Lecture 6 — Finite Fields

Dr. D. Bernhard

In this lecture: finite commutative rings without zero divisors are fields — classification of finite fields — irreducible polynomials — construction of finite fields $GF(p)$ and $GF(p^n)$ — computing in finite fields — isomorphisms between finite fields

Learning outcomes. After this lecture and revision, you should be able to:

- Decide whether or not a finite field of a given size exists.
- Construct a finite field of any size where one exists.
- Compute in finite fields.
- Find isomorphisms between different representations of the same finite field.

6 Finite Fields

A field is a structure in which you can add, subtract, multiply and divide (except by zero). Today we are going to look at finite fields. Recall that $\mathbb{Z}_{256}$ is not a field because of zero divisors. Can we construct a field with 256 elements? We can, but not with the usual addition modulo 256. The first question we have to answer to get our field with 256 elements is, when is a finite ring a field?

6.1 Finite commutative rings

Take any ring $(R, +, \cdot)$. We know that we can classify all elements as zero, unit, zero divisor or neither. But if our ring is finite, the "neither" case cannot happen.

Let's pick an element x in a finite ring that is neither zero nor a zero divisor. This means that if we look at the sequence $x, x \cdot x, x \cdot x \cdot x, \ldots$, we can never hit zero. We can obviously write this as $x, x^2, x^3, \ldots$. But if the ring is finite, at some point an element has to repeat so we get an equation of the form $x^k = x^{k+m}$ for positive integers k, m from which we conclude that $x^m = 1$ (you can cancel x^k since x is not a zero divisor, therefore neither is x^k). Whether or not the ring is commutative, the associative law implies that powers of x commute with each other. Therefore $x \cdot x^{m-1} = 1$ and $x^{m-1} \cdot x = 1$, so x^{m-1} really is the inverse of x under multiplication.

In other words, the only way a nonzero ring element can be neither a unit nor a zero divisor is if the ring is infinite (for example, 3 in $\mathbb{Z}$). In a finite ring such as $\mathbb{Z}_n$, as soon as a nonzero element is not a zero divisor it automatically has an inverse. This proves the following proposition:

Proposition 6.1. A finite commutative ring without zero divisors is a field.

We know that the rings $(\mathbb{Z}_n, +, \cdot)$ satisfy these conditions exactly when n is a prime, except for the special case $(\{0\}, +, \cdot)$. (For a non-prime n, the structure $(\mathbb{Z}_n^\times, \cdot)$ is a group but such a $\mathbb{Z}_n^\times$ is no longer a group under addition so we cannot construct a ring this way, let alone a field.) This means that for each prime p, we can construct a field with p elements.

6.2 Classification of finite fields

Finite fields are relatively "rare" objects. The following theorem describes exactly which ones exist:

Theorem 6.2 (classification of finite fields). For every prime p and every positive integer n, there is exactly one finite field with p^n elements up to isomorphism. These are the only finite fields.

The field with p^n elements can be written either $\mathbb{F}_{p^n}$ or $GF(p^n)$ and pronounced "Galois Field" after the French mathematician E. Galois. The power operator is always left in the description, i.e. one writes $GF(2^8)$ not $GF(256)$.

6.3 Prime fields

The simplest finite fields are those for power $n = 1$: these are just the fields $GF(p) = (\mathbb{Z}_p, +, \cdot)$ with the usual addition and multiplication modulo p that we constructed above. Every other attempt to construct a finite field of order p will produce one isomorphic to the above construction.

6.4 Irreducible polynomials

Here is the general idea to construct a field with p^n elements. Start with the field $GF(p)$ and form the polynomial ring $GF(p)[X]$. This has infinitely many elements. Then, take

this ring modulo a polynomial of degree n to get a ring of p^n elements (sequences of n elements from $\mathbb{Z}_p$). As long as we do not end up introducing any zero divisors, since this ring is finite and commutative it is automatically a field.

How do we prevent zero divisors? When going from $\mathbb{Z}$ to $\mathbb{Z}_n$ (viewed as rings), zero divisors are exactly the non-unit elements that divide n so we don't get any if we pick n to be a prime.

I've said before that in Algebra, polynomials are just "another kind of number". So if we pick a polynomial to divide by that is a "prime polynomial", we should not get any zero divisors for exactly the same reason.

