

MATH 361: NUMBER THEORY — TENTH LECTURE

The subject of this lecture is finite fields.

1. ROOT FIELDS

Let \mathbf{k} be any field, and let $f(X) \in \mathbf{k}[X]$ be irreducible and have positive degree. We want to construct a superfield \mathbf{K} of \mathbf{k} in which f has a root. To do so, consider the quotient ring

$$R = \mathbf{k}[X]/\langle f \rangle,$$

where $\langle f \rangle$ is the principal ideal $f(X)\mathbf{k}[X]$ of $\mathbf{k}[X]$. That is, R is the usual ring of polynomials over \mathbf{k} subject to the additional rule $f(X) = 0$. Specifically, the ring-elements are cosets and the operations are

$$\begin{aligned}(g + \langle f \rangle) + (h + \langle f \rangle) &= (g + h) + \langle f \rangle, \\ (g + \langle f \rangle)(h + \langle f \rangle) &= gh + \langle f \rangle.\end{aligned}$$

The fact that f is irreducible gives R the structure of a field, not only a ring. The only matter in question is multiplicative inverses. To see that they exist, suppose that

$$g + \langle f \rangle \neq \langle f \rangle \quad \text{in } R.$$

The condition is that $g \notin \langle f \rangle$, i.e., $f \nmid g$. so $(f, g) = 1$ (because f is irreducible), and so there exist $F, G \in \mathbf{k}[X]$ such that

$$Ff + Gg = 1.$$

That is, $f \mid Gg - 1$, i.e., $Gg - 1 \in \langle f \rangle$, so that

$$Gg + \langle f \rangle = 1 + \langle f \rangle \quad \text{in } R.$$

That is,

$$(G + \langle f \rangle)(g + \langle f \rangle) = 1 + \langle f \rangle \quad \text{in } R,$$

showing that $G + \langle f \rangle$ inverts $g + \langle f \rangle$ in R .

Now use the field R to create a set \mathbf{K} of symbols that is a superset of \mathbf{k} and is in bijective correspondence with R . That is, there is a bijection

$$\sigma : R \xrightarrow{\sim} \mathbf{K}, \quad \sigma(a + \langle f \rangle) = a \text{ for all } a \in \mathbf{k}.$$

Endow \mathbf{K} with addition and multiplication operations that turn the set bijection into a field isomorphism. The operations on \mathbf{K} thus extend the operations on \mathbf{k} . Name a particular element of \mathbf{K} ,

$$r = \sigma(X + \langle f \rangle).$$

Then

$$\begin{aligned}
 f(r) &= f(\sigma(X + \langle f \rangle)) && \text{by definition of } r \\
 &= \sigma(f(X + \langle f \rangle)) && \text{since algebra passes through } \sigma \\
 &= \sigma(f(X) + \langle f \rangle) && \text{by the nature of algebra in } R \\
 &= \sigma(\langle f \rangle) && \text{by the nature of algebra in } R \\
 &= 0 && \text{by construction of } \sigma.
 \end{aligned}$$

Thus \mathbf{K} is a superfield of \mathbf{k} containing an element r such that $f(r) = 0$.

For example, since the polynomial $f(X) = X^3 - 2$ is irreducible over \mathbf{Q} , the corresponding quotient ring

$$R = \mathbf{Q}[X]/\langle X^3 - 2 \rangle = \{a + bX + cX^2 + \langle X^3 - 2 \rangle : a, b, c \in \mathbf{Q}\}$$

is a field. And from R we construct a field (denoted $\mathbf{Q}(r)$ or $\mathbf{Q}[r]$) such that $r^3 = 2$. Yes, we know that there exist cube roots of 2 in the superfield \mathbf{C} of \mathbf{Q} , but the construction given here is purely algebraic and makes no assumptions about the nature of the starting field \mathbf{k} to which we want to adjoin a root of a polynomial.

2. SPLITTING FIELDS

Again let \mathbf{k} be a field and consider a nonunit polynomial $f(X) \in \mathbf{k}[X]$. We can construct an extension field

$$\mathbf{k}_1 = \mathbf{k}(r_1),$$

where r_1 satisfies some irreducible factor of f . Let

$$f_2(X) = f(X)/(X - r_1) \in \mathbf{k}_1[X].$$

We can construct an extension field

$$\mathbf{k}_2 = \mathbf{k}_1(r_2) = \mathbf{k}(r_1, r_2),$$

where r_2 satisfies some irreducible factor of f_2 . Continue in this fashion until reaching a field where the original polynomial f factors down to linear terms. The resulting field is the **splitting field of f over \mathbf{k}** , denoted

