(Finite) Fields and Polynomial Rings

Def: As mentioned earlier, a division ring is a ring R in which every nonzero element has a multiplicative inverse; If R is commutative, we call it a field; if it is known, that R is non-commutative, then R is often called a skew field.

Examples a) $\mathbb{Z}_p$ for p prime

b) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

c) $\mathbb{H} := \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \;\middle|\; a, b \in \mathbb{C} \right\}$ with known matrix operations. This is a skew field also known under the name Hamiltonian Quaternions

d) $\mathbb{H} := \{ a + ib + jc + kd \mid a, b, c, d \in \mathbb{R} \}$ with $i^2 = j^2 = k^2 = -1$; $ij = k = -ji$

a different representation of the Quaternions, namely over the reals.

e) $\mathbb{F}_4 := \{0, 1, a, a^2\}$
with $1 + a = a^2$
forms a 4-element field while $\mathbb{Z}_4$ is not a field because it contains the zero divisor $x = 2$.

Def. Let $\mathbb{F}$ be a field. Denote by

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{F}; n \in \mathbb{N} \right\}$$

the polynomial ring in the indeterminate x.
A polynomial $f = \sum_{i=0}^{n} f_i x^i$ is called
<u>monic</u> if $f_n = 1$; The degree of a polynomial is the highest k for which $f_k \neq 0$. In this case $f = \sum_{i=0}^{k} f_i x^i$. The degree of the zero polynomial $f = 0$ is set to be $-\infty$, while the degree of any const polynomial $f = f_0 \neq 0$ is clearly $\deg(f) = 0$.

<u>Lemma</u>. The degree function $\mathbb{F}[x] \longrightarrow \mathbb{N} \cup \{-\infty\}$ has the properties

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Proposition $\mathbb{F}[x]$ allows for a division algorithms: For $f, g \in \mathbb{F}[x]$ with $g \neq 0$ there exist $a, b \in \mathbb{F}[x]$ such that $f = ag + b$ and $\deg(b) < \deg(g)$.

Example. $\mathbb{F} = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. For

$$f = x^5 + 2x^4 + 3x^3 + x + 1 \quad \text{and}$$
$$g = 2x^2 + x + 4$$

find $a, b \in \mathbb{F}[x]$ such that $f = ag + b$ and $\deg(b) < 2$.

$\rightsquigarrow$ Long division:

$$x^5 + 2x^4 + 3x^3 + x + 1 \div 2x^2 + x + 4 = 3x^3 + 2x^2 + 2x + 3$$

$$\begin{array}{l}
x^5 + 2x^4 + 3x^3 + x + 1 \\
\underline{x^5 + 3x^4 + 2x^3} \\
\quad 4x^4 + x^3 + x + 1 \\
\quad \underline{4x^4 + 2x^3 + 2x^2} \\
\qquad 4x^3 + 3x^2 + x + 1 \\
\qquad \underline{4x^3 + 2x^2 + 3x} \\
\qquad\quad x^2 + 3x + 1 \\
\qquad\quad \underline{x^2 + 3x + 2} \\
\qquad\qquad\quad 4
\end{array}$$

So we find $a = 3x^3 + 2x^2 + 2x + 3$ and $b = 4$.

Corollary: $\mathbb{F}[x]$ is a so-called principal ideal domain (PID) which means that every ideal $I \leq \mathbb{F}[x]$ is of the form $I = \mathbb{F}[x] \cdot g$ where g is a monic polynomial.

proof: If $I = \{0\}$ there is nothing to show as then $g = 0$ is the right choice. Otherwise there is a nonzero polynomial of smallest positive degree k in I, and we may assume that it is monic. Let this polynomial be called g. Then $I \supseteq \mathbb{F}[x] \cdot g$ by the ideal property and we would like to see that $I \subseteq \mathbb{F}[x] \cdot g$. Let $f \in I$ be an arbitrary element. Then by the division algorithm there exist $a, b \in \mathbb{F}[x]$ such that $f = ag + b$ and $\deg(b) < \deg(g)$.

$$\underset{I}{f} = a\underset{I}{g} + b \to b = f - ag \in I$$

This forces by minimality of $\deg(g) = k$ that $b = 0$, and so $f = ag \in \mathbb{F}[x]g$.