We have to quickly get some terminology out of the way. In general algebra, there are two distinct concepts "prime" and "irreducible". What we actually need to avoid zero divisors are irreducible moduli; both the integers and polynomial rings over fields are special cases where prime and irreducible turn out to be the same thing (technically, so-called unique factorisation domains). While "prime number" is the common term for the integers, when talking about polynomials it is more usual to talk about "irreducible polynomials" which we will do from now on. For the purposes of this course, it is not too inaccurate to imagine "irreducible" to mean "something like prime"

Definition 6.3 (irreducible polynomial). A polynomial p over a field is irreducible if it is not a unit and cannot be decomposed into a product of non-units, i.e. if $p = ab$ then either a or b is a unit.

The definition of irreducible applies not only to polynomial rings over fields but to any integral domain, though we will only be using it for polynomials.

Exercise. ($\star$) If $p = ab$ for an irreducible p, why can't both a and b be units?

In $\mathbb{Z}$ (which is an integral domain), the irreducible elements are exactly those numbers p which are not 1 or -1 where $p = ab$ implies that one of a or b is 1 or -1, in which case the other must be p or $-p$ — these are exactly the usual prime numbers, of course.

6.5 Finding irreducible polynomials

Let's take $GF(7)$ as an example field (the rest of this section works equally well with any finite field) and look at polynomials of low degrees in $GF(7)[X]$.

- The polynomial 0 is the zero element, so it is not irreducible (0 is not a unit).

- Polynomials of degree 0 are sequences (c_0) where c_0 is a non-zero field element. All of these are units and therefore not irreducible (the same reason that 1 is not a prime).
- Polynomials of degree 1 can be written $aX + b$ for field elements a, b with $a \neq 0$. In the polynomial ring over a field without any polynomial "modded out", a polynomial of degree 1 or higher cannot be a unit (there is no "$1/X$" to remove the X). Since all non-zero non-units have degree of at least 1, if a, b are two such polynomials then ab has degree at least 2 so all polynomials of degree 1 are irreducible.
- Degree 2 is where it starts to get interesting. Certainly, any polynomial that is the product of two degree-1 polynomials is not irreducible. Since we can always multiply a polynomial through with the inverse of the leading coefficient, let's consider only polynomials of the form $X^2 + bX + c$. If such a polynomial factors, it will be without loss of generality into the form $(X+u)(X+v)$ which gives $b = u+v$ and $c = uv$. In a finite field, we could in principle make a table with columns $u, v, u + v, uv$ for all values of u and v. To check if a polynomial is irreducible, we see if the pair (b, c) appears in the $(u + v, uv)$ columns anywhere — if so, we have factored the polynomial, otherwise it is irreducible.

  A simple counting argument now shows that there must always be an irreducible polynomial of degree 2 in a field of the form $GF(p)$. There are p possible values each for b, c so there are p^2 quadratic polynomials with leading coefficient 1. Similarly, since our table runs through p values each of u and v, there are p^2 rows in the table. The argument is that if any two rows repeat an $(u + v, uv)$ pair then at least one of the possible (b, c) pairs cannot appear in the table at all. And indeed, for any distinct values of u and v, the rows starting (u, v) and (v, u) will have the same sum and product. For example $(0, 1, 1, 0)$ and $(1, 0, 1, 0)$ both have the same sum of 1 and product of 0.

	u	**v**	**b = u + v**	**c = uv**
	0	0	0	0
⇒	0	1	1	0
	...			
	0	$p-1$	$p-1$	0
⇒	1	0	1	0
	...			

  Table of all possible factorisations of quadratic polynomials, showing repeated b, c entries in two different rows.

  As an example, the polynomial $X^2 + X + 6$ is irreducible over $GF(7)$.
- The situation with polynomials of degree 3 or higher is more complex and we don't treat it here. Suffice it to say that irreducible polynomials of any degree > 0

always exist.

Exercise. ($\star\star$) *Irreducible polynomials.* Find the the following irreducible polynomials:

1. Over $GF(2)$, all irreducible polynomials of degrees 2 and 3.
2. Over $GF(2)$, one irreducible polynomial of degree 4.
3. Over $GF(3)$, all irreducible polynomials of degree 2.
4. Over $GF(5)$, one irreducible polynomial of degree 3.

