Fundamental Theorem of Algebra

Lemma: If $f(x)$ is a polynomial over $\mathrm{GF}(q) \subseteq \mathrm{GF}(Q)$, then β is a zero of $f(x)$ if and only if $x - \beta$ is a divisor of $f(x)$.

Proof: By the division algorithm,

$$f(x) = q(x)(x-\beta) + r(x)\,, \ \text{ where } \ \deg r(x) < \deg(x-\beta) = 1\,.$$

Thus $\deg r(x) \leq 0$, so $r(x)$ is a constant polynomial, $r(x) = r_0$. Therefore

$$r_0 = r(\beta) = f(\beta) - q(\beta)(\beta - \beta) = f(\beta)\,,$$

hence $f(x)$ is a multiple of $x - \beta$ if and only if $f(\beta) = r_0 = 0$.

Lemma: A polynomial $f(x)$ of degree n over a field has at most n zeroes.

Proof: Each zero of $f(x)$ corresponds to a linear factor of $f(x)$.
Because $\deg f(x) = n$, there are at most n linear factors.
Thus there are at most n distinct zeroes (including multiple zeroes).

Blahut (Theorem 4.3.9) calls this the Fundamental Theorem of Algebra. Gauss's FTA: every polynomial equation with complex coefficients and degree ≥ 1 has at least one complex root.

Examples of factors and zeroes

Example: Polynomials of degree 2 over $\mathrm{GF}(2)$:

$$x^2 = x \cdot x\,,\; x^2+1 = (x+1)(x+1)\,,\; x^2+x = x(x+1)\,,\; x^2+x+1$$

The only prime polynomial over $\mathrm{GF}(2)$ of degree 2 has zeroes in $\mathrm{GF}(4)$:

$$(x+\beta)(x+\delta) = x^2 + (\beta+\delta)x + \beta\delta = x^2+x+1\,.$$

Whether a polynomial is prime depends on what coefficients are allowed.

Example: $\mathrm{GF}(2^4)$ can be represented as polynomials in α of degree < 4, where α is a zero of the prime (over $\mathrm{GF}(2)$) polynomial x^4+x+1.

Therefore $x+\alpha$ is a factor of x^4+x+1 over $\mathrm{GF}(2^4)$.

Another zero is a^2:

$$x^4+x+1\big|_{\alpha^2} = (\alpha^2)^4 + \alpha^2 + 1 = (\alpha^4+\alpha+1)^2 = 0^2 = 0\,.$$

Similarly, $\alpha^4 = (\alpha^2)^2$ and $\alpha^8 = (\alpha^4)^2$ are zeroes. Over $\mathrm{GF}(16)$

$$x^4+x+1 = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)\,.$$

$\mathbf{GF}(\boldsymbol{Q})$ consists of zeroes of $\boldsymbol{x^Q - x}$

The order of the multiplicative group of $\mathrm{GF}(Q)$ is $Q-1$.

Let e be the order of β of $\mathrm{GF}(Q)$. By Lagrange's theorem, $e \mid (Q-1)$, so

$$\beta^{Q-1} = \beta^{e\cdot(Q-1)/e} = (\beta^e)^{(Q-1)/e} = 1^{(Q-1)/e} = 1\,.$$

This shows that every *nonzero* element of $\mathrm{GF}(Q)$ is a zero of $x^{Q-1}-1$.

The special case of 0 requires one more factor, $x-0$, which yields

$$x(x^{Q-1}-1) = x^Q - x\,.$$

This polynomial has at most Q zeroes. Thus $\mathrm{GF}(Q) =$ zeroes of $x^Q - x$.

Similarly, for any subfield, $\mathrm{GF}(q) =$ zeroes of $x^q - x$. Factorizations:

$$x^Q - x = \prod_{\beta\in\mathrm{GF}(Q)} (x-\beta)\,, \quad x^q - x = \prod_{\beta\in\mathrm{GF}(q)} (x-\beta)$$

$$x^Q - x = x(x^{Q-1}-1) = x(x^{q-1}-1)(x^{Q-1-(q-1)} + \cdots + x^{q-1} + 1)$$

The last equation holds because $(q-1) \mid (Q-1)$.

Minimal polynomials

Let $\beta \in \mathrm{GF}(Q)$ and $\mathrm{GF}(q) \subseteq \mathrm{GF}(Q)$.

Definition: The *minimal polynomial over* $\mathrm{GF}(q)$ of β is the monic polynomial $f(x)$ over $\mathrm{GF}(q)$ of smallest degree such that $f(\beta) = 0$.

