CS 235: Algebraic Algorithms, Spring 2021

Discussion 8

Tuesday, April 13^{th}, 2021.

Problem 1. Let R be a non-trivial ring. Show that for some $a, b \in R$ such that $ab = 1$, if either a or b is a Zero Divisor then $ba = 1$.

Def 7.1: the set of numbers R is a ring:

(i) R forms a group under $+$-op, 0_R

(ii) $(ab)c = a(bc)$ for $a, b, c \in R$

(iii) $a(b+c) = ab + ac$

(iv) $\exists 1_R \therefore 1 \cdot a = a \cdot 1 = a$, for $a \in R$

(v) $ab = ba$, for $a, b \in R$

$a, b \neq 0 \in R$ s.t. $ab = 0 \Rightarrow a$ & b are zero divisors

Ex: $3, 5 \in \mathbb{Z}_{15}$, $3 5 \equiv 0 \pmod{15}$

$\mathbb{Z}_p$ doesn't have zero divisors

Pf: Suppose a is not a zero divisor

$\therefore$ if $a \cdot x = 0$, then $x = 0$

Consider $x = (ba - 1)$

$\Rightarrow a(\underbrace{ba - 1}_{x}) = aba - a$ (7.1 iii)

$= 1 \cdot a - a = 0$

$\Rightarrow x = ba - 1 = 0 \Rightarrow ba = 1$

Similarly, consider $(ba-1)b \Rightarrow ba - 1 = 0$

Problem 2. Let S and T be subrings of ring R. Show that $S \cap T$ is also a subring of R.

S is (an additive) subring of R:

(i) S is an additive subgroup of R

i.1) $a+b \in S$, for $a, b \in S$ ✓

i.2) $-a \in S$, for $a \in S$.

(ii) $ab \in S$ for $a, b \in S$ ✓

(iii) $1_R \in S$

Pf: Let $a, b \in S \cap T \Rightarrow a, b \in S$; $a, b \in T$

Since S, T are subrings of R, we have

$$\begin{cases} a+b \in S \\ ab \in S \end{cases} \qquad \begin{cases} a+b \in T \\ ab \in T \end{cases}$$

$\Rightarrow a+b \in S \cap T$ & $ab \in S \cap T$

Let $x \in S \cap T \Rightarrow x \in S$ & $x \in T$

Since S, T are subrings, we have:

$-x \in T$ & $-x \in S \Rightarrow -x \in S \cap T$

$\Rightarrow$ every element in $S \cap T$ has additive inverse

Similary, $1_R \in S \cap T$

Hence $S \cap T$ is a subring

What about $S \cup T$? Not quite

$S \cup T$ is a subring $\Leftarrow$ $\left[\begin{array}{l} S \subset T \\ T \subset S \end{array} \right.$

Problem 3. Show that if F is a field, the units in $F[X]$ are exactly nonzero elements of F.

F is a field $\therefore$ F is a ring and every element in F has a mult. inverse

i.e $\underline{a} \in F$, $\exists\, r = a^{-1}$, $\underline{ar = 1}$

$\hookrightarrow$ is the unit

Ring / field F has elements which are numbers

F[X] has " polynomials

(e.g. $X^2 - 2X + 4 = f(X)$)

Pf: Let $f(X) \in F[X]$ of degree n

Then $f(X)$ is a unit if $\exists\, g(X)$ of degree m s.t. $\underline{f(X) \cdot g(X) = 1}$

$\deg(f \cdot g) = \deg(f) + \deg(g) = n + m$

$\deg(1) = 0 \Rightarrow n + m = 0$

Since $n, m \geq 0 \Rightarrow n = m = 0$

$\Rightarrow f(X)$ and $g(X)$ are constant functions

$\Rightarrow f \cdot g = 1 \Rightarrow f$ & g are units of F

$\underline{(F \subset F[X])}$