Notes

October 31, 2014

4.1 #9,12,13

9

$(a^{-1})^{-1} = e(a^{-1})^{-1} = a(a^{-1}(a^{-1})^{-1}) = ae = a$

Note that $-e \cdot -e = e$ $(-a)^{-1} = (e \cdot -a)^{-1} = -e \cdot a)^{-1} = (-e)^{-1}a^{-1} = -ea^{-1} = e \cdot -a^{-1} = -a^{-1}$

last time

examples always keep in mind, $\mathbb{R}\mathbb{Q}\mathbb{C}\mathbb{Z}_p$

$\mathbb{Z}_n$ is a field iff n is prime

$\rightarrow$ n not prime take $m|n, m < n$ then $[m]$ is not invertible so n is prime

def

we say that for polynomials $g(x)|f(x) \in K[x]$ if $\exists h(x)$ such that $f(x) = g(x)h(x)$

for example $(x+1)|(x^2-1)$ in $\mathbb{R}[x]$. $(x+1) \not| (x^2+1)$ in $\mathbb{R}[x]$ but it does in $\mathbb{Z}_2[x]$: $(x+1)(x+1) = x^2+x+x+1 = x^2+x(1+1)+1 = x^2+x(0)+1 = x^2+1$

in $\mathbb{Z}_p$ $(a+b)^p = a^p + b^p$.

thm

if K is a field and $c \in K$ and $f(x) \in K[x]$ then there exists a unique $g(x) \in K[x]$ such that $f(x) = g(x)(x-c) + f(c)$.

proof

claim $x - c|f(x) - f(c)$. $f(x) = a_m x^m + \cdots + a_1 x + a_0$ $f(c) = a_m c^m + \cdots + a_1 c + a_0$ $f(x) - f(c) = a_m(x - c^m) + \cdots + a_1(x - c)$

$x^t - c^t = (x-c)(x^{t-1} + x^{t-2}c + x^{t-3}c^2 + \cdots + xc^{t-2} + c^{t-1}$

and so $f(x) - f(c) = g(x)(x-c) \rightarrow f(x) = g(x)(x-c) + f(c)$.

now assume we have $g'(x)$ and $g(x)$ that satisfy then $g(x)(x-c) - f(c) = g'(x)(x-c) - f(c) \rightarrow (x-c)(g(x) - g'(x)) = 0$. $x - c$ has a coefficient of 1 and so is not zero so $g(x) - g'(x) = 0$ and is unique.

def

$c \in K$ is called a root of $f(x) \in K[x]$ if $f(c) = 0$.

c is a root of $f(x)$ iff $x - c$ divides $f(x)$

$\rightarrow$ assume c is root, then $f(c) = 0$. by previous theorem $\exists q(x) \in K[x]$ such that $f(x) = q(x)(x-c) + f(c) = q(x)(x-c)$ so $(x-c)$ divides $f(x)$

$\leftarrow$ assume $(x-c)$ divides $f(x)$. then $f(x) = h(x)(x-c) \rightarrow f(c) = h(c)(c-c) = h(c) \cdot 0 = 0$.

corollary

$f(x) \in K[x]$, $\deg f = n$. then $f(x)$ has at most n distinct roots. (assuming non-zero polynomial)

induction on n.

$n = 0$ then $f(x) = c \neq 0$. $n = 1$ then $f(x) = a_1 x + a_0$, $a_1 \neq 0$.

assume $c \neq d$ are solutions. then $f(x) = (x - c)q(x)$ and $f(d) = (d - c)q(d)$. note that $(d - c) \neq 0$ then $q(d) = 0$ and then

now take a polynomial of degree $n - 1$ that has $n - 1$. if it has no roots, we are done.