6.6 Example: $GF(7^2)$

Let's look at some example finite fields. To construct $GF(7^2)$ we take $\mathbb{F}_7[X]/(X^2+X+6)$, giving 49 field elements which we can represent as pairs (a,b) or equivalently, as linear polynomials $(a+bX)$. Addition in this field is just component-wise addition in $\mathbb{F}_7$. To multiply two elements (a,b) and (c,d), viewing them as polynomials we get $bdX^2+(bc+ad)X+ac$ which we have to reduce modulo X^2+X+6. So we factor out bd and rewrite the product as

$$bd\cdot(X^2+X+6)+(bc+ad-bd)\,X+(ac-6bd)$$

for the linear and constant terms, we have "telescoped" out the required factor bd. This gives us the following multiplication formula for this particular representation of the field, using $-6=1$:

$$(a,b)\cdot(c,d)=(ac+bd,bc+ad-bd)$$

6.7 Automorphisms of $GF(7^2)$

Let's find the automorphisms of $GF(7)[X]/(X^2+X+6)$, that is the functions f on this domain with $f(x+y)=f(x)+f(y)$, $f(0)=0$, $f(1)=1$ and $f(xy)=f(x)f(y)$. All that we need to determine an automorphism is $f(X)$, since for any element (a,b) of the field we have $f(a+bX)=a+b\cdot f(X)$.

We start with setting $f(X)=u+vX$ for variables u,v. Then we have $f(X)\cdot f(X)=(u+vX)(u+vX)=u^2+2uvX+v^2(X^2+X+6)-v^2(X+6)=(u^2+v^2)+(2uv-v^2)X$. However, we also have $f(X)\cdot f(X)=f(X^2)=f(-X-6)=(1-u)-vX$, giving us the equations $1-u=u^2+v^2$ and $-v=2uv-v^2$. The last equation gives us two cases: either $v=0$, which is definitely not an automorphism, or $v\neq 0$ in which case we divide by v to get $-1=2u-v$ and substitute to get the quadratic equation $1-u=u^2+(2u+1)^2$ which gives us the solutions $u=0,v=1$ and $u=6,v=6$. Our

automorphisms are $f_1(X) = X$ and $f_2(X) = 6 + 6X$, from which we find $f_1(a + bX) = a+bX$ — the identity function, which is not surprising — and $f_2(a+bX) = (a+6b)+6bX$.

Exercise. ($\star$) Why can $v = 0$ in the above calculation not yield an automorphism?

6.8 Isomorphisms in $GF(7^2)$

We said that there is only one finite field $GF(p^n)$ up to isomorphism for each prime p and positive integer n. Let's look at some examples of this too.

For $GF(7^2)$, another representation of the same field comes from choosing a different irreducible polynomial, such as Y^2+1 which gives the multiplication $(a, b)\odot(c, d) = (ac - bd, ad + bc)$.

Let's try and compute the isomorphisms

$$f : GF(7)[X]/(X^2 + X + 6) \to GF(7)[Y]/(Y^2 + 1)$$

We will use the symbol X for elements in the first representation and the symbol Y for elements in the second; this way the symbol name tells us which polynomial we have to use when reducing elements after multiplication.

We know that $f(1, 0) = (1, 0)$ and thus that $f(a, 0) = (a, 0)$ for any field element $a \in GF(7)$ since 1 is a generator of $(\mathbb{Z}_7, +)$. So all we need to find is $f(0, 1) = f(X)$ since $f(a + bX) = a + b \cdot f(X)$. Writing $f(X) = u + vX$ for variables u, v ranging over $GF(7)$, for any element (a, b) we have $f(a, b) = (a + ub, vb)$. Now look at the equation $f(a, b) \odot f(c, d) = f((a, b) \cdot (c, d))$ that any isomorphism must satisfy. Writing this out and combining terms gives the conditions $2uv = -v$ and $u^2 - v^2 = 1 - u$ which give $u = 3$ and $v = 2 \vee v = 5$. So we have two isomorphisms

$$f_1 : (a, b) \mapsto (a + 3b, 2b)$$
$$f_2 : (a, b) \mapsto (a + 3b, 5b)$$

We can describe both these isomorphisms by their action on the polynomial $(0, 1)$ that represents the monomial X: $Y_1 = f_1(X) = 3 + 2X$ and $Y_2 = f_2(X) = 3 + 5X$.

Exercise. ($\star\star$) *The field* $GF(5^2)$.

