14. 09. 2006

Tutorial #1

In the field $0 \neq 1$

in field $(ab)c = a(bc)$ is hard to check.

① Prove that in any field there are no zero divisors.

Def: $a \in F$ is a zero divisor in F. By def'n this means that $\exists$ nonzero $b \in F$

$a.b = 0$ ⊛

By F4 $\exists\, b^{-1}$ s.t. $b.b^{-1} = 1$

Now multiply ⊛ by b^{-1} on the right

$a = a \cdot \underbrace{b \cdot b^{-1}}_{1} = 0 \cdot b^{-1} = 0$

Hence $a = 0$, contradiction proves the claim. Denote "contradiction" by $\lightning$.

examples of a set with zero divisors reminders of division by 4

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$: $\bar{2}.\bar{2} = \bar{4} = \bar{0}$ $\mathbb{Z}/4\mathbb{Z}$ not a field.

but $\mathbb{Z}/5\mathbb{Z}$ or more general $\mathbb{Z}/\text{prime}\,\mathbb{Z}$.

② remark: If we drop the axiom F1 then it can be shown that if the left and

right inverses of $a \in F$ do exist then they are equal.

Indeed: let $a \in F$ & $a_l^{-1} \in F$ be its left inverse

$a_l^{-1} \cdot a = 1$ $(*)$

likewise $a_r^{-1} \in F$ be its right inverse $a \cdot a_r^{-1} = 1$ $(**)$

Then

$$a_l^{-1} = a_l^{-1}\cdot 1 \overset{b(*)}{=} a_l^{-1}(a\cdot a_r^{-1}) \overset{F_2}{=} (a_l^{-1}\cdot a)a_r^{-1} \overset{(**)}{=} 1\, a_r^{-1} = a_r^{-1}$$

$\Rightarrow a_l^{-1} = a_r^{-1}$

(3) Prove that $\forall\, a,b \in F$, $(a,b)^n = a^n \cdot b^n$, $n \in N \to \{1,2,\dots\}$

Proof: is by induction on n.

$n=1$ $\quad ab = ab$

$n=2$ $\quad (ab)^2 = (ab)(ab) \overset{F_2}{=} a(ba)b = a(ab)b = a^2b^2$

you don't need this part for induction

Assume that the equality $(*)$ is valid for $n=k-1$

Let us prove it for $n=k$

$$(ab)^k = (ab)^{k-1}(ab) \xrightarrow[\text{of induction}]{\text{main step}} a^{k-1}b^{k-1}ab \overset{F_2}{=} a^{k-1}\cdot a\cdot b^{k-1}\cdot b$$

(4) Prove that in a field $(a+b)^2 = a^2 + 2ab + b^2$ in $\mathbb{R}$

proof

$$(a+b)^2 = (a+b)(a+b) \overset{F_5}{=} a^2 + ab + ba + b^2 \xrightarrow{F_1(\text{multiplicative})} a^2 + ab + ab + b^2 = a^2 + 2ab + b^2$$

⚠ important remark $\exists$ fields with 3 elements $\{\bar{0}, \bar{1}, \bar{2}\}$

think how to define multiplication here s.t. this will become a field

Hint: there are the reminders mod 3

⑤ Prove that the set $\mathbb{Q}(i) = \{ a+ib,\ a,b \in \mathbb{Q} \}$ it is called one extension field of $\mathbb{Q}$ by i)

Proof: F1, F2, F3, F5 trivial

Multiplication is given by $(a_1+ib_1)(a_2+ib_2) := (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)$

The only hard axiom to check F4 (mult. inverse)

Assume that $a+ib \in \mathbb{Q}(i)$. We are looking for $c+id \in \mathbb{Q}(i)$ s.t.

$(a+ib)(c+id) = 1(1+i0)$ $\qquad b \neq 0$

by defn of multiplication in $\mathbb{Q}(i)$

$(a+ib)(c+id) = (ac-bd) + i(ad+bc) = 1+i0$

Then $\begin{cases} ac-bd=1 \\ ad+bc=0 \end{cases} \Rightarrow$ $c = -\frac{ad}{b}$ plug into 1st equation $\quad \frac{-a^2d - b^2d}{b} = 1$

$-\frac{a^2d}{b} - bd = 1$ $\qquad \left(\frac{-a^2-b^2}{b}\right)d = 1$

$d = -\frac{b}{a^2+b^2}$

but then

$c = -\frac{ad}{b} = -\frac{a}{b}\left(-\frac{b}{a^2+b^2}\right) = \frac{a}{a^2+b^2}$

$\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ is the inverse of $a+ib$.

Note that it lies inside $\mathbb{Q}(i)$