Abstract Algebra. Math 6320. Bertram/Utah 2022-23.
Fields

We have seen several types of fields so far:

• The underlying fields $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ (for primes p) and the rational numbers $\mathbb{Q}$. One (and only one) of these is present as a subfield of each field k, determining the *characteristic* of each field k.

• The fields $\mathbb{R}$ of real numbers and $\mathbb{C}$ of complex numbers, the first of which is the *completion* of the field $\mathbb{Q}$ (with respect to absolute value) and the second of which is $\mathbb{R} + i\mathbb{R}$ (for a choice of square root i of -1).

• Function fields $k(x_1, ..., x_n)$ with coefficients in a fixed field, and more generally, the field of fractions $K(D)$ of an integral domain D, e.g.

$$D = k[x_1, ..., x_n]/P \text{ for a field } k \text{ and prime ideal } P$$

In algebraic geometry, these are the rational functions on an affine variety, and when P is *maximal*, e.g. when $n = 1$ and $P = \langle f(x) \rangle$, then the quotient domain is already a field (and the affine variety is a point).

Definition. (a) An inclusion $K \subset L$ of fields is a *field extension*, in which case L is an algebra and a vector space over K, and if the dimension of L is finite, then:

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

is the *degree* of the finite field extension.

(b) An element $\alpha \in L$ is *algebraic* over K if α is a root of a polynomial:

$$f(x) = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_0 \in K[x]$$

The field extension itself is algebraic if every element of L is algebraic over K.

(c) An element $\alpha \in L$ that is not algebraic over K is called *transcendental*.

Remarks. (i) The polynomial $f(x)$ in (b) may be chosen to be monic and irreducible, in which case it is uniquely determined by $\alpha \in L$.

(ii) A finite field extension is necessarily algebraic, but not vice versa.

Examples. • A finite field extension of $\mathbb{F}_p$ of degree d has $q = p^d$ elements.

• Each $\sqrt[n]{2}$ is algebraic over $\mathbb{Q}$, with irreducible polynomial $f(x) = x^n - 2$.

• $\pi \in \mathbb{R}$ is a transcendental element of the field extension $\mathbb{Q} \subset \mathbb{R}$.

Proposition 1. (a) The degrees of finite field extensions multiply:

$$[L : K] \cdot [K : F] = [L : F] \text{ for finite field extensions } F \subset K \subset L$$

(b) Let $\alpha \in L$ be algebraic over K for $K \subset L$ and consider the ring map:

$$\phi : K[x] \to L \text{ defined by } \phi(x) = \alpha \text{ and } \phi|_K = \mathrm{id}_K$$

Then the kernel of ϕ is the ideal generated by $f(x)$, the polynomial in (b) above and the image of ϕ is $K(\alpha) \subset L$, the smallest subfield of L that contains both the field K and the element $\alpha \in L$. Moreover, $\deg(f(x)) = [K(\alpha) : K]$.

As a corollary, we get a result reminiscent of Lagrange's Theorem for groups:

Corollary. If $[L : K] = d$ then $[F : K]$ divides d for all intermediate $K \subset F \subset L$. In particular, if $d = p$ is prime, then $K(\alpha) = L$ for all $\alpha \in L - K$.

Proof. If $\beta_1, ..., \beta_e$ are a basis for K as a vector space over F, and $\alpha_1, ..., \alpha_d$ are a basis for L as a vector space over K, then if:

$$\alpha = \sum_i k_i \alpha_i \text{ for } c_i \in K \text{ and } c_i = \sum_j f_{ij} \beta_j \text{ for } f_{ij} \in F$$

it follows that:

$$\alpha = \sum_{i,j} f_{i,j} \alpha_i \beta_j$$

so the elements $\alpha_i \beta_j$ span L as a vector space over K, and if:

$$0 = \sum_{i,j} f_{i,j} \alpha_i \beta_j = \sum_i k_i \alpha_i \text{ for } \sum_j f_{i,j} \beta_j = k_i$$

then $k_i = 0$ for all i (α_i is a basis) and then also $f_{i,j} = 0$ for all j (β_j is a basis). So the $\alpha_i \beta_j$ are linearly independent. This gives (a).