1. Find the explicit multiplication formula for the representation of $GF(5^2)$ modulo the irreducible polynomial $X^2 + 2X + 3$.
2. Do the same for the irreducible polynomial $2Y^2 + 4Y + 1$.
3. Find the isomorphisms from the first representation to the second.

6.9 Example: $GF(2^8)$

For $GF(2^8)$, our field with 256 elements, we take the irreducible polynomial

$$p(X) = X^8 + X^4 + X^3 + X + 1$$

as an example. In addition to tuples and expressions with a variable X, we have a third representation of $GF(2^8)$ as 8-bit strings with the lowest coefficient rightmost, i.e. the polynomial $X^3 + X + 1$ which is $(1, 1, 0, 1)$ as a tuple can be written `00001011`. The operations on the individual bits, as elements of $GF(2)$, are:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

These are, of course, the binary exclusive-or (XOR) and AND operations. Addition of tuples is component-wise; for multiplication we could write out the formula as for $GF(7^2)$ but this becomes cumbersome. Instead, we give an example. First, we consider the multiplication of binary polynomials without any polynomial modulus. The special thing about working over $GF(2)$ is that $1 + 1 = 0$ so all coefficients in our polynomials are either present or absent but we don't have to worry about field multiplication too much.

Suppose we want to compute the product of the polynomials represented by the bytes `10001010` and `00101101` in $\mathbb{F}_2[X]$. Just like "normal" multiplication of bytes (as perfomed by the x86 `MUL` operation), the result will be a 2-byte value. Writing these out,

$$\begin{aligned} \texttt{10001010} &= X^7 + X^3 + X \\ \texttt{00101101} &= X^5 + X^3 + X^2 + 1 \end{aligned}$$

we can factor out the second operand and write this multiplication in the form

$$X^7(X^5 + X^3 + X^2 + 1) + X^3(X^5 + X^3 + X^2 + 1) + X(X^5 + X^3 + X^2 + 1)$$

Each left-hand side of a product in this term is a monomial with coefficient 1 (the only nonzero element of the base field). But multiplying with X^k like this is just shifting the right-hand factor to the left by k bits. So we can do polynomial multiplication by repeated addition in the usual longhand way:

$$\begin{array}{rcr} \texttt{10001010} \cdot \texttt{00101101} & = & \texttt{0 0101101.} \\ & + & \texttt{001 01101...} \\ & + & \texttt{0010110 1.....} \\ \hline & & \texttt{00010111 10110010} \end{array}$$

which is the polynomial $X^{12} + X^{10} + X^9 + X^8 + X^7 + X^5 + X^4 + X$.

To take such a polynomial modulo $X^8 + X^4 + X^3 + X + 1$, we write the two bytes that make up the product as (hi, lo) so the polynomial is actually $hi \cdot X^8 + lo$. Since lo is of degree at most 7 it does not need to be reduced any further. For hi, we write out the division with remainder by the modulus polynomial $p(X)$ of all higher powers. For example, $X^8 = 1 \cdot (X^8 + X^4 + X^3 + X + 1) + (X^4 + X^3 + X + 1)$.

power	**q**	**r**	binary **r**
X^8	1	$X^4 + X^3 + X + 1$	00011011
X^9	X	$X^5 + X^4 + X^2 + X$	00110110
X^{10}	X^2	$X^6 + X^5 + X^3 + X^2$	01101100
X^{11}	X^3	$X^7 + X^6 + X^4 + X^3$	11011000
X^{12}	$X^4 + 1$	$X^7 + X^5 + X^3 + X + 1$	10101011
X^{13}	$X^5 + X + 1$	$X^6 + X^3 + X^2 + 1$	01001101
X^{14}	$X^6 + X^2 + X$	$X^7 + X^4 + X^3 + X$	10011010
X^{15}	$X^7 + X^3 + X^2 + 1$	$X^5 + X^3 + X^2 + X + 1$	00101111

With this table, we can just add the lo component of our product to the remainders of all the powers present in the hi component:

$$\begin{array}{rll} & 10110010 & (lo) \\ + & 00011011 & X^8 \\ + & 00110110 & X^9 \\ + & 01101100 & X^{10} \\ + & 10101011 & X^{12} \\ \hline & 01011000 & \end{array}$$

This gives us our result in $GF(2^8)$, represented with the irreducible polynomial $X^8 + X^4+X^3+X+1$, of $10001010 \cdot 00101101 = 01011000$ or $(X^7+X^3+X)\cdot(X^5+X^3+X^2+1) = (X^6 + X^4 + X^3)$.

