An algebraic hierarchy

Vector Space	A vector space, $\mathcal{V}$, consists of *vectors,* which are collections of elements from a field, $\mathcal{F}$, and *scalars,* which are elements of $\mathcal{F}$.
Field	A field, $\mathcal{F}$, is a *commutative ring with identity;* every element, except additive identity, has an inverse wrt. "x"
Ideal	An ideal is a subset of ring, with commutative "+" and $g \times m = c \in \mathcal{I},\ g = \mathcal{I}, m \in \mathcal{R}$
Ring	Rings are *groups* that support two binary operations, commutative "+" and "x", with distribution of "x" over "+".
Group	Groups are *sets* that support a single binary operation, with association a+(b+c)=(a+b)+c, identity and inverse. Not necessarily commutative
Set	Sets are *collections of things.*
Element	Elements are *things,* e.g., integers, polynomials, vectors,

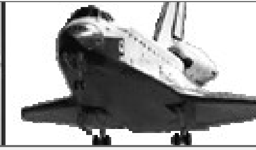
Some examples

- The set of all integers, □ , forms a *group* under normal addition
  - It is closed
  - It is associative
  - It has an inverse and identity
- The set of all integers, $\mathbf{Z}$, does not form a field
  - There is a multiplicative identity…
  - …but multiplicative inverses don’t exist
  - So it is a ring!
  - Even integers are an ideal!
- The set of all rational numbers does form a field…
- …as do real numbers…and complex numbers.
- The set of integers $\{0,1,\ldots,q-1\}$ under modulo q arithmetic may form a field under certain conditions

Galois Fields

- Everiste Galois (1811-1832!) theory of roots of polynomial equations
- A Galois Field is a field with a *finite number of elements*
- We use the nomenclature GF(q) to indicate a Galois field with q elements
- For the integers with modulo q arithmetic, GF(q) requires that q be a prime number!
- The best-known and most used Galois Field is GF(2), the binary field!
- For GF(q) in general, q must be a *power* of a prime.
- The structure of GF(p^m) for powers-of-primes requires algebraic rules more complicated than simple integer modulo arithmetic

What is and isn’t a GF?



- **Simplest example,** $q = 2 \quad GF(2)$ or the binary field

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

- **Closed, associative & distributive from $\mathbb{Z}$, additive identity, additive inverse, multiplicative identity, multiplicative inverse**

- **What about** $q = 2^2 = 4$ **?**

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

The GFAU Task: Operate in GF(2^m)

- Creating a "binary" Galois field $GF(2^m)$
- We write "the set of all polynomials with coefficients in GF(p)" as GF(p)[x]
- Example
  - x^3+x+1 is a polynomial in $GF(2)[x]$
  - So is x^3+x^2+x+1
- Do these polynomials have roots in $GF(2)$?
  - $0+0+1=1, \text{ so } 0 \text{ is not a root}$

    $1+1+1=1, \text{ so } 1 \text{ is not a root}$

    $x^3+x+1 \text{ has no roots in } GF(2)$
  - But x^3+x^2+x+1 has a root for $x=1$
- If a polynomial has no root in $GF(2)$ we call it **irreducible**

- If an irreducible polynomial has another property (that we don’t need to worry about right now), it is not only “irreducible” but also “primitive”.
- We can use m-th order primitive polynomials to generate $GF(2^m)$
- x^3+x+1 is such a primitive polynomial!
- Because it is a 3rd order, primitive polynomial over $GF(2^m)$, we can use it to generate $GF(2^3)=GF(8)$
- The primitive polynomial will be **an input** to the initialization of GFAU!
- You don’t have to identify the primitive polynomials!

- **Let** $\alpha \square GF(2^8)$ **be a root of** x^3+x+1 **, so** $\alpha^3+\alpha+1=0$
- **The coefficients are in** $GF(2)$, **so** $\alpha^3=\alpha+1$
- **Note that** α **is in the "big" field, but the coefficients of the polynomial are in the "little field"**
- $0,1$ **must be in the big field, because a field has additive and multiplicative identities.**
- α **must be in the big field, by assumption**
- α^2 **must be in the big field by closure of multiplication**
- α^3 **must be in the big field, but** $\alpha^3=\alpha+1$
- $\alpha^4=\alpha^3\square\alpha=(\alpha+1)\square\alpha=\alpha^2+\alpha$ **must be in the big field**
- $\alpha^5=\alpha^4\square\alpha=(\alpha^2+\alpha)\square\alpha=\left(\alpha^3+\alpha^2\right)=\alpha^2+\alpha+1$

$$\alpha^6=\alpha^5\square\alpha=\left(\alpha^2+\alpha+1\right)\square\alpha=\alpha^3+\alpha^2+\alpha=\alpha+1+\alpha^2+\alpha=\alpha^2+1$$

$$\alpha^7=\alpha^6\square\alpha=(\alpha^2+1)\square\alpha=\alpha^3+\alpha=\alpha+1+\alpha=1\ (!!!!!)$$

- **We now have polynomials in α, where the coefficients are binary, that is $GF(2)$**
- **We write the symbols of $GF(2^m)$ as m-element vectors in the "little field", $GF(2)$**

Element of $GF(2^3)$	Polynomial form	Symbol (msb on left)
0	0	000
1	1	001
α	α	010
α^2	α^2	100
α^3	$\alpha+1$	011
α^4	$\alpha^2+\alpha$	110
α^5	$\alpha^2+\alpha+1$	111
α^6	α^2+1	101

$\alpha^7=1$, and the process starts over

Addition table for GF(2^3)

GF(2^3)

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

Integers mod 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

For multiplication: $\alpha^k \times \alpha^j = \alpha^{(k+j) \bmod 2^3-1}$

$$\alpha^4 \times \alpha^6 = \alpha^{10 \bmod 7} = \alpha^3 = \alpha + 1$$

α **is called a *primitive element of the field*, because the powers of** α **generate the** $p^m - 1$ **non-zero elements**

- **GFAU Homework**
- **Generate**

1) Show that $x^3 + x + 1$ is irreducible in $GF(2)[x]$

2) Generate the 8 elements of $GF(2^3)$ using the primitive polynomial $x^3 + x^2 + 1$.

3) Generate the addition (bitwise exclusive or) and multiplication tables

for your impleentation of $GF(2^3)$

4) Compare your generation of $GF(2^3)$ to mine.

They will not be the same!