Example: $\mathrm{GF}(4) = \{0, 1, \beta, \delta\}$. Minimal polynomials over $\mathrm{GF}(2)$:

$$0 \to x\,, \quad 1 \to x + 1\,, \quad \beta, \delta \to x^2 + x + 1$$

Theorem: Suppose $\mathrm{GF}(q) \subseteq \mathrm{GF}(Q)$ where $Q = q^m$.

1. Every β in $\mathrm{GF}(Q)$ has minimal polynomial over $\mathrm{GF}(q)$ of degree $\le m$.
2. The minimal polynomial is unique.
3. The minimal polynomial is prime over $\mathrm{GF}(q)$.
4. If $g(x)$ is a polynomial over $\mathrm{GF}(q)$ such that $g(\beta) = 0$ then $f(x) \mid g(x)$.

Every β in $\mathrm{GF}(Q)$ is a zero of $x^Q - x$, whose coefficients $(1, 0, -1)$ belong to $\mathrm{GF}(q)$.
So the minimal polynomial exists and has degree $\le Q$.

Minimal polynomials (cont.)

Proof:

1. $\mathrm{GF}(Q)$ is a vector space over $\mathrm{GF}(q)$ of dimension m.

   Therefore any set of $m+1$ elements is linearly dependent over $\mathrm{GF}(q)$.

   In particular, consider the first $m+1$ powers of β:

   $$\{1,\ \beta,\ \beta^2,\ \ldots,\beta^m\}$$

   There exist $m+1$ scalars $f_0, f_1, \ldots, f_m$ in $\mathrm{GF}(q)$, not all 0, such that

   $$f_0 \cdot 1 + f_1 \cdot \beta + \cdots + f_m \cdot \beta^m = 0 = f(\beta)\,.$$

   In other words, β is a zero of

   $$f(x) = f_0 + f_1 x + \cdots + f_m x^m\,,$$

   which is a nonzero polynomial over $\mathrm{GF}(q)$ of degree $\leq m$.

   Therefore the minimal polynomial of β has degree $\leq m$.

Minimal polynomials (cont.)

2. If $f_1(x)$ and $f_2(x)$ are distinct minimal polynomials of the same degree, then
$$f(x) = f_1(x) - f_2(x)$$
is a nonzero polynomial of smaller degree. Since $f(\beta) = 0$, we have a contradiction.

3. If $f(x) = f_1(x)f_2(x)$ has proper divisors, then
$$f(\beta) = f_1(\beta)f_2(\beta) = 0 \implies \text{either } f_1(\beta) = 0 \text{ or } f_2(\beta) = 0\,,$$
contradicting the minimality of $f(x)$.

4. By the division algorithm,
$$g(x) = q(x)f(x) + r(x)\,, \quad \text{where} \quad \deg r(x) < \deg f(x)\,.$$
If $g(\beta) = 0$ then
$$r(\beta) = g(\beta) - q(\beta)f(\beta) = 0\,.$$
If $r(x) \neq 0$ then $f(x)$ is not minimal. Thus $r(x) = 0 \implies f(x) \mid g(x)$.

Conjugates

Definition: The *conjugates over* $\mathrm{GF}(q)$ of β are the zeroes of the minimal polynomial over $\mathrm{GF}(q)$ of β (including β itself).

Example: $\mathrm{GF}(4) = \{0, 1, \beta, \delta\}$. Then β and $\delta = \beta + 1$ are conjugates since

$$(x+\beta)(x+\delta) \;=\; x^2 + (\beta+\delta)x + \beta\delta \;=\; x^2 + x + 1\,.$$

Example: $\mathrm{GF}(8) = \{0,\, 1,\, \alpha,\, \alpha{+}1,\, \alpha^2,\, \ldots,\, 1{+}\alpha{+}\alpha^2\}$, where $\alpha^3 = \alpha + 1$.

The minimal polynomial of α is $f(x) = x^3 + x + 1$. Another zero is α^2:

$$f(\alpha^2) = (\alpha^2)^3 + \alpha^2 + 1 = (\alpha^3 + \alpha + 1)^2 = 0$$

So α^2 and $\alpha^4 = \alpha + \alpha^2$ are conjugates of α, which gives the factorization:

$$x^3 + x + 1 = (x+\alpha)(x+\alpha^2)(x+\alpha^4) = (x + \begin{bmatrix}0\\1\\0\end{bmatrix})(x + \begin{bmatrix}0\\0\\1\end{bmatrix})(x + \begin{bmatrix}0\\1\\1\end{bmatrix})$$

(The 3-tuple representations of α^i have lsb in the first row.)

