Lecture 1-6: Field extensions

January 6, 2025

I begin the quarter by shifting gears, looking at extensions of fields, that is, fields L containing a given subfield K. Last term I looked briefly at rings B containing a subring A, defining the notion of an element of B integral over A. This time I can use the machinery of linear algebra to express the relationship between K and L much more precisely than I could for A and B.

Definition, p. 511

Given a field extension $K \subset L$, the *degree* of L over K, denoted $[L : K]$, is the dimension of L as a vector space over K. If this is finite, then we say that L is finite over K.

Assume first that L is generated over K as a field by a single element y, so that every element of L takes the form $\frac{p(y)}{q(y)}$ for some $p, q \in K[x], q \neq 0$. Such an extension of K is called simple (see p. 517). The simplest case occurs when $q(y) \neq 0$ for any $q \neq 0$; in this case we say that y is transcendental over K. Clearly $[L : K]$ is infinite in this case and every element of L takes the form $\frac{p(y)}{q(y)}$ for some nonzero $q \in K[x]$.

If instead $q(y) = 0$ for some nonzero polynomial q, then the unique monic q of least degree with this property is irreducible over K. We say that y is algebraic over K in this situation; thus $y \in L$ is algebraic over K if and only if the field $K(y)$ generated by K and y is finite over K, or if and only if the ring $K[y]$ generated by K and y is finite-dimensional over K. In particular, if y is algebraic over K then so is every element of $K(y)$. We say that L is algebraic over K if every element of it is (even if the degree of L over K is infinite). Recall also that if q is irreducible in $K[x]$, then the quotient $K[x]/(q)$ is an extension field finite over K, of degree equal to that of q. Finiteness of extensions is transitive in the following fundamental sense.

Theorem 14, p. 523

If $K \subset L \subset M$ are fields with L finite over K and M finite over L, then M is finite over K and $[M : K] = [M : L][L : K]$.

Proof.

If $[L : K]$ and $[M : L]$ are both finite, then let $\alpha_1, \ldots, \alpha_m$ be a basis of L over K and $\beta_1, \ldots, \beta_n$ a basis of M over L. Then I claim that the products $\alpha_i\beta_j$ form a basis of M over K, so that indeed $[M : K] = nm = [M : L][L : K]$. Indeed, any $m \in M$ is a combination $\sum \ell_j\beta_j$ for some $\ell_j \in L$; writing each ℓ_j as a combination $\sum k_{ij}\alpha_i$ with $k_{ij} \in K$, we see that the $\alpha_i\beta_j$ span M over K. The proof of their linear independence is similar. $\square$

As a corollary, if L is an extension of K and $\alpha, \beta \in L$ are algebraic over K, then so are $\alpha \pm \beta, \alpha\beta$, and α/β (Corollary 18, p. 527). In particular, if L is algebraic over K and M is algebraic over L, then M is algebraic over K (Theorem 20, p. 527. We saw earlier for that if elements α, β of a ring B are *integral* over a smaller ring A, then so are $\alpha \pm \beta$ and $\alpha\beta$, but in that setting α/β need not be integral over A.

Let K_1, K_2 be two extensions of a field K both contained in a larger field L. The composite K_1K_2 of K_1 and K_2 is the subfield of L generated by K_1 and K_2.

Proposition 21, p. 529

With notation as above, if the K_i are finite over K, then so is the composite K_1K_2, and in fact $[K_1K_2 : K] \leq [K_1 : K][K_2 : K]$.

Indeed, if $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ are respective basis of K_1 and K_2 over K then the proof of Theorem 14 above shows that the products $\alpha_i\beta_j$ span K_1K_2 over K (though they need not be independent). If moreover n and m are relatively prime, however, then the degree $[K_1K_2 : K]$, being a multiple of both n and m by Theorem 14, must be exactly nm, so that in this case the $\alpha_i\beta_j$ do form a basis of K_1K_2.