$$\text{spl}_{\mathbf{k}}(f).$$

Continuing the example of the previous section, compute that

$$\frac{X^3 - 2}{X - r} = X^2 + rX + r^2 \quad \text{in } \mathbf{Q}(r)[X].$$

Let $s = rt$ where $t^3 = 1$ but $t \neq 1$. Then, working in $\mathbf{Q}(r, t)$ we have

$$s^2 + rs + r^2 = r^2t^2 + r^2t + r^2 = r^2(t^2 + t + 1) = r^2 \cdot 0 = 0,$$

Thus $s = rt$ satisfies the polynomial $X^2 + rX + r^2$, and now compute that

$$\frac{X^2 + rX + r^2}{X - rt} = X - rt^2 \quad \text{in } \mathbf{Q}(r, t)[X].$$

That is,

$$X^3 - 2 = (X - r)(X - rt)(X - rt^2) \in \mathbf{Q}(r, t)[X],$$

showing that

$$\text{spl}_{\mathbf{Q}}(X^3 - 2) = \mathbf{Q}(r, t).$$

3. EXAMPLES OF FINITE FIELDS

We already know the finite fields

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}, \quad p \text{ prime.}$$

For any positive integer n we can construct the extension field

$$\mathbf{K} = \text{spl}_{\mathbf{F}_p}(X^{p^n} - X).$$

Furthermore, *the roots of $X^{p^n} - X$ in \mathbf{K} form a subfield of \mathbf{K}* . To see this, check that if $a^{p^n} = a$ and $b^{p^n} = b$ then

$$\begin{aligned} (ab)^{p^n} &= a^{p^n} b^{p^n} = ab, \\ (a+b)^{p^n} &= a^{p^n} + b^{p^n} = a + b, \\ (a^{-1})^{p^n} &= (a^{p^n})^{-1} = a^{-1} \text{ if } a \neq 0, \\ (-a)^{p^n} &= (-1)^{p^n} a^{p^n} = -a \text{ (even if } p = 2). \end{aligned}$$

(The modulo p result that $(a+b)^p = a^p + b^p$ is sometimes called *the freshman's dream*.) Thus the splitting field \mathbf{K} is *exactly* the roots of $X^{p^n} - X$. The roots are distinct because the derivative

$$(X^{p^n} - X)' = -1$$

is nonzero, precluding multiple roots. Thus \mathbf{K} contains p^n elements. We give it a name,

$$\mathbf{F}_q = \text{spl}_{\mathbf{F}_p}(X^{p^n} - X) \quad \text{where } q = p^n.$$

4. EXHAUSTIVENESS OF THE EXAMPLES

In fact the fields

$$\mathbf{F}_q, \quad q = p^n, \quad n \geq 1$$

are the only finite fields, up to isomorphism. To see this, let \mathbf{K} be a finite field. The natural homomorphism

$$\mathbf{Z} \longrightarrow \mathbf{K}, \quad n \longmapsto n \cdot 1_{\mathbf{K}}$$

has for its kernel an ideal $I = n\mathbf{Z}$ of \mathbf{Z} such that

$$\mathbf{Z}/I \hookrightarrow \mathbf{K},$$

and so \mathbf{Z}/I is a finite integral domain. This forces $I = p\mathbf{Z}$ for some prime p , and so

$$\mathbf{F}_p \hookrightarrow \mathbf{K}.$$

Identify \mathbf{F}_p with its image in \mathbf{K} . Then \mathbf{K} is a finite-dimensional vector space over \mathbf{F}_p , so that $|\mathbf{K}| = p^n$ for some n . Every nonzero element $x \in \mathbf{K}^\times$ satisfies the condition $x^{p^n-1} = 1$, and so every element $x \in \mathbf{K}$ satisfies the condition $x^{p^n} = x$. In sum, $\mathbf{K} = \mathbf{F}_q$ up to isomorphism where again $q = p^n$.

5. CONTAINMENTS OF FINITE FIELDS

A natural question is:

For which $m, n \in \mathbf{Z}^+$ do we have $\mathbf{F}_{p^m} \subset \mathbf{F}_{p^n}$?

Assuming that the containment holds, the larger field is a vector space over the smaller one, and so $p^n = (p^m)^d = p^{md}$ for some d , showing that $m \mid n$. Conversely, if $m \mid n$ then

$$\frac{X^{p^n-1} - 1}{X^{p^m-1} - 1} = \sum_{i=0}^{\frac{p^n-1}{p^m-1}-1} X^{(p^m-1)i}.$$

(Note that $p^m - 1 \mid p^n - 1$ by the finite geometric sum formula; specifically, their quotient is $\sum_{j=0}^{n/m-1} p^{mj}$.) So

$$X^{p^m-1} - 1 \mid X^{p^n-1} - 1,$$

and so

$$\mathbf{F}_{p^m} \subset \mathbf{F}_{p^n}.$$

In sum,

$$\mathbf{F}_{p^m} \subset \mathbf{F}_{p^n} \iff m \mid n.$$

For example, \mathbf{F}_{27} is not a subfield of \mathbf{F}_{81} .