Binomial coefficients and prime numbers

Lemma: If p is prime and $0 < k < p$ then p is a divisor of $\binom{p}{k}$.

Proof: $\binom{p}{k} = \dfrac{p(p-1)\cdots(p-k+1)}{k!} = p \cdot \dfrac{(p-1)\cdots(p-k+1)}{k!}$

Denominator $k!$ divides $p \cdot (p-1)\cdots(p-k+1)$ and is relatively prime to p.

Therefore $k!$ divides $(p-1)\cdots(p-k+1)$, so $\binom{p}{k}$ is a multiple of p.

Lemma: In $\mathrm{GF}(p^m)$, $(a+b)^p = a^p + b^p$.

Proof: By the binomial theorem,

$$(a+b)^p = a^p \ + \ \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k \ + \ b^p = a^p + b^p\,,$$

since $\binom{p}{k}$ is multiple of p ($0 < k < p$) and in $\mathrm{GF}(p^m)$ multiples of p are 0.

Corollary: In $\mathrm{GF}(2^m)$, $(a+b)^2 = a^2 + b^2$. In other words, squaring is linear.

Corollary: In $\mathrm{GF}(q)$ ($q = p^m$), $(a+b)^q = (a+b)^{p^m} = a^{p^m} + b^{p^m} = a^q + b^q$.

Conjugates of β

Theorem: The conjugates of β over $\mathrm{GF}(q)$ are

$$\beta,\ \beta^q,\ \beta^{q^2},\ \ldots\ ,\ \beta^{q^{r-1}}$$

where r is the least positive integer such that $\beta^{q^r} = \beta$.

Note: $\beta^{q^m} = \beta^Q = \beta$, so $r \le m$. In fact, we will see that $r \mid m$.

Proof: First we show that β^{q^i} are conjugates. For any $f(x)$ over $\mathrm{GF}(q)$

$$\begin{aligned} f(\beta)^q &= (f_0 + f_1\beta + f_2\beta^2 + \cdots)^q \\ &= f_0^q + f_1^q\beta^q + f_2^q\beta^{2q} + \cdots \\ &= f_0 + f_1\beta^q + f_2\beta^{2q} + \cdots = f(\beta^q)\,, \end{aligned}$$

since $f_i^q = f_i$ for coefficients in $\mathrm{GF}(q)$.

If $f(x)$ is the minimal polynomial of β, then

$$f(\beta^q) = f(\beta)^q = 0^q = 0\,.$$

Therefore β^q is a zero of the minimal polynomial and so is a conjugate of β.

Conjugates of β (cont.)

Next we show that *all* conjugates of β are in $\{\beta^{q^i}\}$. Consider the product

$$f(x) = (x-\beta)(x-\beta^q)(x-\beta^{q^2})\cdots(x-\beta^{q^{r-1}})$$

of linear factors for all the distinct conjugates of β of the form β^{q^i}:

$$\begin{aligned} f(x)^q &= (x^q-\beta^q)(x^q-\beta^{q^2})\cdots(x^q-\beta^{q^r}) \\ &= (x^q-\beta^q)(x^q-\beta^{q^2})\cdots(x^q-\beta) = f(x^q) \end{aligned}$$

since $\beta^{q^r} = \beta$. Therefore

$$f_0^q \;+\; f_1^q x^q \;+\; \cdots \;+\; f_r^q x^{q^r} \;=\; f_0 \;+\; f_1 x^q \;+\; \cdots \;+\; f_r x^{q^r}$$

Since $f_i^q = f_i$, all the coefficients of $f(x)$ are in $\mathrm{GF}(q)$.

Obviously, β is a zero of $f(x)$. Any polynomial over $\mathrm{GF}(q)$ that has β as zero must have the same r linear factors.

Therefore $f(x)$ is a divisor of every such polynomial, hence $f(x)$ is minimal.

Conjugates: summary

The conjugates of β are the zeroes of the minimal polynomial of β.

The conjugates of β over $\mathrm{GF}(q)$ are β, β^q, $\beta^{q^2}, \ldots, \beta^{q^{r-1}}$.

The minimal polynomial of β is prime over $\mathrm{GF}(q)$ but factors over any field $\mathrm{GF}(Q)$ that contains β (and hence its conjugates):

$$f(x) = (x-\beta)(x-\beta^q)(x-\beta^{q^2})\cdots(x-\beta^{q^{r-1}})$$

If $\beta \in \mathrm{GF}(q^m)$ then β has at most m conjugates (including itself).

