Lecture 27

It is a fairly difficult theorem to show that any two finite fields of the same order (that is, having the same number of elements) are isomorphic. I want to illustrate this with a couple of examples.

Example 1.

Show that $\mathbb{Z}_5[x]_{x^2+2}$ is a field and that it is isomorphic to $\mathbb{Z}_5[y]_{y^2+y+1}$.

First $x^2 + 2$ and $y^2 + y + 1$ have no roots in $\mathbb{Z}_5$ and so are prime polynomials in $\mathbb{Z}_5[x]$. Hence both $\mathbb{Z}_5[x]_{x^2+2}$ and $\mathbb{Z}_5[y]_{y^2+y+1}$ are fields with $5^2$ elements.

That they are isomorphic is interesting. Indeed there are exactly two isomorphisms between the two fields. Note of course that $x \rightarrow y$ is not an isomorphism since $y^2 + y + 1 \neq 0$ in $\mathbb{Z}_5[y]_{y^2+y+1}$.

Search for an element $a + by \in \mathbb{Z}_5[y]_{y^2+y+1}$ such that $(a + by)^2 + 2 = 0$. The miracle is that there are exactly two such elements. We need

\[
\begin{align*}
  a^2 + 2aby + b^2y^2 + 2 &= 0 \\
  a^2 + b^2(-1 - y) + 2aby + 2 &= 0 \\
  a^2 - b^2 + 2 + by(2a - b) &= 0, \text{ and so} \\
  a^2 - b^2 + 2 &= 0, \text{ and} \\
  b(2a - b) &= 0.
\end{align*}
\]

First $b \neq 0$ since there is no value of $a$ such that $a^2 + 2 = 0 \in \mathbb{Z}_5$. So we must have $b = 2a$ and then $a^2 - b^2 + 2 = a^2 - 4a^2 + 2 = 2a^2 + 2 = 0$. Hence $a = \pm 2$ and so $b = \pm 4$. Hence if there is an isomorphism $\varphi$ between the two fields it must be defined by

\[\varphi(x) = \pm(2 + 4y).\]

It is routine to check that this map $\varphi(a + bx) = a \pm b(2 + 4y)$ remembers addition and multiplication and so is an isomorphism, for each choice of $\pm 1$.

Example 2. Show that $x^4 + x + 1$ and $x^4 + x^3 + 1$ are prime in $\mathbb{Z}_2[x]$. Hence construct fields $\mathbb{F} = \mathbb{Z}_2[x]_{x^4+x+1}$ and $\mathbb{F}' = \mathbb{Z}_2[y]_{y^4+y^3+1}$ with 16 elements. Find four isomorphisms between $\mathbb{F}$ and $\mathbb{F}'$.

Here is a list of primes in $\mathbb{Z}_2[x]_{\text{mat}}$

\[
\begin{align*}
x &
x + 1 \\
x^2 + x + 1 &
\end{align*}
\]

\[
\begin{align*}
x^3 + x + 1 &
x^3 + x^2 + 1 \\
x^4 + x + 1 &
x^4 + x^3 + 1 \quad x^4 + x^3 + x^2 + x + 1
\end{align*}
\]

Easy to show that the two polynomials are prime in $\mathbb{Z}_2[x]$. Neither of them have any roots and so neither of them has a linear factor. On the other hand, there is only one quadratic
prime polynomial in $\mathbb{Z}_2[x]$, namely $x^2 + x + 1$. Hence if these quartics are products of prime quadratics, they must be $(x^2 + x + 1)^2 = x^4 + x^2 + 1$.

Hence both $x^4 + x + 1$ and $x^4 + x^3 + 1$ are prime in $\mathbb{Z}_2[x]$ and by Theorem 48, both $\mathbb{Z}_2[x]_{x^4 + x + 1}$ and $\mathbb{Z}_2[y]_{y^4 + y^3 + 1}$ are fields. There is no need (but not much difficulty) to calculate the inverses of elements. For example, for $\mathbb{F} = \mathbb{Z}_2[x]_{x^4 + x + 1}$:

$$\begin{array}{cccccc}
X & 0 & 1 & x & x + 1 & x^2 \\
X^{-1} & * & 1 & x^3 + x^2 & x^3 + x^2 + x & x^3 + x^2 + 1 \\
\end{array}$$

$$\begin{array}{cccccc}
X & x^2 + 1 & x^2 + x & x^2 + x + 1 & x^3 & x^3 + 1 \\
X^{-1} & x^3 + x + 1 & x^2 + x + 1 & x^2 + x & x^3 + x^2 + x + 1 & x \\
\end{array}$$

$$\begin{array}{cccccc}
X & x^3 + x & x^3 + x + 1 & x^3 + x^2 & x^3 + x^2 + 1 & x^3 + x^2 + x & x^3 + x^2 + x + 1 \\
X^{-1} & x^3 + x^2 & x^2 + 1 & x^3 + x & x^2 & x + 1 & x^3 \\
\end{array}$$