This concludes $I = \mathbb{F}[x] \cdot g$ and we are done.

Def: Let $f, g \in \mathbb{F}[x]$ be arbitrary polynomials.

Then $I = \{ af + bg \mid a, b \in \mathbb{F}[x] \}$

$= \langle f, g \rangle = \mathbb{F}[x]a + \mathbb{F}[x]b$

is a principal ideal, and hence we know of a monic polynomial d such that $I = \mathbb{F}[x] \cdot d$.

We will call d the <u>greatest common divisor</u> $\gcd(f, g)$.

<u>Lemma</u>. The properties of the $\gcd(f, g) =: d$

(a) $d \cdot r = f$, $d \cdot s = g$ for some $r, s \in \mathbb{F}[x]$, which means d is a divisor of both f and g.

(b) If e has the property that $e \mid f$ and $e \mid g$ (stands for "is a divisor of") Then $e \mid d$.

<u>Proof</u>: See standard text books on basic abstract algebra.

<u>Def</u>: We say f and $g \in \mathbb{F}[x]$ are co-prime, if $\gcd(f, g) = 1$.

Lemma: If $f \mid gh$ and f, g coprime then $f \mid h$.

proof: We have $a, b \in \mathbb{F}[x]$ such that $af + bg = 1$, moreover we have $s \in \mathbb{F}[x]$ such that $fs = gh$. Now $h = h \cdot 1$
$= h \cdot (af + bg) = haf + bgh = haf + bsf$
$= (ha + bs)f$ which shows $f \mid h$.

Def: A polynomial $p \in \mathbb{F}[x]$ (of degree > 0) is called irreducible if $p = f \cdot g$ implies $f = \text{const}$ or $g = \text{const}$

Examples: a) $x^2 + 1 \in \mathbb{R}[x]$

b) $x^2 - x - 1 \in \mathbb{Q}[x]$

c) $x^2 + x + 1 \in \mathbb{F}[x]$ with $\mathbb{F} = \{0, 1\}$

Observation: a) All polynomials of deg 1 are irreducible

b) A polynomial p of deg 2 or 3 is irreducible if $p(a) \neq 0$ for all $a \in \mathbb{F}$.
Here for $p = \sum_{i=0}^{k} p_i x^i$ we set $p(a)$
$= \sum_{i=0}^{k} p_i a^i$.

Theorem. $\mathbb{F}[x]$ is a so-called Unique-Factorization-Domain (UFD): any non-constant polynomial $f \in \mathbb{F}[x]$ allows for the representation

$$f = c \cdot p_1^{k_1} \cdots p_s^{k_s}$$

where c is a constant and the p_i are distinct monic irreducible polynomials and $k_i \in \mathbb{N}$.

If $c \cdot p_1^{k_1} \cdots p_s^{k_s} = f = d \cdot q_1^{l_1} \cdots q_t^{l_t}$ are two ~~diff~~ such representations, then $c = d$ and $p_i = q_i$ (after rearrangement) (see above) and particularly and $k_i = l_i$

$s = t$.

Proposition. Let $\mathbb{F}$ be a finite field. The intersection of all subfields in $\mathbb{F}$ is the smallest subfield in $\mathbb{F}$, which is generated by $\{0,1\}$ and of the structure of $\mathbb{Z}_p$ where p is the characteristic of $\mathbb{F}$ (i.e. $p \cdot 1 = 0$, with $p > 0$ minimal).

Accordingly, as $\mathbb{F}$ is a vector space over this p-element prime field, there holds $|\mathbb{F}| = p^n$ for suitable $n \in \mathbb{N}$.

<u>proposition</u> : let $\mathbb{F}_p$ be the field with p ~~elements~~ elements, p a prime number. Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree m. Then the factor ring

$$R := \mathbb{F}_p[x] / \mathbb{F}_p[x] \cdot f$$

is a finite field with p^m elements.

<u>Remark</u> : It can be proved that if $\mathbb{F}$ is a field and m is a positive integer, then there exists an irreducible polynomial $f \in \mathbb{F}[x]$ with $\deg(f) = m$.

All this combined allows the conclusion that finite fields of size M exist exactly for $M = p^m$ where p is a prime and m is a positive integer.