For (b), notice that the image of $K[x]$ is a domain, so the kernel is a prime ideal, which is a maximal ideal (in the PID $K[x]$), generated by an irreducible polynomial $f(x) \in K[x]$ of degree d satisfying $f(\alpha) = 0$. Any two such polynomials necessarily generate the same ideal, so $f(x)$ is unique, given that it is also monic, and a basis of $K(\alpha)$ as a vector space over K is given by $1, \alpha, ..., \alpha^{d-1}$. □

Definition. An extension $K \subset L$ *splits* a monic polynomial $f(x) \in K[x]$ if:

$$f(x) = \prod_{i=1}^{d} (x - \alpha_i) \text{ as a polynomial in } L[x]$$

Remark. In this definition, there is no requirement that $f(x) \in K[x]$ be irreducible. Thus, K itself splits all products of linear polynomials in $K[x]$.

Proposition 2. A splitting extension exists for each $f(x) \in K[x]$.

Proof. Let $g(x)$ be an irreducible factor of $f(x)$ of degree > 1 in the ring $K[x]$ (if no such factor exists, then we are done by the Remark). Construct the field:

$$L = K[x]/\langle g(x) \rangle \text{ and let } \alpha = \overline{x} \in L$$

Then in the ring L, the polynomial $g(x)$ has a linear factor $x - \alpha$ and the number of linear factors of $f(x)$, thought of as a polynomial in $L[x]$, is *at least* one more than the number of linear factors of $f(x)$ in $K[x]$. Replace K with L and repeat. □

Examples. (a) Consider the polynomial:

$$f(x) = x^n - 1 \in \mathbb{Q}[x]$$

Then $\mathbb{Q} \subset \mathbb{C}$ is a splitting extension, and if $\omega = e^{2\pi i/n}$, then $\mathbb{Q} \subset \mathbb{Q}(\omega)$ is already a splitting extension. The degree is not n, but rather the degree of the *cyclotomic* polynomial, i.e. the irreducible polynomial relation satisfied by ω.

(b) Consider instead the polynomial

$$g(x) = x^n - 2$$

Then this polynomial is irreducible, but $\mathbb{Q}(\sqrt[n]{2})$ only picks up two roots if n is even and only one root if n is odd. We do, however, obtain a splitting extension by tossing in ω at the next iteration, since all nth roots of 2 are in $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2})(\omega)$.

There is a really remarkable corollary to Proposition 2 in characteristic p.

Corollary. There exist fields $\mathbb{F}_q$ with **any** prime power $q = p^d$ ($d \geq 1$) of elements.

Proof. Let $\mathbb{F}_p \subset L$ be a splitting extension for $x^q - x$, and consider:

$$F = \{\alpha \in L \mid \alpha^q - \alpha = 0\} \subset L$$

Then $\mathbb{F}_p \subset F$ by Fermat's little theorem, since $a^{p^d} = (a^p)^{p^{d-1}} = a^{p^{d-1}} = ... = a$ for all $a \in \mathbb{F}_p$, and if $\alpha \in F$, then $-\alpha \in F$ and $1/\alpha \in F$; and if $\alpha_1, \alpha_2 \in F$, then $\alpha_1\alpha_2 \in F$ and $\alpha_1 + \alpha_2 \in F$, the latter, similarly, being a result of:

$$(\alpha_1 + \alpha_2)^{p^d} = ((\alpha_1 + \alpha_2)^p)^{p^{d-1}} = (\alpha_1 + \alpha_2)^{p^{d-1}} = \cdots = \alpha_1 + \alpha_2$$

by the binomial theorem (and the fact that $p\alpha = 0$ for all $\alpha \in F$).

