A summary of MT5826 — Finite Fields

Max Neunhöffer

22nd April 2013

1 Cyclic groups

A group G is called *cyclic*, if there is a $g \in G$ with $G = \{g^z \mid z \in \mathbb{Z}\} =: \langle g \rangle$.
Let $G = \langle g \rangle$ and $|G| = m < \infty$, then there is a bijection:

$$\begin{array}{ccc} \{\text{divisors of } m\} & \longleftrightarrow & \{\text{subgroups of } G\} \\ d & \longmapsto & \left\langle g^{m/d} \right\rangle \end{array} \qquad \text{(of order } d\text{)}$$

If $h \in G$ has order k, then h^ℓ has order $k/\gcd(\ell, k)$.

2 Rings and fields

Definition: Ring, ring with identity, integral domain, division ring, field.
Theorem: Every finite integral domain is a field.
Definition: Let R be a commutative ring with identity and I an ideal in R, then

$$R/I := \{r + I \mid r \in R\} \quad \text{where} \quad r + I := \{r + i \mid i \in I\}.$$

We define $(a + I) + (b + I) := (a + b) + I$ and $(a + I) \cdot (b + I) := (a \cdot b) + I$. In particular: $\mathbb{Z}/(n)$ and $F[x]/(f)$, where $(n) = \{nz \mid z \in \mathbb{Z}\}$ and $(f) = \{fg \mid g \in F[x]\}$ and F a field.
Lemma: $\mathbb{Z}/(n)$ is a field iff n is a prime and $F[x]/(f)$ is an extension field of F iff f is irreducible.
Definition/Proposition: Let R be a ring, the smallest $k \in \mathbb{N}$ with $kr = \underbrace{r + r + \cdots + r}_{k \text{ times}} = 0$ is called the *characteristic of* R. If there is no such k, the characteristic is 0. If R is an integral domain, then the characteristic is 0 or a prime. $\mathbb{F}_p := \mathbb{Z}/(p)$ has characteristic p, the rationals $\mathbb{Q}$ have characteristic 0, $F[x]/(f)$ has the same characteristic as F.
Definition: *The prime field* of a field F is the intersection of all its subfield, it is either $\mathbb{F}_p$ or $\mathbb{Q}$, depending on the characteristic of F. *A prime field* is one with no proper subfields. The prime field of any field is a prime field.

3 Polynomials and roots

Definition: Let $f \in F[x]$ and let E be an extension field of F. Then $a \in E$ is called a *root of* f, if $f(a) = 0$. If $a \in E$ is the root of some polynomial $f \in F[x]$, then a is called *algebraic over* F. In that case there is a unique monic polynomial $g \in F[x]$ of least degree with $g(a) = 0$, it is called the *minimal polynomial of* a *over* F and it is always irreducible over F.
Lemma: In this situation, $f(a) = 0$ for some $f \in F[x]$ if and only if g divides f in $F[x]$. This covers the case that $a \in F$, then $g = x - a$.
Definition: A root $a \in F$ of $f \in F[x]$ has *multiplicity* k, if $(x - a)^k$ divies f but $(x - a)^{k+1}$ does not divide f in $F[x]$. It is called *simple*, if $k = 1$ and *multiple* otherwise.
Lemma: A root $a \in F$ of $f \in F[x]$ is a multiple root if and only if $x - a$ divides both f and f' (formal derivative).

