Week 12

Theorem (Wilson) Let p ba a prime. Then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Sine p is a prime, $< \mathbb{Z}_p^* , \cdot >$ is a group. Therefore each element in $\mathbb{Z}_p^*$ has an inverse element. This implies that $\mathbb{Z}_p$ has no zero divisors. Hence the equation $x^2 - 1 \equiv 0 \pmod{p}$ has exactly two solutions in $\mathbb{Z}_p^*$, 1 and $p-1$. So, all the other elements $a \in \mathbb{Z}_p^* \setminus \{1, p-1\}$ has an inverse which is not a itself. Thus, we conclude that $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$ ■

Example of division ring which is not a field

$(*)$ By Wedderburn's Theorem, every finite division ring is a field, we have to find an example with infinite elements.

The Quaternions

$R = \mathbb{R}^4$, $1 = (1,0,0,0)$, $i = (0,1,0,0)$, $j = (0,0,1,0)$, $k = (0,0,0,1)$,

$\forall\ x \in R$, $x = a_1 + a_2 i + a_3 j + a_4 k = (a_1, a_2, a_3, a_4)$. $i^2 = j^2 = k^2 = -1$,

$ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i$ and $ik = -j$.

$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) =$

$(a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$.

$(a_1+a_2 i+a_3 j+a_4 k)(b_1+b_2 i+b_3 j+b_4 k) = (a_1 b_3 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)i + (a_1 b_3 + a_2 b_4 + a_3 b_1 - a_4 b_2)j + (a_1 b_4 + a_2 b_3 + a_3 b_2 - a_4 b_1)k$.

Then $< R, +, \cdot >$ is a division ring.

Since the other properties of a division ring is easy to see, we check that each element in R has an inverse (multiplication). By the definition of multiplication, an element $a = a_1 + a_2 i + a_3 j + a_4 k$ has an inverse if and only if

$$det \begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{bmatrix} \neq 0$$

and this can be checked by finding the determinant. In fact, the inverse of a is $\frac{1}{\|a\|}(a_1 - a_2 i - a_3 j - a_4 k)$ where $\|a\| = \sum_{i=1}^{4} a_i^2$.

How to construct a field by using an integral domain?

Step 1 Let $S = \{(a, b) \mid a, b \in D \text{ and } b \neq 0\}$ where D is an integral domain.

Step 2 Partition S into equivalence classes $[(a, b)]$ where the equivalence relation $\sim$ in S is defined by $(a_1, b_1) \sim (a_2, b_2)$ if and only if $a_1 b_2 = a_2 b_1$.

Step 3 Let F be the set of all equivalence classes obtained in Step 2 and treat each classes as an element.

Theorem (The field of quotients of an integral domain)

$< F, +, \cdot >$ is a field where $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$ and $[(a,b)] \cdot [(c,d)] = [(ac, bd)]$.

Proof.

1° Well-defined. $(+)$

Let $(a_1, b_1) \in [(a,b)]$ and $(c_1, d_1) \in [(c,d)]$. It suffices to show that $(a_1d_1 + b_1c_1, b_1d_1) \in [(ad+bc, bd)]$, i.e.,

$$(a_1d_1 + b_1c_1)bd = b_1d_1(ad+bc).$$

Since $a_1b = b_1a$ and $c_{1d} = d_1c$ the left hand side is equal to $a_1d_1bd + b_1c_1bd = b_1d_1ad + b_1d_1cd$. Thus, we have the proof. ■

2° Well-defined. $(\cdot)$

We claim $(a_1c_1, b_1d_1) = (ac, bd)$. This is followed by $(ac)(b_1d_1) = a_1bcd_1 = a_1bc_1d = (a_1c_1)(bd)$.

3° $< F, + >$ is an abelian group.

4° $< F^*, \cdot >$ is an abelian group.

5° The distributive laws hold in F.

Note $0 = [(0,1)]$, $[(a,b)] + [(-a,b)] = 0$, $[(a,b)][(b,a)] = 1$ where $1 = [(1,1)]$. (Remember that D is an integral domain.) ■

Step 4 The field F from Step 3 can be considered as a field which contains D.

Lemma The map $\pi : D \to F$ given by $\pi(a) = [(a, 1)]$ is a 1-1 homomorphism from D into F, i.e., D is isomorphic to a subring of F.

Proof. $\pi(a + b) = [(a + b, 1)] = [(a, 1)] + [(b, 1)] = \pi(a) + \pi(b)$.
$\pi(a \cdot b) = [(ab, 1)] = [(a, 1)][(b, 1)] = \pi(a)\pi(b)$.
$\pi(x) = \pi(y) \Rightarrow [(x, 1)] = [(y, 1)] \Rightarrow x \cdot 1 = y \cdot 1 \Rightarrow x = y$. ■

Step 5 Any two fields of quotients of D are isomorphic.