If β has r conjugates, then the linear subspace of $\mathrm{GF}(q^m)$ spanned by

$$\{1, \beta, \beta^2, \ldots, \beta^{r-1}\}$$

is a field with q^r elements. Reciprocals exist because $f(x)$ is prime.

If $r < m$ then β belongs to $\mathrm{GF}(q^r)$, a proper subfield of $\mathrm{GF}(q^m)$.

Since $\mathrm{GF}(q^m)$ is a vector space over $\mathrm{GF}(q^r)$, we conclude that $r \mid m$.

Euler phi function

The *Euler phi function* $\phi(n)$ is the number of integers between 0 and n that are relatively prime to n.

We can express $\phi(n)$ in terms of the factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$:

- if p is prime then $\phi(p) = p - 1$ ($1, 2, \ldots, p-1$ are coprime to p)
- if p is prime then $\phi(p^e) = p^e - p^{e-1}$ (multiples of p are not coprime).
- $\phi(n)$ is *multiplicative*; i.e., if $\gcd(r,s) = 1$ then $\phi(rs) = \phi(r)\phi(s)$.

Combining these facts, we obtain the final formula:

$$\phi(n) = \begin{cases} p-1 & \text{if } n = p \text{ is a prime} \\ (p-1)p^{e-1} = \left(1-\dfrac{1}{p}\right)p^e & \text{if } n = p^e \text{ is power of prime} \\ \phi(p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}) = \displaystyle\prod_{i=1}^{t} (p_i - 1) p_i^{e_i - 1} & \text{in general} \end{cases}$$

Primitive elements

Fact: Multiplicative group of the finite field $\mathrm{GF}(q)$ is cyclic of order $q-1$.

A *primitive element* of $\mathrm{GF}(q)$ is a generator of the multiplicative group

- Let α be a primitive element of $\mathrm{GF}(q)$. All primitive elements of $\mathrm{GF}(Q)$ are powers α^i where $\gcd(i, q-1) = 1$.
  - $1 = ai + b(q-1) \implies \alpha = \alpha^{ai+b(q-1)} = \alpha^{ai} = (\alpha^i)^a$.
  - Conversely, if $\gcd(i, q-1) = d > 1$ then the order of α^i is $\dfrac{q-1}{d} < q-1$.
- In general, $\mathrm{GF}(q)$ has $\phi(q-1)$ primitive elements.
- If $q-1$ is prime then there are $q-2$ primitive elements. (This is possible only for $q = 3$ and for $q = 2^m$ with m odd.)
- $\mathrm{GF}(4)$, $\mathrm{GF}(8)$, $\mathrm{GF}(16)$, $\mathrm{GF}(32)$ have respectively 2, 6, 8, 30 primitive elements.

The proof that every finite field has a primitive element uses a lemma about groups: if for every divisor d of the order of a group there are at most d elements of order dividing d, then the group is cyclic.

Primitive elements and polynomials

Let α be a primitive element of $\mathrm{GF}(Q)$ and $\mathrm{GF}(q)$ be a subfield of $\mathrm{GF}(Q)$. Let $f(x)$ be the minimal polynomial over $\mathrm{GF}(q)$ of α and $m = \deg f(x)$.

- Every nonzero element of $\mathrm{GF}(Q)$ is a power of α:
$$\mathrm{GF}(Q) = \{1,\, \alpha,\, \alpha^2,\, \ldots,\, \alpha^{Q-2}\}$$
- Every element of $\mathrm{GF}(Q)$ is a polynomial in α of degree $\leq m-1$:
$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1}$$
where $b_0, b_1, \ldots, b_{m-1}$ are coefficients from $\mathrm{GF}(q)$.
- Multiplication by α of a polynomial in α uses the equation $f(\alpha) = 0$:
$$\alpha(b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}) =$$
$$b_0\alpha + b_1\alpha^2 + \cdots + b_{m-2}\alpha^{m-1} - b_{m-1}(f_0 + \cdots + f_{m-1}\alpha^{m-1})$$
- A *primitive polynomial* is the minimal polynomial of a primitive element. Equivalently: monic $f(x)$ of degree m is primitive if the order of $f(x)$ is $q^m - 1$; i.e., the smallest n such that $x^n = 1 \bmod f(x)$ is $n = q^m - 1$.