6.10 Implementation of $GF(2^8)$ multiplication

Here is binary multiplication in $\mathbb{F}_2[X]/p(X)$ written as `C` code, where `u8` is an unsigned 8-bit integer datatype and `bool` is a boolean datatype (`int` would do fine as well):

```
/*
Multiply two values a, b in GF(2^8) represented by
p(X) = X^8 + X^4 + X^3 + X + 1  (0x1b).
*/
u8 mul(u8 a, u8 b)
{
    u8 x, y, r;
```

```
    bool carry;
    x = a;
    y = b;
    r = 0x00;
    while (x)
    {
        if (x & 0x01) { r ^= y; }
        carry = y & 0x80;
        y <<= 1;
        x >>= 1;
        if (carry) { y ^= 0x1b; }
    }
    return r;
}
```

The result accumulates in `r`. Each pass through the loop looks at the low-order bit of `x` with `x & 0x01` and if set, adds the current multiple of `b` (which is stored in `y`) to `r`. Afterwards, we shift `x` one position to the right to get the next bit. After each loop iteration, we shift `y` one position to the left, representing a multiplication by the polynomial X. If this overflows, we have to reduce `y` modulo $p(X)$ which has the binary representation `0x1b = 00011011`.

◇ The `C` language does not offer a way to check for carries except with an explicit variable (`carry = y & 0x80` checks if the high bit of `y` is set). In an assembler implementation, this could be handled much better by a branch-if-carry instruction using the processor's carry flag. The small number of constants and local variables involved would also suggest implementing the entire algorithm in the processor's registers.

6.11 Automorphisms of finite fields

The group of automorphisms of a finite field can be found with the following theorem:

> **Theorem 6.4.** The group of automorphisms of $GF(p^n)$ is isomorphic to the group $(\mathbb{Z}_n, +)$ and the Frobenius map $X \mapsto X^p$ is a generator of the automorphism group.

In a finite field represented as $GF(p)[X]/q(X)$, we can compute $f(X)$ for all the automorphisms by repeatedly applying the Frobenius map giving $X^p, X^{p^2}, X^{p^3}, \ldots$ and reducing modulo $q(X)$.

In our case, $p = 2$ and we compute the powers of the Frobenius map for representations of $GF(2^8)$ modulo $p(X) = X^8 + X^4 + X^3 + X + 1$ and $q(Y) = Y^8 + Y^4 + Y^3 + Y^2 + 1$.

n	mod $p(X)$	mod $q(Y)$
0	X	Y
1	X^2	Y^2
2	X^4	Y^4
3	X^4+X^3+X+1	$Y^4+Y^3+Y^2+1$
4	$X^6+X^4+X^3+X^2+X$	$Y^6+Y^3+Y^2$
5	$X^7+X^6+X^5+X^2$	$Y^7+Y^4+Y^3+Y^2+1$
6	$X^6+X^3+X^2+1$	$Y^6+Y^4+Y^3+Y^2+Y+1$
7	$X^7+X^6+X^5+X^4+X^3+X$	Y^7+Y^2+1

6.12 Isomorphisms of $GF(2^8)$

Next, let's look for the isomorphisms of $GF(2^8)$ from the representation modulo $p(X) = X^8+X^4+X^3+X+1$ to another representation, for example $q(Y) = Y^8+Y^4+Y^3+Y^2+1$ (this is another irreducible polynomial; note the Y^2 in place of the X). That is, we're looking for an isomorphism f that maps field elements to other field elements such that $f(a \cdot b) = f(a) \odot f(b)$ where $\odot$ is multiplication modulo $q(Y)$ and $\cdot$ is multiplication modulo $p(X)$. Again, the value $f(X)$ will determine an isomorphism f from the representation modulo $p(X)$ to the representation modulo $q(Y)$.

If we find any one isomorphism from $GF(2)[X]/p(X)$ to $GF(2)[X]/q(Y)$ then we can get the whole set of isomorphisms by composing our one isomorphism with these automorphisms.