Theorem Let L be a field containing D and F be the field of quotients of D. Then there exists a subfield of L, L', $F \cong L'$, moreover, if ψ is the isomorphism, then $\forall\ a \in D \quad \psi(a) = a$.

Proof. Let ψ be the map such that $\psi(a) = a \quad \forall\ a \in D$ and $\psi(a/_F b) = \psi(a)/_{L'}\psi(b)$ where $a/_F b$ denotes the quotient of a by b i.e., $a/_F b \leftrightarrow [(a, b)]$ in the meaning of quotients defined in Step 2.

Check ψ is well-defined and ψ is an isomorphism.

1° If $a/_F b = c/_F d$, then $ad = bc$ in D. Hence $\psi(ad) = \psi(bc)$, $\psi(ad) = ad = \psi(a)\psi(d) = \psi(b)\psi(c)$. This implies that $\psi(a)/_{L'}\psi(b) = \psi(c)/_{L'}\psi(d)$. ψ is well-defined.

2° $\psi(a/_F b + c/_F d) = \psi(ad + bc/_F bd) = \psi(ad + bc)/_{L'}\psi(bd)$
$= ad + bc/_F bd = a/_F b + c/_F d = \psi(a)/_{L'}\psi(b) + \psi(c)/_{L'}\psi(d)$
$= \psi(a/_F b) + \psi(c/_F d)$.
The others can also be proved similarly. ■

Corollary Every field L containing an integral domain D contains a field of quotients of D.

Proof. Since every element of L' is of the form $\psi(a)/_{L'}\psi(b)$, L contains a field of quotients of D. (By above theorem.) ■

Corollary Any fields of quotients of an integral domain are isomorphic.

Proof. Every field of quotient of an integral domain D is isomorphic to the same field L' in the above theorem. ■

Example $< \mathbb{C}, +, \cdot >$ is a field.
$D = \{m + ni \mid m, n \in \mathbb{Z}\}$ is an integral subdomain of $\mathbb{C}$ (complex number). D is the set of Guassian integers.
Then we can define the quotients of D as above and in fact it is the set $\{a + bi \mid a, b \in \mathbb{Q}\}$ which is a field.

Example $< \mathbb{Z}, +, \cdot >$ is also an integral subdomain of $\mathbb{C}$. The field of quotients of $\mathbb{Z}$ is "$\mathbb{Q}$".

Theorem Let R be a ring in which $x^3 = x$ for each $x \in R$. Then R is a commutative ring.

Proof.

Claim 1 If $a^2 = a$ and $\forall\ m \in \mathbb{Z}^+,\ a^m \neq 0$ where $a \neq 0$, then $ax = xa$ for each $x \in R$.

$$(ax - axa)^2 = (ax)(ax) - (ax)(axa) + (axa)(ax) + (axa)(axa)$$
$$= axax - axaxa - axax + axaxa = 0$$

$(xa - axa)^2 = 0.$

$\Rightarrow ax - axa = 0$ and $xa - axa = 0 \Rightarrow ax = xa.$

Claim 2 If $x^3 = x$, then R contains no a s.t. $a^m = 0$ for $m \in \mathbb{Z}^+$ and $a \neq 0$.

Suppose not. Let $m \in \mathbb{Z}^+$, and $a^m = 0$, m is the smallest one.

1. If $m \equiv 0 \pmod 3$, then $a^m = (a^{\frac{m}{3}})^3 = a^{\frac{m}{3}} = 0\ \rightarrow\leftarrow$.
2. If $m \equiv 1 \pmod 3$, then $a^m \cdot a^2 = a^{3k+3} = a^{k+1} = 0\ \rightarrow\leftarrow$.
3. If $m \equiv 2 \pmod 3$, then $a^m \cdot a = a^{3k+3} = a^{k+1} = 0\ \rightarrow\leftarrow$.

Claim 3 $\forall\ x \in R\quad (x^2)^2 = x^4 = x^3x = x^2$, hence $x^2z = zx^2\ \forall\ z \in R$ (by Claim 1 and 2).

$xyxy = x^2xyxy = x(xy)^2x = xxyxyx = x^2(yx)(yx) = (yx)(yx)x^2 = yxyx$

$(*)\quad xy = (xy)^3 = xyxyxy = xyyxyx = xy^2xyx = x^2yx = yx^3 = yx.$