August 29:

Math 432 Class Lecture Notes

- Fields, Characteristic, Prime Field
- Degree of a Field Extension
- Minimal Polynomials
- Lemma

0.1 The characteristic of a fields

A field is a set F together with two binary operations called addition and multiplication (written with standard algebraic notation and conventions) such that:

- Addition is commutative, associative, has an identity, and has inverses.
- Multiplication is commutative, associative, and has an identity; elements not equal to the additive identity have multiplicative inverses.
- The additive and multiplicative identities are distinct.
- Multiplication distributes over addition, i.e., $x(y+z) = xy + xz$ for all $x, y, z \in F$.

The additive and multiplicative identities in a field F will usually be denoted 0 and 1 respectively, though on occasion they will be denoted 0_F and 1_F if it is useful to emphasize that they are in a specific field F.

Let F be a field. Then there is a canonical ring homomorphism $h\colon \mathbf{Z} \to F$, basically defined by taking 1 to 1_F. More precisely we define

$$h(n) = n_F := 1_F + \cdots + 1_F, \quad (n \quad \text{times})$$

for nonnegative n (i.e., $h(n)$ is defined by recursion) and take $h(n) = -h(-n)$ for $n < 0$.

There are two things that can happen. The kernel of h might be trivial. By the isomorphism theorem "domain/kernel $\simeq$ image" it follows that the image is isomorphic to $\mathbf{Z}$. Since F "contains" integers r and s it contains their quotient r/s, and F contains (an isomorphic copy of) the rational numbers $\mathbf{Q}$. In this case the field is said to be of **characteristic** 0, written $\text{char}(F) = 0$, and the **prime field** of F, which is the smallest field contained in F, is $\mathbf{Q}$.

On the other hand the kernel of h might be a nonzero ideal in $\mathbf{Z}$. (An ideal in a ring is a nonempty subset closed under addition, and multiplication by arbitrary elements of the ring.) Any ideal in the ring of integers $\mathbf{Z}$ is "principal", i.e., the set of all multiples of a fixed integer:

$$(n) := n\mathbf{Z} = \{xn : x \in \mathbf{Z}\}.$$

(Any ring with this property is said to be a principal ideal domain, PID; the proof that $\mathbf{Z}$ is a PID is given in an Appendix below.) If $h(n) = 0$ and $n = rs$ then

$$h(n) = h(r)h(s) = 0$$

and since F is a field we conclude that $h(r) = 0$ or $h(s) = 0$. It follows that that $\ker(h)$ is of the form (p) where p is a prime.

By the aforementioned isomorphism theorem for ring maps, the image of h is isomorphic to the domain modulo the kernel, i.e.,

$$\text{im}(\mathbf{Z}) \simeq \mathbf{Z}/p\mathbf{Z}.$$

The image is (isomorphic to) the field $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ with p elements. In this case we say that F has characteristic p, written $\text{char}(F) = p$, and that the prime field of F is $\mathbf{F}_p$.

0.2 The degree of a field extension

Suppose that a field F is a subfield of a field E. We say that E is an **extension** of F. If we restrict the multiplication map on E to multiplication of elements of E by elements of F, then the resulting operation

$$\times : F \times E \to E$$

gives E the structure of a vector space over F (where addition of "vectors" is just the underlying field operation of addition on E; the vector space axioms are immediate consequences of the field axioms on E).

The dimension of this vector space is the **degree** of the extension, written

$$[E : F] := \dim_F(E).$$

An extension is **finite** if its degree is finite. In that case one can choose a basis $x_1, \cdots, x_n$ consisting of elements of E such that every element of E has a unique representation in the form

$$x = a_1 x_1 + \cdots + a_n x_n$$

where the a_i lie in the field F.

Example 1. The field $\mathbf{C}$ is an extension of the real numbers $\mathbf{R}$. If we forget how to multiply complex numbers by complex numbers, and merely remember how to multiply complex numbers by real numbers, we get the two-dimensional vector space $\mathbf{R}^2$; thus $[\mathbf{C} : \mathbf{R}] = 2$.