To get an isomorphism f, it is enough to find $f(X)$ which completely determines the isomorphism. To find this, we have to briefly work with p as a polynomial over $GF(2^8)$. So far, we have considered polynomials over $GF(2)$ to represent elements of $GF(2^8)$, i.e. our polynomials had coefficients in $GF(2)$. Now, we consider polynomials with coefficients in $GF(2^8)$. This can seem confusing at first because we will need two variable symbols: one to represent the "variable" of the polynomial and one to represent elements of $GF(2^8)$. For example, if a and b are elements of $GF(2^8)$ then $f(X) = aX + b$ is a polynomial over $GF(2^8)$ with coeffcients a, b. Suppose that $a = Y^2 + 1$ and $b = 2Y$, so we are using the letter Y to represent elements, then $f(X) = (Y^2 + 1)X + 2Y$. f is still a degree-one polynomial in one variable X; we just needed another variable symbol Y to write some of the coefficients which are elements of $GF(2^8)$.

In $GF(2^8)$ represented modulo p, we have $p(X) = 0$. So for any isomorphism f out of this representation we also have $f(p(X)) = 0$. But since f is an isomorphism we must also have $p(f(X)) = 0$. This means that $f(X)$, which is an element of the representation modulo q, must be a zero of the polynomial p modulo q. So our recipe for finding isomorphisms is to factor the polynomial $p(X)$ in the representation modulo $q(Y)$, where we treat X as a variable. In other words, we are looking for elements b such that $(X - b)$ divides $p(X)$ modulo $q(Y)$.

Theorem 6.5. A function f is an isomorphism from $GF(z^n)$ represented modulo $p(X)$ to $GF(z^n)$ represented modulo $q(Y)$ if and only if f commutes with addition and multiplication, $f(1) = 1$ and for $b = f(X)$, $(X - b)$ divides $p(X)$ as polynomials modulo $q(Y)$.

One of the isomorphisms has $b = Y + 1$. We can check this by computing $p(X)/(X - (Y + 1))$ modulo $q(Y)$ and find

$$\begin{aligned}(X^8 + X^4 + X^3 + X + 1) = (X - (Y + 1)) \cdot (& \\ 1 & \; X^7 \\ +(Y + 1) & \; X^6 \\ +(Y^2 + 1) & \; X^5 \\ +(Y^3 + Y^2 + Y + 1) & \; X^4 \\ +Y^4 & \; X^3 \\ +(Y^5 + Y^4 + 1) & \; X^2 \\ +(Y^6 + Y^4 + Y + 1) & \; X \\ +(Y^7 + Y^6 + Y^5 + Y^4 + Y^2) & \\ ) \pmod{q(Y)} &\end{aligned}$$

If the mixture of X and Y variables is confusing, we can also represent elements of $GF(2)[Y]/(Y + 1)$ as two-digit hexadecimal numbers. In this case, $b = \texttt{0x03}$ and the above equation is

$$(X^8 + X^4 + X^3 + X + 1) = (X - \texttt{0x03})(X^7 + \texttt{0x03}\,X^6 + \texttt{0x05}\,X^5 + \texttt{0x0f}\,X^4 + \texttt{0x10}\,X^3 + \texttt{0x31}\,X^2 + \texttt{0x53}\,X + \texttt{0xf4}) \pmod{q(Y)}$$

6.13 Factoring polynomials in SAGE

Factoring polynomials to find isomorphisms, like factoring integers, is a job best delegated to computers. This is how one can use SAGE to factor polynomials.

```
1  F=GF(2)
2  R.<x>=F[x]
3  U.<y>=GF(2^8,modulus=x^8+x^4+x^3+x^2+1)
4  S.<x>=U[x]
5  S(x^8+x^4+x^3+x+1).factor()
```

```
(x + y + 1) * (x + y^2 + 1) * (x + y^4 + 1) *
(x + y^4 + y^3 + y^2) * (x + y^6 + y^3 + y^2 + 1) *
(x + y^6 + y^4 + y^3 + y^2 + y) * (x + y^7 + y^2) *
(x + y^7 + y^4 + y^3 + y^2)
```

In line 3 we set up the finite field U with a modulus of our choice; lines 1 and 2 prepare this (we can only use a custom modulus if we have bound the variable to the correct ring). Line 4 constructs S as the polynomial ring over our finite field, (re-)using the variable x. In line 5 we finally take the polynomial that we want to factor, inject it into the ring S and then call the factor operation. The factors are presented as field elements (of U) using the variable y.

