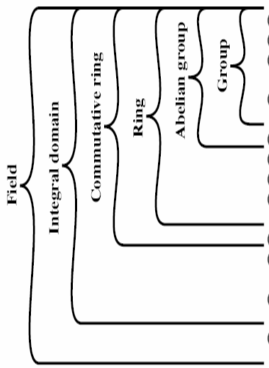
Compléments de mathématique

Compléments de mathématique

Groupes, anneaux, champs

Groupe, Anneau, champ



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Exemples

- Groupe abelien
  - L'ensemble des entiers (positif, négatif, et 0) sous l'addition
  - L'ensemble des nombres réels sous la multiplication
- Groupe cyclique
  - Le groupe additif des entiers positifs est un groupe cyclique infini généré par l'élément 1
- Anneau
  - En respect avec l'addition et la multiplication, l'ensemble des matrices n carrée sur les réels est un anneau R

Exemples

- Anneau commutatif
  - L'ensemble des entiers pairs (>0, <0, =0) sous les opérations habituelles de l'addition et de la multiplication.
- Domaine d'intégration
  - L'ensemble des entiers (>0, <0, =0) sous les opérations habituelle de l'addition
- Champs
  - Les nombres rationnels, les nombres réels, les nombres complexes mais pas l'ensemble des nombres entiers

Champs finis de la forme GF(p)

- Intérêt : on peut montrer que l'ordre d'un champ fini (nombre d'éléments dans le champ) doit être une puissance d'un nombre premier p^n où n est un entier positif.
- Le champ fini d'ordre p^n est généralement écrit $GF(p^n)$.
- Pour n=1 : GF(p)

Arithmétique polynomiale et GF(2^n)

Arithmétique polynomiale

- On s'intéresse à la classe de l'arithmétique polynomiale dans laquelle l'arithmétique sur les coefficients est effectuée modulo p (c-à-d dont les coefficients sont dans $\mathbb{Z}_p$.

Exemple d’arithmétique polynomiale

$$\begin{array}{r} x^3 + x^2 \qquad + 2 \\ + \quad (x^2 - x + 1) \\ \hline x^3 + 2x^2 - x + 3 \end{array}$$

(a) Addition

$$\begin{array}{r} x^3 + x^2 \qquad + 2 \\ - \quad (x^2 - x + 1) \\ \hline x^3 \qquad + x + 1 \end{array}$$

(b) Subtraction

$$\begin{array}{r} x^3 + x^2 \qquad + 2 \\ \times \quad (x^2 - x + 1) \\ \hline x^3 + x^2 \qquad + 2 \\ -x^4 - x^3 \qquad - 2x \quad \\ x^5 + x^4 \qquad + 2x^2 \qquad \qquad \\ \hline x^5 \qquad + 3x^2 - 2x + 2 \end{array}$$

(c) Multiplication

$$\begin{array}{r|l} & x + 2 \\ \hline x^2 - x + 1 & x^3 + x^2 \qquad + 2 \\ & x^3 - x^2 + x \\ \hline & \quad 2x^2 - x + 2 \\ & \quad 2x^2 - 2x + 2 \\ \hline & \qquad x \end{array}$$

(d) Division

Arithmétique polynomiale pour GF(2)

$$\begin{array}{r} x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\ + (x^3 \quad + x + 1) \\ \hline x^7 \quad + x^5 + x^4 \qquad \qquad \qquad \end{array}$$

(a) Addition

$$\begin{array}{r} x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\ - (x^3 \quad + x + 1) \\ \hline x^7 \quad + x^5 + x^4 \qquad \qquad \qquad \end{array}$$

(b) Subtraction

$$\begin{array}{r} x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\ \times (x^3 \quad + x + 1) \\ \hline x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\ x^8 \quad + x^6 + x^5 + x^4 \quad + x^2 + x \quad \\ x^{10} \quad + x^8 + x^7 + x^6 \quad + x^4 + x^3 \qquad \qquad \\ \hline x^{10} \qquad \qquad + x^4 \quad + x^2 \quad + 1 \end{array}$$

(c) Multiplication

$$\begin{array}{r|l} & x^4 + 1 \\ \hline x^3 + x + 1 & x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\ & x^7 \quad + x^5 + x^4 \\ \hline & \qquad \qquad \qquad x^3 \quad + x + 1 \\ & \qquad \qquad \qquad x^3 \quad + x + 1 \\ \hline \end{array}$$

