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 field $\mathbb{K}$ containing $\mathbf{k}$ 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, consider a nonzero element of R,

$$g + \langle f \rangle \neq \langle f \rangle.$$

This nonzeroness condition is $g \notin \langle f \rangle$, 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

$$Ff + Gg = 1.$$

Equivalently, $f \mid Gg - 1$, 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 $\mathbb{K}$ of symbols that contains $\mathbf{k}$ and is in bijective correspondence with R. That is, there is a bijection

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

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

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

Then

$$\begin{aligned}
f(r) &= f(\sigma(X + \langle f\rangle)) && \text{by definition of } r \\
&= \sigma(f(X + \langle f\rangle)) && \text{because algebra passes through } \sigma \\
&= \sigma(f(X) + \langle f\rangle) && \text{because } R \text{ inherits its algebra from } \mathbf{k}[X] \\
&= \sigma(\langle f\rangle) && \text{because } f(X) \in \langle f\rangle \\
&= 0 && \text{by construction of } \sigma.
\end{aligned}$$

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

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

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

is a field. And from R we construct a field (denoted $\mathbb{Q}(r)$ or $\mathbb{Q}[r]$) such that $r^3 = 2$. Yes, we know that there exist cube roots of 2 in the superfield $\mathbb{C}$ of $\mathbb{Q}$, 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. Thus

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

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 k**, denoted

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

Continuing the example of the previous section, compute that

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

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

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

That is,

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

showing that

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

3. Examples of Finite Fields

We already know the finite fields

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

For any positive integer n we can construct the extension field

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

Furthermore, *the roots of* $X^{p^n} - X$ *in* $\mathbb{K}$ *form a subfield of* $\mathbb{K}$. 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*, but this derisive label can distract a person from appreciating the important idea that *raising to the pth power is a ring homomorphism in characteristic p that doesn't exist in characteristic* 0. In any case, the splitting field $\mathbb{K}$ consists of *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. Altogether, $\mathbb{K}$ contains p^n elements. We give it a name,

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

4. Exhaustiveness of the Examples

In fact the fields

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

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

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

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

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

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

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

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

5. Containments of Finite Fields

A natural question is:

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

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 $p^m - 1 \mid p^n - 1$ by the finite geometric sum formula, their quotient being $q = \sum_{i=0}^{n/m-1} p^{mi}$, and then in turn

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

That is, $X^{p^m-1} - 1 \mid X^{p^n-1} - 1$, and so $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. Altogether,

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

For instance, $\mathbb{F}_{27}$ is not a subfield of $\mathbb{F}_{81}$.

6. Cyclic Structure

For any prime power $q = p^n$, the unit group $\mathbb{F}_q^\times$ is cyclic. The proof is exactly the same as for $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$. One argument is to quote the structure theorem for finitely-generated abelian groups. Alternatively, 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 left side has a full contingent of $q-1$ roots in $\mathbb{F}_q$, forcing each factor on the right to have as many roots as its degree, so that in particular the first factor has d roots. 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 $\phi(r^e)$ roots of order r^e. Thus there are $\phi(q-1)$ elements of order $q-1$ in $\mathbb{F}_q$. That is, $\mathbb{F}_q^\times$ 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 $\mathbb{F}_3$. The polynomial $X^2 + 1$ will do. Thus up to isomorphism,

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

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

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

> Note that the principle *no roots implies irreducible* is valid only for polynomials of degree 2 and 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 (recalling that $2 = 0$ here)

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

Thus, again up to isomorphism,

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

8. A Remarkable Polynomial Factorization

Fix a prime p and a positive integer n. To construct the field $\mathbb{F}_{p^n}$, we need an irreducible monic polynomial of degree n over $\mathbb{F}_p$. Are there such? How do we find them?

For any $d \geq 1$, let $\mathrm{MI}_p(d)$ denote the set of monic irreducible polynomials over $\mathbb{F}_p$ of degree d. We will show that

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

To establish the identity, let $F_n(X) = X^{p^n} - X$, so that the field $\mathbb{F}_{p^n}$ consists of a set of roots of F_n. The polynomial $F_n(X)$ factors uniquely in $\mathbb{F}_p[X]$ as a product of monic irreducibles of positive degree, with no repeat factors because $F_n'(X) = -1$.

- Each monic irreducible factor f of F_n, lying in $\mathrm{MI}_p(d)$ for some d, has a root α in $\mathbb{F}_{p^n}$, and the subfield $\mathbb{F}_p(\alpha)$ of $\mathbb{F}_{p^n}$ has order p^d. Thus d divides n.
- Conversely, for each divisor d of n and each $f \in \mathrm{MI}_p(d)$, each root α of f generates a field $\mathbb{F}_p(\alpha)$ of order p^d; so $\alpha^{p^d-1} = 1$, from which $\alpha^{p^n-1} = 1$ because $p^d - 1 \mid p^n - 1$, giving $F_n(\alpha) = 0$. Thus f divides F_n.