Notice that the roots of $f(x) = x^q - x$ are *distinct* since the derivative satisfies:

$$f'(x) = -1 \text{ and any multiple root of } x^q - x \text{ is a root of } f'(x)$$

by the Leibniz rule for differentiation. Thus F is a field with $q = p^d$ elements! □

Proposition 3. If F is a field and $G \subset (F^*, \cdot)$ is a finite subgroup, then G is cyclic.

Proof. Let $|G| = n$. Then by Lagrange's Theorem, each $g \in G$ is a root of:

$$f(x) = x^n - 1 \in F[x]$$

so in particular the nth roots of 1 are distinct in F, and G **is** the (full) set of them. Next, we claim that there is a "primitive" root $g \in G$ generating the group G of nth roots of 1. Consider an element $h \in G$ generating a proper cyclic subgroup $C_d = H \subset G$. Then d divides n and H is the (full) set of roots of the polynomial $x^d - 1$ in F. Moreover, the *primitive* dth roots of 1 in F are the generators of H, and there are $\phi(d)$ generators of C_d, as we've discussed earlier. But:

$$n = \sum_{d|n} \phi(d)$$

as one can check, for instance, by considering the case $F = \mathbb{C}$, in which we already know that the group of nth roots of 1 is cyclic. It follows from this that:

$$\sum_{d|n, d \neq n} \phi(d) = n - \phi(n) < n$$

so G has extra nth roots, after accounting for all the non-primitive nth roots h, and each of those left-over roots generates G as a cyclic group. □

Corollary. There are irreducible polynomials of all degrees in $\mathbb{F}_p[x]$.

Proof. Fix $q = p^d$ and let $\mathbb{F}_q$ be a field with q elements. Since $(\mathbb{F}_q)^*$ is cyclic by the Proposition, it follows that $(\mathbb{F}_q)^*$ is generated by an element $\alpha \neq 0$, and then

$$\mathbb{F}_p(\alpha) = \mathbb{F}_q$$

and if we let $f(x) = 0$ be the monic, irreducible polynomial equation satisfied by the (necessarily algebraic) element $\alpha \in \mathbb{F}_q$, then $f(x)$ has degree d. □

Remark. The corollary only establishes the existence of the irreducible polynomials. It does not give any hints about how to find them.

Examples. The irreducible polynomials for $\mathbb{F}_2[x]$ of degrees $2, 3, 4$ are:

$$x^2 + x + 1,\ x^3 + x + 1,\ x^3 + x^2 + 1,\ x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$$

so we see that the irreducible polynomials in a given degree need not be unique. However, we will see that the **fields** with q elements are all isomorphic.

In $\mathbb{F}_3[x]$, we see that x^2+1 is irreducible, so

$$F = \mathbb{F}(\alpha) = \mathbb{F}_3[x]/\langle x^2+1\rangle \text{ is a field with 9 elements}$$

The generator $\alpha = x$ of this field does not generate the **group** F^* since

$$\alpha^2 = -1 \text{ and } \alpha^4 = 1 \text{ so } \alpha \text{ only has order 4}$$

Remark. However, once can check that $\alpha + 1$ generates F^*.

Here is an application of Proposition 1 to a problem from antiquity.

(Non)-Constructible Numbers. Mark points "0" and "1" in the plane and use a compass and (unmarked) straightedge to construct a sequence of additional points as intersection points of lines (through two previously constructed points) drawn with the help of the straightedge, and circles (centered at a previously constructed point with radius equal to the distance between two previously constructed points) drawn with the compass. A distance between two points constructed in this way is *constructible*.

Perpendicular lines (to a given line through a given point) can be constructed, all angles can be bisected, constructible lengths can be added (easy), multiplied and inverted (using similar triangles), so the constructible real numbers together with zero and their additive inverses are a *subfield* $K \subset \mathbb{R}$.

By means of the Pythagorean Theorem, one learns that if l is constructible, then $\sqrt{1+l^2}$, $\sqrt{2l}$ and $\sqrt{l}$ are constructible. From this it follows that every tower of quadratic (degree two) field extensions $\mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset \mathbb{R}$ can be realized by adjoining constructible square roots $\alpha_i = \sqrt{l_i}$ (via the quadratic formula).