So the 8 isomorphisms of $GF(2^8)$ from the representation modulo $p(X) = X^8 + X^4 + X^3 + X + 1$ to the representation modulo $q(Y) = Y^8 + Y^4 + Y^3 + Y^2 + 1$ are the functions $f_1, \ldots, f_8$ with

$$\begin{array}{ll} f_1(X) = Y + 1 & f_2(X) = Y^2 + 1 \\ f_3(X) = Y^4 + 1 & f_4(X) = Y^4 + Y^3 + Y^2 \\ f_5(X) = Y^6 + Y^3 + Y^2 + 1 & f_6(X) = Y^6 + Y^4 + Y^3 + Y^2 + 1 \\ f_7(X) = Y^7 + Y^2 & f_8(X) = Y^7 + Y^4 + Y^3 + Y^2 \end{array}$$

Exercise. ($\star\star$) *Computation in* $GF(2^8)$. Let $p(X) = X^8 + X^4 + X^3 + X + 1$.

- Compute $(X^7 + X + 1)(X^6 + X^3 + X) + (X^7 + X^2 + 1)$ in $GF(2^8)$ using the representiation modulo $p(X)$.
- Solve the equation $X^3 + X + 1 = W \cdot (X^5 + 1)$ for W in $GF(2^8)$ represented modulo $p(X)$. Note: W is a polynomial, not an integer.
- Compute the powers of the Frobenius map in $GF(2^8)$ modulo $r(Z) = Z^8 + Z^7 + Z^2 + Z + 1$ (this is irreducible).
- Find an isomorphism from $GF(2)[Z]/r(Z)$ to $GF(2)[X]/p(X)$.

Exercise. ($\star$) *Computation in* $GF(2^3)$. Once you have mastered finite fields, you will be expected to solve exercises like this one for small enough fields almost as easily as arithmetic on integers. This exercise contains a lot of computations, each of which should be quick and easy.

We consider the field $GF(2^3)$ in the representations modulo the irreducible polynomials $p(X) = X^3 + X + 1$ and $q(Y) = Y^3 + Y^2 + 1$.

1. Reduce X^3 and X^4 modulo $p(X)$ and Y^3 and Y^4 modulo $q(Y)$.
2. How many elements does the group of automorphisms of $GF(2^3)$ have? What are these elements "called"?
3. Compute the Frobenius map for the representations modulo $p(X)$ and $q(Y)$. The quickest way to do this is to start with $\phi(X) = X^2$ and find $\phi(X^2)$, then express ϕ for an arbitrary field element as $\phi(aX^2 + bX + c) = uX^2 + vX + w$, i.e. find u, v, w in terms of a, b, c.

4. Do the same for all powers of the Frobenius map, in both representations (hint: there aren't too many.)
5. Find all the isomorphisms from the representation modulo $p(X)$ to the representation modulo $q(Y)$. Hint: how many are there? Find one isomorphism, then derive the others as follows: if f is one isomorphism and a is an automorphism of $GF(2^3)$ represented modulo $p(X)$, then $g = f \circ a$ is an isomorphism too. So compute $f(a(X))$ to get the value of $g(X)$.
6. ($\star\star$) Find the explicit multiplication formulas in both representations. That is, for $(aX^2 + bX + c)(dX^2 + eX + f) = (uX^2 + vX + w)$ find u, v, w in terms of a to f. Repeat the same for Y.

◇ You might be wondering why we can factor $p(X)$ when we chose it to be irreducible, otherwise we wouldn't have got a field in the first place. $p(X)$ is indeed irreducible over $GF(2)[X]$ but not anymore over $GF(2^8)$. This is a similar situation to saying that 3 is prime (irreducible) in $\mathbb{Z}$ but not anymore in $\mathbb{Q}$ since it has an inverse there.

In fact something even more interesting is happening. Over $\mathbb{R}$, the polynomial $X^2 + 1$ has no zeroes but if we extend to the complex numbers $\mathbb{C}$ then $X^2 + 1$, along with every other polynomial, splits into linear factors. The same happens in finite fields: every polynomial splits into linear factors over any finite field. In a sense, finite fields not only abandon the distinction between positive and negative numbers, they also abandon the distinction between real and imaginary numbers.