

Proposition 4. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique monic polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$. (A polynomial is *monic* if its leading coefficient is 1, i.e., if the coefficient of its term of highest degree is 1.)

Proof. Let I be the set of $f \in K[x]$ such that $f(\alpha) = 0$. Then I is an ideal, and since $K[x]$ is a PID, there exists $p \in K[x]$ such that $I = (p)$. By dividing through by the leading coefficient of p, we may assume that p is monic. If f is any nonzero element of I, we may write

$$f = pq$$

for some nonzero $q \in K[x]$. We have

$$\deg(f) = \deg(pq) = \deg(p) + \deg(q) \geq \deg(p).$$

If $\deg(f) = \deg(p)$, then $\deg(q) = 0$. So q is a nonzero element of K. Two polynomials are, by definition, equal if and only if their coefficients are equal. So if $\deg(f) = \deg(p)$ and f is monic, it follows that $f = p$. □

Definition 5. The polynomial p in the above proposition is called the *minimal polynomial for α over K*.

Proposition 6. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. First, suppose that p is the minimal polynomial for α. Suppose $p = fg$ with $f, g \in K[x]$. Then $0 = p(\alpha) = f(\alpha)g(\alpha)$ implies that $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, say $f(\alpha) = 0$. Further, since p has positive degree, $p \neq 0$, and hence, $f \neq 0$. So since $f(\alpha) = 0$, it follows that $\deg(f) > 0$.[1] We have

$$\deg(p) = \deg(f) + \deg(g).$$

By minimality of p, we have $\deg(f) = \deg(p)$ and $\deg(g) = 0$. So g is a (nonzero) element of K, and nonzero elements of K are invertible in $K[x]$, i.e., units. We have shown that if f factors, then one of those factors is a unit. Thus, f is irreducible.

Conversely, suppose that p is irreducible and that $f \in K[x]$ is the minimal polynomial for α over K. By definition of the minimal polynomial, we have $\deg f \leq \deg p$ and $f(\alpha) = 0$. Use the division algorithm to write

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$. Then,

$$0 = p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha).$$

If $r \neq 0$, let $\tilde{r}$ be r divided by its leading coefficient. It follows that $\tilde{r}$ is a monic polynomial with $\tilde{r}(\alpha) = 0$ and $\deg(\tilde{r}) < \deg(f)$, contradicting the definition of f. So $r = 0$ and $p = qf$. Since p is irreducible $f \notin K$, it must be that q is a unit (i.e., and nonzero element of K). Since p and f are monic, $p = f$. □

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let $K[\alpha]$ be the smallest subring of L containing α, and let $K(\alpha)$ be the smallest subfield of L containing α. Then

$$K[\alpha] := \{f(\alpha) : f \in K[x]\},$$

and

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}.$$

Theorem 7. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof. First suppose that $[K(\alpha):K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n+1$ (not necessarily distinct) elements in a vector space of dimension n, so they are linearly dependent. This means $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero. Define the polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$. Then $f \in K[x]$ and $f(\alpha) = 0$. So α is algebraic over K.

Conversely, suppose that α is algebraic over K, and let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial. We first claim that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent. If not, then

[1] If $\deg(f) = 0$, then f is a constant. In that case, the only way we could have $f(\alpha) = 0$ is for that constant to be 0. However, $f \neq 0$.

there is a nontrivial linear relation $\sum_{i=0}^{n-1} b_i \alpha^i$. Defining $f = \sum_{i=0}^{n-1} b_i x^i$, we have $f \in K[x]$ and $f(\alpha) = 0$. However, $\deg(f) < \deg(p) = n$, which contradicts the minimality of p.

Next, consider the vector space $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. We claim that V is a field. To see this, first note that rearranging $p(\alpha) = 0$, we have

$$\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i.$$

It follows that V is closed under multiplication. Most of the field properties then follow trivially from the fact that $V \subseteq L$ and L is a field. What remains is to show that nonzero elements have inverses. So let $v \in V \setminus \{0\}$ and write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$. Define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $v = h(\alpha)$. Now p is irreducible, hence, prime. So the only prime factor h and p could share is p, itself, but $\deg(h) < \deg(p)$. Hence, h and p are relatively prime, i.e., they share no prime factors. It follows that there are $f, g \in K[x]$ such that

$$fh + gp = 1.$$

Therefore,

$$1 = f(\alpha)h(\alpha) + g(\alpha)p(\alpha) = g(\alpha)h(\alpha) = f(\alpha)v.$$

Hence v has the multiplicative inverse $f(\alpha) \in V$.

Since V is a field in L containing α and $K(\alpha)$ is the smallest field in L containing α, it follows that $K(\alpha) \subseteq V$. On the other hand, $V \subseteq K[\alpha]$. In sum,

$$K(\alpha) \subseteq V \subseteq K[\alpha] \subseteq K(\alpha).$$

We have shown that $K(\alpha) = K[\alpha]$ of dimension $\deg(p)$. □

Here is another perspective. Suppose that $\alpha \in L$ is algebraic over the subfield K. Define a mapping

$$\begin{aligned} \phi\colon K[x] &\to K[\alpha] \\ f &\mapsto f(\alpha). \end{aligned}$$

We have

$$\ker(\phi) = \{f \in K[x] : f(\alpha) = 0\}.$$

Since $K[x]$ is a PID, we can write $\ker(\phi) = (p)$ for some monic polynomial $p \in K[x]$. In fact, p must be the minimal polynomial for α. By the standard isomorphism theorem, we have

$$K[x]/(p) \approx K[\alpha].$$

Since p is irreducible and $K[x]$ is a PID, it follows that (p) is a maximal ideal. Hence, $K[x]/(p)$ is a field. Therefore, $K[\alpha]$ is a field, and it follows that $K[\alpha] = K(\alpha)$.

Corollary 8. If $[L : K] < \infty$ and $\alpha \in L$, then α is algebraic over K.

Proof. Suppose $[L : K] < \infty$ and $\alpha \in L$. Then since $K(\alpha)$ is a K-subvector space of L, it follows that $[K(\alpha) : K] < \infty$, and the result follows from Theorem 7. □