4 Field Extensions

In the whole section, E is an extension field of F and L one of E.
Observation: E is an F-vector space, using addition and multiplication from E.
Definition: The *degree* $[E : F]$ is the dimension of E as F-vector space.
And: $[L : F] = [L : E] \cdot [E : F]$ if all are finite.
Theorem: If $[E : F]$ is finite, then E is an *algebraic extension* of F: all $a \in E$ are algebraic over F.
Definition: For any subset $M \in E$, we denote by $F(M)$ the smallest subfield of E that contains both F and M. It is the intersection of all such subfields and as such a subfield of E.
Definition: The *degree* of an element $a \in E$ over F is equal to $[F(a) : F]$, it is finite if and only if a is algebraic over F.
Theorem: Let $a \in E$ be algebraic over F and let g be its minimal polynomial. Then $F[x]/(g)$ is isomorphic to $F(a)$ via the isomorphism mapping every $b \in F$ to itself and $x + (g)$ to a. Therefore, the degree d of $F(a)$ (and thus of a) over F is equal to the degree of g, and $(1, a, a^2, \ldots, a^{d-1})$ is an F-basis of F.
Theorem (Kronecker): Let $f \in F[x]$ be an irreducible polynomial. Then there is a simple algebraic extension E of F with a root of f as defining element.
Definition: A polynomial $f \in F[x]$ *splits* over E, if $f = \prod_{i=1}^{n}(x - a_i)$ for some $a_i \in E$. The field E is called a splitting field, if f splits over E and $E = F(a_1, \ldots, a_n)$. That is, a splitting field is a smallest possible extension field containing all roots of f.
Theorem: For every polynomial $f \in F[x]$ there is a splitting field E and all such splitting fields are isomorphic.

5 Finite fields

Theorem: For every prime power $q = p^n$ there is (up to isomorphism) exactly one finite field, denoted by $\mathbb{F}_q$. It has characteristic p and is the splitting field of $x^q - x$ over $\mathbb{F}_p$.
Theorem: Let p and r be primes. Then $\mathbb{F}_{p^m}$ is isomorphic to a subfield of $\mathbb{F}_{r^n}$ if and only if $p = r$ and m is a divisor of n. In this case $\mathbb{F}_{p^n}$ has exactly one subfield (not up to isomorphism!) with p^m elements, namely the set of roots of $x^{p^m} - x$.
Theorem: Every finite subgroup G of the multiplicative group $\mathbb{F}^*$ of a field $\mathbb{F}$ is cyclic.
So in particular, $\mathbb{F}_q^*$ is cyclic and has $q - 1$ elements, the generators (as group) are called *primitive elements*. If $q = p^n$, they all have degree n over $\mathbb{F}_p$. Note that there can be elements $\mathbb{F}_q$ of degree n but whose order is a proper divisor of $q - 1$.
Corollary: For every prime power q and every $n \in \mathbb{N}$, there is an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree n. Just take the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^n}$.

6 Irreducible polynomials

Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n, then $\mathbb{F}_q[x]/(f)$ is an extension field of $\mathbb{F}_q$ of degree n, so $\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^n}$. Let $a \in \mathbb{F}_{q^n}$ be any root of f, then f is the minimal polynomial of a over $\mathbb{F}_q$.
Theorem: The roots of f all lie in $\mathbb{F}_{q^n}$, they are $a, a^q, a^{q^2}, \ldots, a^{q^{n-1}}$. These elements are called the *conjugates of* a *over* $\mathbb{F}_q$. This implies that $\mathbb{F}_{q^n} = \mathbb{F}_q(a)$ and $\mathbb{F}_{q^n}$ is the splitting field of f over $\mathbb{F}_q$.
Theorem: $x^{q^n} - x$ is the product of all monic irreducible polynomials $f \in \mathbb{F}_q[x]$ with $\deg f \mid n$.
Definition: The Moebius function $\mu : \mathbb{N} \to \mathbb{N}$ is: $\mu(n) = 0$ if n is divisible by a square of a prime and $\mu(p_1 \cdot \cdots \cdot p_k) = (-1)^k$ if the p_i are pairwise distinct primes.
Theorem: (Moebius Inversion) For $H, h : \mathbb{N} \to G$ we have

$$H(n) = \sum_{d|n} h(d) \quad \forall\, n \in \mathbb{N} \quad \iff \quad h(n) = \sum_{d|n} \mu(d) H(n/d) = \sum_{d|n} \mu(n/d) H(d) \quad \forall\, n \in \mathbb{N},$$

if G is written additively, and

$$H(n) = \prod_{d|n} h(d) \quad \forall\, n \in \mathbb{N} \quad \Longleftrightarrow \quad h(n) = \prod_{d|n} H(n/d)^{\mu(d)} = \prod_{d|n} H(d)^{\mu(n/d)} \quad \forall\, n \in \mathbb{N},$$

if G is written multiplicatively.
Theorem: The product of all monic irreducible polynomials of degree n over $\mathbb{F}_q$ is

$$I(q, n; x) = \prod_{d|n} \left(x^{q^d} - x \right)^{\mu(n/d)}.$$

Corollary: If $N_q(n)$ is the number of monic irreducible polynomials over $\mathbb{F}_q$, then