(d) Division

GCD pour l'arithmétique polynomiale

- Le polynôme c(x) est le gcd de a(x) et b(x) si
  1. c(x) divise a(x) ET b(x)
  2. Tout diviseur de a(x) ET b(x) est un diviseur de c(x)
- gcd[a(x),b(x)] est le polynôme de degré maximal qui divise a(x) et b(x)
- L'équation d'égalité est conservée :

  gcd([a(x),b(x)] = gcd[b(x), a(x) mod b(x)]
- On suppose que le degré de a(x) > degré b(x)

Algorithme d'Euclide pour les polynômes

- EUCLID[a(x),b(x)]

```
1. A(x) ← a(x); B(x) ← b(x)
2. IF B(x) = 0 RETURN A(x) = gcd[a(x),b(x)]
3. R(x) = A(x) mod B(x)
4. A(x) ← B(x)
5. B(x) ← R(x)
6. GOTO 2
```

Champs finis de la forme $GF(2^n)$

- Considérer l'ensemble S de tous les polynômes de degré n 1 ou moins dans le champ Z_p. Il y a un total de p^n différents polynômes dans S. Avec la définition appropriée des opérations arithmétiques, chaque ensemble S de ce type est un champ fini. La définition comprend les éléments suivants :
  1. l'arithmétique suit les règles ordinaires de l'arithmétique polynomiale en utilisant les règles de base de l'algèbre
  2. l'arithmétique sur les coefficients se fait modulo p. C'est-à-dire, nous employons les règles de l'arithmétique pour le champ fini Z_p.
  3. si la multiplication résulte en un polynôme de degré plus grand que n-1, alors le polynôme est réduit modulo un certain polynôme irréductible m(x) de degré n. C'est-à-dire, que nous divisons par m(x) et gardons le reste. Pour un polynôme f(x), le reste est exprimé en tant r(x) = f(x) mod m(x).

Algorithme d'Euclide pour $GF(2^n)$

- `EXTENDED EUCLID[m(x), b(x)]`

```
1. [A1(x),A2(x),A3(x)] ← [1,0,m(x)];
   [B1(x),B2(x),B3(x)] ← [0,1,b(x)]
2. IF B3(x)=0 RETURN A3(x)=gcd[m(x),b(x)]; no inverse
3. IF B3(x)=1 RETURN B3(x)=gcd[m(x),b(x)];
   B2(x) = b(x)^-1 mod m(x)
4. Q(x) = quotient of A3(x)/B3(x)
5. [T1(x),T2(x),T3(x)] ← [A1(x)-Q(x)B1(x), A2(x)-
   Q(x)B2(x), A3-Q(x)B3(x)]
6. [A1(x),A2(x),A3(x)]←[B1(x),B2(x),B3(x)]
7. [B1(x),B2(x),B3(x)]←[T1(x),T2(x),T3(x)]
8. GOTO 2
```

Euclide étendu pour $GF(2^n)$

Initialization	$A1(x) = 1; A2(x) = 0; A3(x) = x^8 + x^4 + x^3 + x + 1$ $B1(x) = 0; B2(x) = 1; B3(x) = x^7 + x + 1$
Iteration 1	$Q(x) = x$ $A1(x) = 0; A2(x) = 1; A3(x) = x^7 + x + 1$ $B1(x) = 1; B2(x) = x; B3(x) = x^4 + x^3 + x^2 + 1$
Iteration 2	$Q(x) = x^3 + x^2 + 1$ $A1(x) = 1; A2(x) = x; A3(x) = x^4 + x^3 + x^2 + 1$ $B1(x) = x^3 + x^2 + 1; B2(x) = x^2 + 1; B3(x) = x$
Iteration 3	$Q(x) = x^3 + x^2 + x$ $A1(x) = x^3 + x^2 + 1; A2(x) = x^2 + 1; A3(x) = x$ $B1(x) = x^6 + x^2 + x + 1; B2(x) = x^7; B3(x) = 1$
Iteration 4	$B3(x) = \gcd[(x^7 + x + 1), (x^8 + x^4 + x^3 + x + 1)] = 1$ $B2(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

Remarques

- L'addition de 2 polynômes dans $GF(2^n)$ correspond à une opération XOR
- $x * f(x) =$
  - $(b_6b_5b_4b_3b_2b_1b_00)$ si $b_7 = 0$
  - $(b_6b_5b_4b_3b_2b_1b_00) \oplus (00011011)$ si $b_7 = 1$