Math 152 Notes

Lucas Garron

September 26, 2009

20090924

If $R = Z$, I is called principal if I = all multiples of some $a \in R$.

If $a, b \in R$ (comm.), $a|b$ (a divides b) means $b = ac$ for some $c \in R$. Equivalent: b is a "multiple" of a, $b \equiv (moda)$

$b \equiv b' moda$ means $a|b - b'$

(a) = al multiples of a $= am|m \in R$ (ideal)

Greatest Common Divisor: "greater than" refers to ordering with respect to divisibility. A common divisor of a, b would be c s.t. $c|a$ and $c|b$. Finite such, so there's a largest. i.e. $\exists c$ s.t. $c|a$, $c|b$ and if $d|a$, $d|b$, then $c > d$ (Obvious.)

THEOREM: $\exists c$ (same c) with $c|a$, $c|b$ if $d|a$ and $d|b \Rightarrow d|c$ (which implies $d < c$ but has more content.)

Proof: Let $I = \{ma + nb|m, n \in R\}$ ideal $= (c)$ I = all mults. of c. $a = 1a + 0b \in I$ so a is a multiple of $c \in I$ so $c = m_0 a + n_0 b$ some m_0, n_0. Suppose $d|a, b$. $d|m_0 a, n_0 b \Rightarrow d|m_0 a + n_0 b = c$ QED.

Let R be a camm. ring. $\epsilon \in R$ is a unit if $\epsilon|1$, i.e. $1 = \epsilon\delta$ for some $\delta \in R$. a, b associates if $a = \epsilon b$ for ϵ a unit. (Equivalently: $a|b$ and $b|a$)

$p \in R$ is irreducible ("prime") if $p \neq 0$, p is not a unit, and $p = ab \Rightarrow$ a is a unit or b is a unit.

Proposition: If p is prime and $p = ab \Rightarrow p|a$ or $p|b$ (true if every ideal is principal). Proof: Let $i = \{ma + nb|m, n \in R\}$ is an ideal. I is principal., so $I = (c)$ for some c (c is $GCD(a, b)$) $a, p \in I$ ($a = 1 * a + 0 * p \in I$) So a, p are multiples of c. $c|p \Rightarrow$ c is a unit or c is an associate of p. ($c|p \Rightarrow$ c unit or c' unit. 2nd case: c, p assoc.)

Case 1: If c unit. $I = (c) = R$, so $1 \in I \Rightarrow 1 = mo + nb \exists m, n \in R$ $b = bma + bnp$ ($p = ab \Rightarrow p|$ both terms) So $p|b$.

Case 2: c is an assoc. of $p \Rightarrow I = (c)(p) \Rightarrow p|$(any alt of I). In particular, $a \in I \Rightarrow p|a$.

Corollary: If $p|a_1....a_n \Rightarrow \exists i$ $p|a_i$ (Induction.)

THEOREM: Suppose $a \neq 0$ and a not unit. Then $a = p_1...p_n$ has a factorization into primes. If $a = q_1...q_m$ is another factorization., then $m = n$ and the p_i are associates of q_i rearranged.

Proof: If a prime, $a = p_1$ ($p_1 = a$, $n = 1$) Otherwise a is divisible by some prime (true if every principal is ideal.) $a = p_1 a'$, $a' < a$, so by induction, $a' = p_2...p_n$, so a can be factored into primes. If $a = p_1...p_n = q_1...q_m$ are two such factorizations. $p_1|a = q_1...q_m \Rightarrow p_1|q_i \exists i$ (WLOG $i = 1$). $p_i|q_1$ means p_1, q_1 associates. (q_1 is a prime so q_1 $p_1\epsilon$. p_1 is not a unit, so ϵ is a unit $\Rightarrow p, q$ assoc.) $q_1 = p_1\epsilon$, $p_1...p_N = \epsilon q_1...q_M \Rightarrow p_2...p_N = \epsilon q_2...q_M = q_2' q_3...q_M$. $q_2' = \epsilon q_2$. By induction on N, thm is true for $a' = p_2...p_N = q_2'...q_M \Rightarrow N = M$, $q_2, ..., q_M$ are associates of $p_2, ..., p_N$

Used fact that we're in an integral domain: $ax = ay, a \neq 0 \Rightarrow x = y$.

THEOREM: (Fermat's Little Theorem) Let p be a prime. Then $a^p \equiv a$ mod p. This means $p|a^p - a$

If $p|a \Rightarrow p|a^p$, so $a^p \equiv 0 \equiv a$ mod p. Easy.. So assume p does not divide a. Then need to prove: $pnot|a \Rightarrow a^{p-1} \equiv 1$ mod p. ($a^p \equiv$ follows by multiplying by a.)