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

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

to get

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

By Möbius inversion, with μ the Möbius function as usual,

$$|\mathrm{MI}_p(n)| = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d.$$

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 $|\mathrm{MI}_p(n)| > 0$ for all $n > 0$. That is, there do exist monic irreducible polynomials of every degree over every field $\mathbb{F}_p$.

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

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

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

$$|\mathrm{MI}_2(1)| = \frac{1}{1}\mu(1)2^1 = 2,$$
$$|\mathrm{MI}_2(3)| = \frac{1}{3}(\mu(1)2^3 + \mu(3)2^1) = \frac{1}{3}(8-2) = 2.$$

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

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

and

$$|\mathrm{MI}_3(1)| = \frac{1}{1}\mu(1)3^1 = 3,$$
$$|\mathrm{MI}_3(2)| = \frac{1}{2}(\mu(1)3^2 + \mu(3)3^1) = \frac{1}{2}(9-3) = 3.$$

9. Common Errors

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

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

10. Primes in Extensions

We return to a question from the very first lecture: Does a given odd prime p factor or remain prime in the Gaussian integer ring $\mathbb{Z}[i]$? Equivalently, is the quotient ring $\mathbb{Z}[i]/p\mathbb{Z}[i] = \mathbb{Z}[i]/\langle p\rangle$ an integral domain? Compute,

$$\mathbb{Z}[i]/\langle p\rangle \approx \mathbb{Z}[X]/\langle p, X^2+1\rangle \approx \mathbb{F}_p[X]/\langle X^2+1\rangle.$$

Thus the question is whether X^2+1 is reducible or irreducible in $\mathbb{F}_p[X]$, which is to say whether the Legendre symbol $(-1/p)$ is 1 or -1. By Euler's Criterion, $(-1/p) = (-1)^{(p-1)/2}$, so the 1 mod 4 primes p factor in $\mathbb{Z}[i]$ while the 3 mod 4 primes p don't. Returning to quotient ring structure, we have shown that

$$\mathbb{Z}[i]/\langle p\rangle \approx \mathbb{F}_p[X]/\langle X-r\rangle \times \mathbb{F}_p[X]/\langle X+r\rangle, \quad p = 1 \bmod 4,$$

where $r^2 = -1 \bmod p$. Take, for example, $p = 5$, and create two ideals of $\mathbb{Z}[i]$ modeled on the two polynomial ideals in the previous display with $r = 2$.

$$I_1 = \langle 5, i-2\rangle, \qquad I_2 = \langle 5, i+2\rangle.$$

Their product is generated by the pairwise products of their generators,

$$I_1 I_2 = \langle 5^2, 5(i-2), 5(i+2), -5\rangle.$$

Each generator of $I_1 I_2$ is a multiple of 5 in $\mathbb{Z}[i]$, and 5 is a $\mathbb{Z}[i]$-linear combination of the generators. That is, the methods being illustrated here have factored 5 as an ideal of $\mathbb{Z}[i]$,

$$I_1 I_2 = 5\mathbb{Z}[i].$$

The previous example deliberately overlooks the elementwise factorization $5 = (2-i)(2+i)$. Here is another example. For any odd prime $p \neq 19$,

$$\mathbb{Z}[\sqrt{19}]/\langle p\rangle \approx \mathbb{Z}[X]/\langle p, X^2-19\rangle \approx \mathbb{F}_p[X]/\langle X^2-19\rangle,$$

and this ring decomposes if $(19/p) = 1$. For example, $(19/5) = 1$ because $2^2 = 4 = 19 \bmod 5$, and so we compute that in $\mathbb{Z}[\sqrt{19}]$,

$$\langle 5, \sqrt{19}-2\rangle \cdot \langle 5, \sqrt{19}+2\rangle = \langle 5^2, 5(\sqrt{19}-2), 5(\sqrt{19}+2), 15\rangle = 5\mathbb{Z}[\sqrt{19}].$$

Here we have factored the ideal $5\mathbb{Z}[\sqrt{19}]$ without factoring the element 5 itself.

Similarly, letting q be an odd prime and $\Phi_q(X)$ the qth cyclotomic polynomial (the smallest monic polynomial over $\mathbb{Z}$ satisfied by ζ_q), compute for any odd prime $p \neq q$,

$$\mathbb{Z}[\zeta_q]/\langle p\rangle \approx \mathbb{Z}[X]/\langle p, \Phi_q(X)\rangle \approx \mathbb{F}_p[X]/\langle \Phi_q(X)\rangle.$$

Thus if

$$\Phi_q(X) = \prod_{i=1}^{g} \varphi_i(X)^{e_i} \quad \text{in } \mathbb{F}_p[X]$$

then the Sun Ze Theorem gives the corresponding ring decomposition

$$\mathbb{Z}[\zeta_q]/\langle p\rangle \approx \prod_{i=1}^{g} \mathbb{F}_p[X]/\langle \varphi_i(X)^{e_i}\rangle,$$

and plausibly this decomposition somehow indicates the decomposition of p in $\mathbb{Z}[\zeta_q]$. Factoring $\Phi_q(X)$ in $\mathbb{F}_p[X]$ is a finite problem, so these methods finite-ize the determination of how p decomposes in $\mathbb{Z}[\zeta_q]$.