Example. The (complex) primitive fifth root of unity $\zeta_5 = \cos(2\pi/5) + i\sin(2\pi/5)$ is a root of the irreducible (cyclotomic) polynomial

$$x^4 + x^3 + x^2 + x + 1$$

which factors as a product of quadratic polynomials:

$$(x^2 + \alpha x + 1)(x^2 + \beta x + 1) \text{ for } \alpha + \beta = 1, \alpha\beta = -1$$

These cannot be solved with integers, but they do have "golden mean" solutions:

$$\alpha = \frac{1-\sqrt{5}}{2},\ \beta = \frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$$

from which we deduce the fact (from a root of the α quadratic factor) that:

$$\cos(2\pi/5) = \frac{\sqrt{5}-1}{4} \in \mathbb{Q}(\sqrt{5}) \text{ and}$$

$$\sin(2\pi/5) = \frac{\sqrt{2(\sqrt{5}+5)}}{4} \in \mathbb{Q}(\sqrt{5})\left(\sqrt{2\sqrt{5}+5)}\right)$$

are both constructible.

Proposition 4. Every subfield $F \subset K$ that is a *finite* field extension of $\mathbb{Q}$ satisfies:

$$[F : \mathbb{Q}] = 2^d \text{ for some } d$$

Proof. We may construct perpendicular lines and therefore an (integer) grid on the plane. Given two points in the plane with coordinates in L for some finite field extension L of $\mathbb{Q}$, then by the Pythagorean theorem, the distance between the two points is in L or the field $L(\sqrt{l})$ for some $l = a^2 + b^2 \in L$.

If two lines are drawn through points with coordinates in L, their intersection point has coordinates in L, and if one such line and one or two circles are drawn centered at points wit coordinates in L with radii of the circle(s) in L, then the coordinates of the intersection points are also in $L(\sqrt{l})$ for some $l \in L$. Thus, (a basis of) F lies in a field extension $\mathbb{Q} \subset L$ obtained by a series of degree two extensions:

$$\mathbb{Q} \subset L_1 = \mathbb{Q}(\sqrt{l}_1) \subset L_2 = L_1(\sqrt{l}_2) \subset \cdots \subset L = L_{n-1}(\sqrt{l}_n)$$

so $\mathbb{Q} \subset F$ itself is a field extension of degree 2^d (dividing 2^n) by Proposition 1. $\square$

Corollary. (a) The cube may not be doubled with a straightedge and compass.

(b) There is no way to trisect a general angle with straightedge and compass.

Proof. If the unit cube may be doubled (in volume), i.e. if the side length of the cube satisfies $\sqrt[3]{2} \in K$, then it must be constructible in a finite number of steps, and then $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset F$ for some F, which is impossible by Proposition 1 since

$$3 = \mathbb{Q}([\sqrt[3]{2} : \mathbb{Q}] \text{ does not divide } 2^d \text{ for any } d$$

Similarly, if there were a method for trisecting a general angle, then it could be applied to the angle $\pi/3$ to construct $\pi/9$ (since the angle $\pi/3$ is easily constructed). Angles can be translated with a straightedge and compass so setting the vertex of the angle at the origin, with lower edge on the real line (through "0" and "1") and projecting to the axes would allow one to construct lengths:

$$\cos(\pi/9) \text{ and } \sin(\pi/9)$$

But $\alpha = \cos(\pi/9)$ is a root of the cubic polynomial equation:

$$f(x) = 8x^3 - 6x - 1 = 0$$

(which follows from the triple angle formula $\cos(3\theta) = 4\cos(\theta)^2 - 3\cos(\theta)$) so as above we conclude that $\mathbb{Q}(\cos(2\pi/9)) \not\subset F$ for any finite subfield of K, and we conclude that the angle $\pi/9$ cannot be constructed. So $\pi/3$ cannot be trisected.