Example 2. If F is a finite field, then its prime field is $\mathbf{F}_p$ for some prime p, and F is a finite-dimensional vector space over $\mathbf{F}_p$. From the representation

$$x = a_1 x_1 + \cdots + a_n x_n$$

we see that F has p^n elements, where $n = [E : F]$, since each of the a_i can be chosen arbitrarily in $\mathbf{F}_p$.

A direct proof (see homework!) shows that if E is an extension of F and E' is an extension of F then

$$[E' : F] = [E' : E][E : F].$$

0.3 Minimal polynomials

Let E be an extension of F, and let α be an element of E.

Then there is a natural ring homomorphism, h, from the ring $F[x]$ of polynomials with coefficients in F to the field E defined by being the identity on F and taking the indeterminate x to α. Thus

$$h(f) = h(\sum a_i x^i) = \sum a_i h(x)^i = \sum a_i \alpha^i$$

and h is just the "evaluate at α map.

The kernel of h is an ideal in $F[x]$. The ring $F[x]$ is a PID (see appendix below). There are two cases.

If $\ker(h) = \{0\}$ is trivial, then α is said to be **transcendental** over F.

Example 3. By a highly nontrivial theorem, π is transcendental over $\mathbf{Q}$ and $[\mathbf{R} : \mathbf{Q}]$ is infinite. Similarly, e is transcendental over $\mathbf{Q}$.

If, on the other hand, $\ker(f)$ is nontrivial then

$$\mathrm{im}(f) \simeq F[x]/(f(x))$$

where the kernel of h is the principal ideal (f) of all multiples of a polynomial f. The polynomial f can be chosen canonically if we require it to be the unique element of the kernel that is monic (the coefficient of its highest degree term is 1); THEN f is said to the the **minimal** polynomial of α over F, and we will write this polynomial as $m_\alpha(x) \in F[x]$.

In this case α is said to be **algebraic** over F.

Moreover, in order for $F[x]/(m_\alpha)$ to be a field, the minimal polynomial m_α has to be irreducible (analogous to the earlier proof that the kernel of the map from $\mathbf{Z}$ to a field is generated by a prime).

It is easy to see that if $n = \deg(m_\alpha)$ then $1, \alpha, \alpha^2, \cdots \alpha^{n-1}$ is a basis for $\mathrm{im}(h)$ over F. (Hint: given an element $g(\alpha)$ of $\mathrm{im}(h)$, divide m_α into $g(x)$ to get a quotient and a remainder

$$g(x) = q(x)m_\alpha(x) + r(x)$$

and then evaluate at α.)

The smallest subfield of E that contains F and α is the set of all rational functions $f(\alpha)/g(\alpha)$, where g isn't divisible by m_α; this field is usually denoted $F(\alpha)$. However, by the remarks above on the basis of the field we see that the set of polynomials of degree less than $n = \deg(m_\alpha)$ is a field, and we conclude that

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \right\} = F[\alpha] = \{f(\alpha) : \deg(f) < n\}.$$

Example 4. $\mathbf{C} = \mathbf{R}(i)$ and $m_i(x) = x^2 + 1$.

Example 5. If $F = \mathbf{F}_2$ and $m_\alpha(x) = x^3 + x + 1$ then $\mathbf{F}_2(\alpha)$ is a field with 8 elements.

0.4 Appendix: Two lemmas

Lemma 6. Any ideal in $\mathbf{Z}$ is principal, i.e. an ideal I has the form

$$I = (n) = n\mathbf{Z}$$

for some integer n.

Sketch of Proof: If I is nontrivial let n be its least positive element. Then I contains the set of all multiples (n) of n. On the other hand, if x is any element of I then by dividing x by n we get

$$x = qn + r, \quad 0 \le r < n.$$

then $r = x - qn$ is in I. By the definition of n as the least positive element, we have $r = 0$ and therefore x is in (n) as desired.

Lemma 7. Any ideal in $\mathbf{F}[x]$ is principal.

Sketch: If an ideal I is nontrivial then it contains an element f of least possible degree. Divide f into an arbitrary element g of I

$$g = qf + r$$

and reason that I consists exactly of the multiples of f i.e., $I = (f)$ as desired.