Just for fun you can see that $\mathbb{Z}_2[x]_{x^4 + x + 1}$ has a generator $x$, in fact. The generators are thus: 

$$x, x^2, x^4, x^7, x^{11}, x^{13}, x^{14}.$$ 

Check that the polynomial $X^4 + X + 1$ has roots $x, x^2, x^4 = x + 1$, $x^8 = (x + 1)^2 = x^2 + 1 \in \mathbb{F}$. So

$$X^4 + X + 1 = (X + x)(X + x^2)(X + x + 1)(X + x^2 + 1).$$

Check also that $X^4 + X^3 + 1 = 0$ has four roots in $\mathbb{F}$ also. They are 

$$x^3 + 1,$$

$$(x^3 + 1)^2 = x^6 + 1$$

$$= x^2(x + 1) + 1$$

$$= x^3 + x^2 + 1,$$

$$(x^3 + 1)^4 = x^{12} + 1$$

$$= (x + 1)^3 + 1$$

$$= x^3 + x^2 + x + 1 + 1$$

$$= x^3 + x^2 + x,$$ and

$$(x^3 + 1)^8 = x^{24} + 1$$

$$= (x^8)^3 + 1$$

$$= (x^2 + 1)^3 + 1$$

$$= x^6 + x^4 + x^2 + 1 + 1$$

$$= x^2(x + 1) + (x + 1) + x^2$$

$$= x^3 + x + 1.$$ 

Hence

$$X^4 + X^3 + 1 = (X + x^3 + 1)(X + x^3 + x^2 + 1)(X + x^3 + x^2 + x)(X + x^3 + x + 1).$$

There are four isomorphisms from $\mathbb{F} = \mathbb{Z}_2[x]_{x^4 + x + 1}$ to $\mathbb{Z}_2[y]_{y^4 + y^3 + 1}$, given by:
1. \( x \rightarrow y^3 + 1 \)
2. \( x \rightarrow y^3 + y + 1 \)
3. \( x \rightarrow y^3 + y^2 + y \)
4. \( y \rightarrow y^3 + y + 1 \).

I’m only including this calculation here to show that this can be done in a few minutes of calculation - with a pen and no computer. You should try it.

I want us to see more properties of fields before leaving them.

If \( F \) is a field, then consider the set of all sums \( 1_F, 1_F + 1_F, \ldots, 1_F + 1_F + \ldots + 1_F \). If there exists \( k \) such that \( k1 = (1 + 1 + \ldots + 1) = 0 \), the smallest such positive \( k \) is called the characteristic of the field.

**Definition** If \( F \) is a field then \( \text{char} \ F \) is the smallest positive integer \( k \) such that \( k.1 = 0 \), if one exists. Otherwise \( \text{char} \ F = 0 \).

**Theorem 49**

(i) If \( F \) is a field of characteristic \( \neq 0 \), then \( \text{char}(F) = p \) a prime and \( F \) contains a subfield isomorphic to \( \mathbb{Z}_p \).

(ii) If \( F \) has characteristic 0, then \( F \) contains a subfield isomorphic to \( \mathbb{Q} \).

*Remark: Such a subfield is called the ground field. Usually we decide to agree that \( \mathbb{Z}_p \) or \( \mathbb{Q} \) are not only isomorphic to a subfield of \( F \) but are equal to a subfield of \( F \). This makes the notation easier.*

Proof. Suppose that \( k \) is the least positive integer such that \( k.1 = 0 \in F \). Then if \( k = ab \) we have \( ab.1_F = a.1_F \cdot b1_F = 0 \). In a field, if \( a.1_F \neq 0 \) we can divide by it and get \( b.1_F = 0 \). Hence either \( a.1_F = 0 \) or \( b.1_F = 0 \). In either case, the minimality of \( k \) gives a contradiction and so \( k \) is a prime, \( \text{char}(F) = p \) is prime.

It is clear that in this case, \( \{n.1_F : n = 0, 1, \ldots, p - 1\} \) is a subfield isomorphic to \( \mathbb{Z}_p \) by an obvious isomorphism.

(ii) If \( k.1_F \neq 0 \) for any \( k \in \mathbb{Z} \), then since \( F \) is a field, it follows that

\[
\left\{ \frac{p.1_F}{q.1_F} : p, q \in \mathbb{Z}, q \neq 0 \right\}
\]

is a subfield of \( F \) isomorphic to \( \mathbb{Q} \) again by an obvious isomorphism.

This completes the proof.