H.W.5

1.

F be a field

Claim: $F[x]$ is a ED ($\Rightarrow$ PID $\Rightarrow$ UFD)

$f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in F[x]$, $a_n \neq 0$

$g = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0 \in F[x]$, $b_m \neq 0$

check: $\exists q, r \in F[x]$ s.t. $f = qg + r$, $r = 0$ or $deg(r) < deg(g)$

$deg(g) = m \neq 0, b_m = 0$

Case1. $n < m$

let $q = 0, r = f$ then $f = 0g + f \therefore n = deg(r) < deg(g) = m$

Case2. $n \geq m$(By induction on n)

Basic step: $n = 0$ then $m = 0$

let $f = a_0, g = b_0 \neq 0$

let $q = a_0 b_0^{-1}$, then $a_0 = (a_0 b_0^{-1})b_0 + 0$ is true.

Induction step: Assume that $deg(f^{'}) < n$, the assertion is true.

let $f^{'} = f - (a_n b_m^{-1} x^{n-m})g = f - a_n x^n - a_n b_m^{-1} b_{m-1} x^{n-1} - ...$, then $deg(f^{'}) < n$.

(By induction hypothesis)$\exists q^{'}, r \in F[x]$ s.t. $f^{'} = q^{'}g + r$ where $r = 0$ or $deg(r) < deg(g)$.

Then $f - (a_n b_n^{-1} x^{n-m})g = q^{'}g + r$

Hence $f = qg + r$ $(q = q^{'} + a_n b_m^{'} x^{n-m})$ ∎

2.

(a)(i)$f(x) = a_0 +_1 x + ...$ where a_0 is unit in $\mathbb{R}$.

Then f is unit in $R[[x]]$.

Since 1 is unit in $\mathbb{Z}$.

Hence $x + 1$ is unit in $\mathbb{Z}[[x]]$.

(ii)Suppose $x + 1$ is unit in $\mathbb{Z}[x]$.

let $(x+1)^{-1} = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$

(i.e. $(x+1) * (a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0) = 1$)

Then $a_n x^{n+1} + (a_n + a_{n-1})x^n + ... + (a_1 + a_0)x + a_0 = 1$.

Then $a_0 = 1, a_1 = a_2 = ... = a_n = 0$. This implies $x + 1 = x$, a contradiction. ∎

(b)$x^2 + 3x + 2 = (x + 2)(x + 1)$

(i)$\because$ (a)$x + 1$ is unit in $\mathbb{Z}[[x]]$

Since $x + 2$ is irreducible in $\mathbb{Z}[[x]]$, $x^2 + 3x + 2$ is irreducible.

(ii)x+1,x+2 are nonunits in $\mathbb{Z}[x]$. ∎

3.

(a)$(x) = xf(x) | f(x) \in F[x]$

(i)Suppose (x) is not a maximal ideal, there exists M s.t. $(x) \subsetneq M \subsetneq F[x]$.

Then for every $g(x) \in M - (x)$, $g(x) = a + f(x)$ for some $f(x) \in (x)$ and $a \neq 0 \in F$.

Since $f(x), g(x) \in M$ and M is ideal, then $g(x) - f(x) \in M$.

For $h(x) \in F[x]$

Since $a \in M$ and M is ideal, then $ah(x) \in M$

$\because F$ is a field $\therefore \frac{h(x)}{a} \in F[x]$

Then $h(x) = a\frac{h(x)}{a} \in M$

Hence $F[x] \subsetneqq M \subsetneq F[x]$, a contradiction.
(ii)Claim: For $p(x)$ is irreducible, then (p(x)) is a maximal ideal.
Suppose not, there exists N be a maximal ideal s.t. $(p(x)) \subsetneq N \subsetneq F[x]$.
Since F is a field, implies $N = (g(x))$ (i.e. N is prime ideal).
There exists $q(x)$ s.t. $p(x) = g(x)q(x)$.
But $p(x)$ is irreducible, implies $g(x)$ or $q(x)$ is unit.
Thus $g(x)$ or $q(x) \in F$
W.L.O.G., let $q(x) \in F$
let $p(x) = cg(x)$ for $c \in F$
Then $g(x) = \frac{p(x)}{c}$
Thus $g(x) \in (p(x))$, a contradiction. ∎

(b)Claim: (i)$F[[x]]$ is an integral domain. (ii) All ideals are principle.
(i)check: $F[[x]]$ has no zero divisor.
let $A = \sum_{i=0}^{\infty} a_i x^i \neq 0$, $B = \sum_{i=0}^{\infty} b_i x^i \neq 0$
There exist $\alpha, \beta \in \mathbb{N}$ s.t. $a_\alpha, b_\beta \neq 0$ and $\forall i < \alpha, j < \beta$ $\alpha_i, \beta_j = 0$.
Then $AB = a_\alpha b_\beta x^{\alpha+\beta} + ... \neq 0$.
(ii)Pick an ideal $I \subsetneqq F[[x]]$.
Suppose $I \neq (0), (1)$.
Pick $0 \neq f(x) \in I$ with the lost degree term is the least among all nonzero elements in I.
Suppose $f(x) = a_i x^i + a_{i+1} x^{i+1} + ...$ where $a_i \neq 0$.
It is easy to check $I = (x^i)$, done! ∎