6. CYCLIC STRUCTURE

For any prime power $q = p^n$, the unit group \mathbf{F}_q^\times is cyclic. The proof is exactly the same as for $\mathbf{F}_p^\times = (\mathbf{Z}/p\mathbf{Z})^\times$. Either we quote the structure theorem for finitely-generated abelian groups, or we note that for any divisor d of $q - 1$,

$$X^{q-1} - 1 = (X^d - 1) \sum_{i=0}^{(q-1)/d-1} X^{di},$$

and the first factor on the right side has at most d roots while the second factor has at most $q - 1 - d$ roots. But the left side has a full contingent of $q - 1$ roots in \mathbf{F}_q . Now factor $q - 1$,

$$q - 1 = \prod r^{e_r}.$$

For each prime factor r , $X^{r^e} - 1$ has r^e roots and $X^{r^{e-1}} - 1$ has r^{e-1} roots, showing that there are $\phi(r)$ roots of order r^e . Thus there are $\phi(q - 1)$ elements of order $q - 1$ in \mathbf{F}_q . That is, \mathbf{F}_q^\times has $\phi(q - 1)$ generators.

7. EXAMPLES

To construct the field of $9 = 3^2$ elements we need an irreducible polynomial of degree 2 over \mathbf{F}_3 . The polynomial $X^2 + 1$ will do. Thus up to isomorphism,

$$\mathbf{F}_9 = \mathbf{F}_3[X]/\langle X^2 + 1 \rangle.$$

Here we have created \mathbf{F}_9 by adjoining a square root of -1 to \mathbf{F}_3 .

To construct the field of $16 = 2^4$ elements we need an irreducible polynomial of degree 4 over \mathbf{F}_2 .

(Note that the principle *no roots implies irreducible* is valid only for polynomials of degree 1, 2, or 3. For example, a quartic polynomial can have two quadratic factors.)

The polynomial $X^4 + X + 1$ works: it has no roots, and it doesn't factor into two quadratic terms because

$$(X^2 + aX + 1)(X^2 + bX + 1) = X^4 + (a + b)X^3 + abX^2 + (a + b)X + 1.$$

Thus, again up to isomorphism,

$$\begin{aligned} \mathbf{F}_{16} &= \mathbf{F}_2[X]/\langle X^4 + X + 1 \rangle \\ &= \mathbf{F}_2(r) \text{ where } r^4 + r + 1 = 0 \\ &= \{a + br + cr^2 + dr^3 : a, b, c, d \in \mathbf{F}_2\}. \end{aligned}$$

8. A REMARKABLE POLYNOMIAL FACTORIZATION

In general, to construct the field \mathbf{F}_q where $q = p^n$, we need an irreducible monic polynomial of degree n over \mathbf{F}_p . Are there such? How do we find them?

Fix a prime p and a positive integer n . For any $d \geq 1$, let $\text{MI}_p(d)$ denote the set of monic irreducible polynomials of degree d over \mathbf{F}_p . Then

$$X^{p^n} - X = \prod_{d|n} \prod_{f \in \text{MI}_p(d)} f(X) \quad \text{in } \mathbf{F}_p[X].$$

To establish the identity, consider any monic irreducible polynomial f , and let d denote its degree. We want to show that $f(X) \mid X^{p^n} - X$ if and only if $d \mid n$. Working in a field large enough to contain all roots of f and all roots of $X^{p^n} - X$, we have

$$f(X) \mid X^{p^n} - X \text{ in } \mathbf{F}_p[X] \iff \text{each root of } f(X) \text{ is a root of } X^{p^n} - X.$$