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

7 Roots of unity

Definition: Let F be a field and $n \in \mathbb{N}$. Then $F^{(n)}$ is the *n-th cyclotomic field of F* (the splitting field of $x^n - 1$ over F) and $E^{(n)}$ is the set of *n-th roots of unity over F*. An element of $E^{(n)}$ of order n is called a *primitive n-th root of unity*.
Theorem: If $p = \text{char } F$ and $p \nmid n$, then $E^{(n)}$ (with multiplication of $F^{(n)}$) is a cyclic group of order n. If $n = p^k \cdot m$ and $p \nmid m$, then $F^{(n)} = F^{(m)}$ and $E^{(n)} = E^{(m)}$.
Definition/Proposition: Assume char $F \nmid n \in \mathbb{N}$. Then the *n-th cyclotomic polynomial* is defined as

$$Q_n(x) = \prod_{\substack{1 \le s \le n \\ \gcd(s,n)=1}} (x - \zeta^s),$$

where ζ is a primitive n-th root of unity. $Q_n(x)$ has coefficients in the prime field of F (and in $\mathbb{Z}$ if char $F = 0$), and:

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

If $F = \mathbb{F}_q$ and $d = \text{ord}_n(q)$, the polynomial Q_n factors over $\mathbb{F}_q$ into a product of $\phi(n)/d$ distinct monic irreducible factors of degree d and $\mathbb{F}_q^{(n)}$ is the splitting field of any of these factors.
Theorem: We have $I(q, n; x) = \prod_m Q_m(x)$ where m runs through the positive divisors of $q^n - 1$ for which $n = \text{ord}_m(q)$ and where $Q_m(x)$ is the m-th cyclotomic polynomial over $\mathbb{F}_q$.

8 Automorphisms, traces and norms

Definition: Let E be an extension field of F. An *automorphism of E over F* is a field automorphism of E that fixes every single element of F.
Theorem: The field automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are precisely the mappings $\sigma_j : a \mapsto a^{q^j}$. They form a cyclic group of order n under composition. This is the *Galois group* of the extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
Definition/Proposition: Let $E = \mathbb{F}_{q^n}$ and $F = \mathbb{F}_q$. Then the *trace of E/F* is the map $\text{Tr}_{E/F} : E \to F$ which maps $a \in E$ to the sum $a + a^q + a^{q^2} + \cdots + a^{q^{n-1}}$ of its conjugates. $\text{Tr}_{E/F}$ is a surjective F-linear map and $(a, b) \mapsto \text{Tr}_{E/F}(a \cdot b)$ is a non-degenerate F-bilinear form on E.
Definition/Proposition: Let $E = \mathbb{F}_{q^n}$ and $F = \mathbb{F}_q$. Then the *norm of E/F* is the map $N_{E/F} : E \to F$ which maps $a \in E$ to the product $a \cdot a^q \cdot a^{q^2} \cdot \cdots \cdot a^{q^{n-1}} = a^{\frac{q^n-1}{q-1}}$ of its conjugates. $N_{E/F}$ is a surjective group homomorphism from E^* to F^*.
Theorem: If $F \subseteq E \subseteq L$ are fields, then

$$\text{Tr}_{L/F}(a) = \text{Tr}_{E/F}(\text{Tr}_{L/E}(a)) \qquad \text{and} \qquad N_{L/F}(a) = N_{E/F}(N_{L/E}(a))$$

for all $a \in L$.