4.
(a)check: $\exists (1-ab)^{-1}$ s.t. $(1-ab)(1-ab)^{-1} = 1$ and $\exists (1-ba)^{-1}$ s.t. $(1-ba)(1-ba)^{-1} = 1$
Since $(1-ab)^{-1} = \frac{1}{1-ab} = 1 + ab + abab + ...$
then $(1-ba)^{-1} = \frac{1}{1-ba} = 1 + ba + baba + ... = 1 + b(1 + ab + abab + ...)a = 1 + b(1-ab)^{-1}a$
Hence $(1-ba)(1 + b(1-ab)^{-1}a) = 1 - ba + b(1-ab)^{-1}a - bab(1-ab)^{-1}a = 1 - b(1 - ab)(1-ab)^{-1}a = 1 - ba + ba = 1$
similarly, $(1 + b(1-ba)^{-1}a)(1-ab) = 1$ ∎

(b)Suppose not, assume that a has more than one right inverse and it has finitely many.
Let $b_1, b_2, ..., b_n$ are distinct right inverse of a.
Then $b_1, b_1 + 1 - b_1 a, , b_1 + 1 - b_2 a, , b_1 + 1 - b_3 a, ..., , b_1 + 1 - b_n a$, are n+1 distinct right inverse of a.
(1)$a(b_1 + 1 - b_i a) = ab_1 + a - (ab_i)a = 1 + a - a = 1$ for $i = 1, 2, ..., n$
(2)$b_1 + 1 - b_i a \neq b_1$ for $i = 1, 2, ..., n$
if $b_1 + 1 - b_i a = b_1$ for some i, then $b_i a = 1$
Pick b is a right inverse of a
Since $ab = 1$ then $b_i = b_i(ab) = (b_i a)b = b$
Implies, right inverse of a is uniquely determined, a contradiction.
(3)Claim: $b_1 + 1 - b_i a \neq b_1 + 1 - b_j a$ for $i \neq j$
if $b_1 + 1 - b_i a = b_1 + 1 - b_j a \Rightarrow b_i a = b_j a$
$\Rightarrow (b_i - b_j)a = 0$
$\Rightarrow (b_i - b_j)(ab_1) = 0$
$\Rightarrow b_i = b_j$, a contradiction. ∎

(c)$a, b \in R, a, b, ab-1$ units
(1)check: $a - b^{-1}$ is unit
Since $(a - b^{-1} = (ab-1)b^{-1}$
Hence $[b(ab-1)^{-1}](a-b^{-1}) = [b(ab-1)^{-1}][(ab-1)b^{-1}] = bb^{-1} = 1$ and $(a-b^{-1})[b(ab-1)^{-1}] = (ab-1)b^{-1}b(ab-1)^{-1} = 1$
(2)check: $(a-b^{-1})^{-1} - a^{-1}$ is unit
Since $a[(a-b^{-1})^{-1}a - 1]^{-1} = aba - a$
Then $((a-b^{-1})^{-1} - a^{-1})(aba-a) = (a-b^{-1})^{-1}(aba-a) - (ba-1) = (a-b^{-1})^{-1}(a + b^{-1})ba - ba + 1 = 1$
similarly, $(aba-a)[(a-b^{-1})^{-1} - a^{-1}] = 1$ ∎

5.
(a)$\mu(n_1, n_2) = \mu(n_1)\mu(n_2)$ if $(n_1, n_2) = 1$.
Case1. One of n_1, n_2 is 1
W.L.O.G., $\mu(n_1, n_2) = \mu(n_2) = \mu(n_1)\mu(n_2)$
Case2. One of n_1, n_2 has a square factor.
So does $n_1 n_2$. Then $\mu(n_1, n_2) = 0 = \mu(n_1)\mu(n_2)$
Case3. Since $(n_1, n_2) = 1$
We can assume $n_1 = p_1 p_2 ... p_s, n_2 = q_1 q_2 ... q_t$ where p_i, q_i are distinct primes.
Then $\mu(n_1, n_2) = (-1)^{s+t} = (-1)^s(-1)^t = \mu(n_1)\mu(n_2)$ ∎

(b) Case1. If $n = 1$ $\sum_{d|n} \mu(d) = \sum_{d|1} \mu(d) = \mu(1) = 1$
Case2. If $n \neq 1$, let $n = p_1^{s_1} p_2^{s_2} ... p_t^{s_t}$ where p_i are distinct prime and $s_i \geq 1$.
$\sum_{d|n} \mu(d) = \sum_{d|p_1 p_2 ... p_t} \mu(d) = \sum_{i=0}^{t} \binom{t}{i}(-1)^i = (1-1)^t = 0$ ∎

(c)$\sum_{d|n} \mu(\frac{n}{d}) \sum_{d'|n} f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) = f(n)$ ——by (b) ∎

(d)(e)

Theorem 0.1 *Let $GF(q)$ be a finite field and let n be a positive integer. Then the product of all monic irreducible polynomials over $GF(q)$, whose degree divide n is*

$$f_{q^n}(x) = x^q - x$$

Def. $N_q(d) :=$ number of monic irreducible polynomials of degree over $GF(q)$.

Corollary 0.2 *For all positive integers d and n, we have $q^n = \sum_{d|n} dN_q(d)$.*

Corollary 0.3 $N_q(d) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$.

let $g(n) = q^n, f(d) = dN_q(d)$, done! ∎