(The “ \Leftarrow ” direction is a little subtle, because conceivably f could have repeat roots. Indeed, there do exist so-called *inseparable* scenarios where the roots of an irreducible polynomial over a field do repeat. But in our context, if even *one* root a of f is a root of $X^{p^n} - X$ then $f(X) \mid X^{p^n} - X$. To see this, substitute a for X in the relation $X^{p^n} - X = q(X)f(X) + r(X)$ (where $r = 0$ or $\deg(r) < \deg f$) to get $r(a) = 0$. Thus $r = 0$ since otherwise a satisfies some irreducible factor of r along with satisfying the irreducible f , but a can not satisfy two distinct irreducible polynomials because then it would satisfy their gcd, which is the constant polynomial 1. Since $r = 0$, $f(X) \mid X^{p^n} - X$ as desired.) Recall that the set of roots of $X^{p^n} - X$ is precisely \mathbf{F}_{p^n} . Also, up to isomorphism, if we adjoin any root of f to \mathbf{F}_p then we get a field $\mathbf{F}_p(r) = \mathbf{F}_p[X]/\langle f \rangle = \mathbf{F}_{p^d}$ (recall that $d = \deg(f)$). Thus

$$f(X) \mid X^{p^n} - X \text{ in } \mathbf{F}_p[X] \iff \mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}.$$

And so, by the nature of finite field containments, we have shown exactly what we want: For any monic irreducible polynomial f over \mathbf{F}_p , letting d denote its degree,

$$f(X) \mid X^{p^n} - X \text{ in } \mathbf{F}_p[X] \iff d \mid n.$$

To count the monic irreducible polynomials over \mathbf{F}_p of a given degree, take the degrees of both sides of the identity

$$X^{p^n} - X = \prod_{d|n} \prod_{f \in \text{MI}_p(d)} f(X) \quad \text{in } \mathbf{F}_p[X]$$

to get

$$p^n = \sum_{d|n} d \cdot |\text{MI}_p(d)|.$$

By Möbius inversion,

$$|\text{MI}_p(n)| = \frac{1}{n} \sum_{d|n} \mu(n/d)p^d \quad (\text{where } \mu \text{ is the Möbius function}).$$

The sum on the right side is positive because it is a base- p expansion with top term p^n and the coefficients of the lower powers of p all in $\{0, \pm 1\}$. So $|\text{MI}_p(n)| > 0$ for all $n > 0$. That is, there do exist monic irreducible polynomials of every degree over every field \mathbf{F}_p .

For example, taking $p = 2$ and $n = 3$,

$$\begin{aligned} X^8 - X &= X(X^7 - 1) = X(X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1) \\ &= X(X - 1)(X^3 + X^2 + 1)(X^3 + X + 1) \pmod{2}, \end{aligned}$$

a product of two linear factors and two cubic factors. And the counting formula from the previous section gives the results that it must,

$$\begin{aligned} |\text{MI}_2(1)| &= \frac{1}{1} \mu(1)2^1 = 2, \\ |\text{MI}_2(3)| &= \frac{1}{3}(\mu(1)2^3 + \mu(3)2^1) = \frac{1}{3}(8 - 2) = 2. \end{aligned}$$

Similarly, taking $p = 3$ and $n = 2$,

$$\begin{aligned} X^9 - X &= X(X^8 - 1) = X(X^4 - 1)(X^4 + 1) \\ &= X(X^2 - 1)(X^2 + 1)(X^2 + X + 1)(X^2 - X + 1) \pmod{3} \\ &= X(X - 1)(X + 1)(X^2 + 1)(X^2 + X^2 + 1)(X^2 + X + 1), \end{aligned}$$

and

$$\begin{aligned} |\text{MI}_3(1)| &= \frac{1}{1} \mu(1)3^1 = 3, \\ |\text{MI}_3(2)| &= \frac{1}{2}(\mu(1)3^2 + \mu(3)3^1) = \frac{1}{2}(9 - 3) = 3. \end{aligned}$$

9. COMMON ERRORS

The finite field \mathbf{F}_q where $q = p^n$ is neither of the algebraic structures $\mathbf{Z}/q\mathbf{Z}$ and $(\mathbf{Z}/p\mathbf{Z})^n$ as a ring. As a vector space, $\mathbf{F}_q = \mathbf{F}_p^n$, but the ring (multiplicative) structure of \mathbf{F}_q is not that of $\mathbf{Z}/q\mathbf{Z}$ or of $(\mathbf{Z}/p\mathbf{Z})^n$.

The finite field \mathbf{F}_{p^m} is not a subfield of \mathbf{F}_{p^n} unless $m \mid n$, in which case it is.

10. GAUSS SUMS AGAIN

Let p and q be odd primes.

Working in \mathbf{F}_{q^2} , the multiplicative generator g has order $q^2 - 1 = 0 \pmod{8}$. Consequently, $g^{(q^2-1)/8}$ has order 8 and can serve as ζ_8 in the Gauss sum calculation of $(2/q)$.

Working in $\mathbf{F}_{q^{p-1}}$, the multiplicative generator g has order $q^{p-1} - 1 = 0 \pmod{p}$. Consequently, $g^{(q^{p-1}-1)/p}$ has order p and can serve as ζ_p in the Gauss sum proof of the main quadratic reciprocity law.