We have seen that any finite simple extension L of K takes the form $K[x]/(q)$ for some irreducible polynomial $q \in K[x]$; but it is emphatically *not* true for monic irreducible q_1, q_2 that the fields $K[x]/(q_1)$ and $K[x]/(q_2)$ are isomorphic if and only if $q_1 = q_2$. For example, the quadratic formula (which is valid over any field of characteristic different from two) shows that given any irreducible quadratic polynomial $q = x^2 + bx + c \in K[x]$ and any extension L of K in which $\beta = b^2 - 4c$ has a square root α, the subfields $K_1 = K(\alpha)$ and $K_2 K(r)$ of L coincide for any root r of q. Here $K_1 \cong K[x]/(x^2 - \beta), K_2 \cong K[x]/(q)$. In fact any quadratic extension L (having degree two) of a field K with characteristic different from 2 is generated by a single element α with $\alpha^2 \in K$.

Thus given two elements α, β of a field L both algebraic over a smaller field K, it is by no means obvious in general when the subfields $K(\alpha), K(\beta)$ respectively generated by α, β over K coincide; it is even more difficult to decide more generally whether or not $\beta \in K(\alpha)$. Often one can rule this out by looking at degrees.

Definition, p. 520

Given an extension L of a field K and $\alpha \in L$ the *degree of α over K* is defined to be the degree $[K(\alpha) : K]$ of the field extension $K(\alpha)$ over K.

Clearly this is infinite if and only if α is transcendental over K and coincides with the degree d of the minimal polynomial of α over K otherwise.

It follows at once from Theorem 14 that the degree of any $\alpha \in L$ divides the degree $[L : K]$ of L over K. Thus for example we can say immediately that $\alpha = 2^{1/3}$, the (real) cube root of 2, does not lie in any quadratic extension of the rational field $\mathbb{Q}$, for the polynomial $x^3 - 2$ is easily seen to be irreducible over $\mathbb{Q}$ by Eisenstein's Criterion, whence the degree of α over $\mathbb{Q}$ is 3. It is also true for example that $\sqrt{3}$ does not lie in the subfield $\mathbb{Q}(\sqrt{2})$ (say of $\mathbb{C}$), but the proof is a little harder. By looking at degrees we see that the only way this could hold is if $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2})$; but if $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$, then by squaring both sides and equating coefficients we would get in particular that $ab = 0$; but there is no rational square root of 3 or $3/2$, so this is a contradiction.

If p is a prime number, then the polynomial $x^{p-1} + \ldots + x + 1$ is irreducible over $\mathbb{Q}$ (as one sees from Eisenstein's Criterion by changing the variable from x to $x + 1$), so that the complex pth root of 1 $e^{2\pi i/p} \in \mathbb{C}$ has degree $p - 1$ over $\mathbb{Q}$. Now it turns out for odd p that $\sqrt{p}$ lies in the field $\mathbb{Q}(e^{2\pi i/p})$, but this is far from obvious; on the other hand, it is not ruled out by degree considerations, since 2 divides $p - 1$. In fact a famous result called the Kronecker-Weber Theorem implies in particular that for any $r \in \mathbb{Q}$ that the extension $\mathbb{Q}(\sqrt{r})$ lies in $\mathbb{Q}(e^{2\pi i/n})$ for some n.

I conclude with a brief look at finite fields (to which I will return later). Clearly any such field F has prime characteristic $p > 0$; by looking at the dimension of F over its prime subfield $F_p = \mathbb{Z}_p$, we conclude that F has order a power p^n of p. At this point, we cannot quite say conversely for any prime power p^n that there is a field of order p^n, but I will later show that this is indeed the case (so that the hypothesis in a HW problem last quarter is always satisfied). For now observe that if a field F_m of order p^m lies in another one F_n of order p^n, then (again by looking at dimensions) one deduces that m divides n (since p^n must be a power of p^m). I will show conversely later that any field of order p_n indeed contains a subfield of order p^m if m divides n.

Note also that any field $F = F_n$ of order p^n is such that $x^{p^n-1} = 1$ for all nonzero $x \in F$, since x lies in a finite group of order $p^n - 1$. The polynomial $x^{p^n} - x$ then has every $y \in F$ as a root. This gives reason to believe that any two fields of order p^n are isomorphic; again we will show later that this is always the case.