Homework 17 - MATH 791

Will Thomas

Let R be an integral domain. In what follows, $a, b, c, d, e, f \in R$ will be non-zero, non-unit elements. Given $a, b \in R, d \in R$ is said to be a *greatest common divisor*, or GCD, of a and b if the following conditions hold:

(i) $d \mid a$ and $d \mid b$

(ii) Whenever $e \mid a$ and $e \mid b$, then $e \mid d$

Use this definition to prove the following problems.

Problem 1:
Show that if GCDs exist, they are unique up to a unit multiple.
Solution:
Let us assume that we have two GCD's d_1, d_2 that are GCD's for a and b.
This means

$$\exists q_1, q_1', q_2, q_2',\ a = q_1 * d_1 \wedge a = q_2 * d_2 \wedge b = q_1' * d_1 \wedge b = q_2' * d_2$$

Let us have $ab = q_1 * d_1 * q_2' * d_2$ and $ab = q_1' * d_1 * q_2 * d_2$, we can factor out and set these equal to get $q_1 * q_2' = q_1' * q_2$
We also know by (ii) that $d_1 \mid d_2 \wedge d_2 \mid d_1$. This implies that
$d_1 = u_1 d_2 \wedge d_2 = u_2 d_1 \implies d_1 = u_1 u_2 d_1 \implies 1 = u_1 u_2$
Thus u_1, u_2 are units, which means that $d_1 = u_1 d_2 \implies d_1$ and d_2 only differ by unit multiples.

$\therefore$ GCD's are unique up to a unit multiple

Problem 2:
Suppose d_1 is a GCD of ab and ac, and d_2 is a GCD of b and c. Prove that, d_1 is a unit multiple of ad_2. Use this to show that if d is a GCD of a and b, then 1 is a GCD of a/d and b/d
Solution:
We know that $d_1 \mid ab \wedge d_1 \mid ac \wedge d_2 \mid b \wedge d_2 \mid c$.

$$d_1 = q_1 ab \wedge d_1 = q_2 ac \wedge d_2 = q_3 b \wedge d_2 = q_4 c$$

$$d_2 \mid b \implies d_2 \mid ab \wedge d_2 \mid c \implies d_2 \mid ac$$
$$\implies d_2 \mid d_1$$

So we can find $d_1 = qd_2$, $q_1ab = qq_3b \implies q_1a = qq_3$ also $q_2ac = qq_4c \implies q_2a = qq_4$

$$q_1a + q_2a = qq_3 + qq_4 \implies (q_1 + q_2)a = (q_3 + q_4)q \implies (q_1 + q_2)/(q_3 + q_4)a = q$$

$$d_1 = (q_1 + q_2)/(q_3 + q_4)ad_2$$

We need to now show that $(q_1 + q_2)/(q_3 + q_4)$ is a unit.

Admitted

We can use this to prove that $1 = GCD(a/d, b/c)$
Taking $d_1 \mid a \wedge d_1 \mid b$, and then also $d_2 \mid ad_1' \wedge d_2 \mid bd_1'$, we know then that $d_2 = u_1 * a * d_1$, or also $d_2 = u_2 * b * d_1$. We can use this to reduce to
$u_1 * a * d_1 \mid ad_1' \implies u_1 * d_1 \mid d_1' \wedge u_2 * b * d_1 \mid bd_1'$
Since u_1, u_2 are units,

Admitted

Problem 3:
Show that if 1 is a GCD of a and b is and 1 is also a GCD of a and c, then 1 is a GCD of a and bc.
Solution:
$\gcd(a, b) = 1 \implies 1 \mid a \wedge 1 \mid b$ and $\forall e, e \mid a \wedge e \mid b \implies e \mid d$.
From this, we can conclude that the only possible values e could take are 1 as $\nexists e > 1$ s.t. $e \mid d$
Similarly for $\gcd(a, c) = 1 \implies 1 \mid a \wedge 1 \mid b$ and $\forall e, e \mid a \wedge e \mid b \implies e \mid d$.
This also shows that the only possible values for e are 1.
To find $\gcd(a, bc)$ we need a value d such that $d \mid a \wedge d \mid bc$.

$$d \mid bc \iff d \mid b \vee d \mid c$$

Combining this, we get that we need a value d such that

$$d \mid a \wedge (d \mid b \vee d \mid c) \iff (d \mid a \wedge d \mid b) \vee (d \mid a \wedge d \mid c)$$

We proved earlier that for $(d \mid a \wedge d \mid b)$ the only values d can take are 1, and also $(d \mid a \wedge d \mid c)$ the only values d can take are also 1.

$$\therefore \gcd(a, bc) = 1$$

Problem 4:
Show that if R is a PID, and $a, b \in R$, then d is a GCD of a and b if and only if $\langle a, b \rangle = \langle d \rangle$. In particular, every two non-zero, non-units have a GCD, and if d is a GCD of a and b, then $d = ra + sb$ for some $r, s \in R$

Solution:

$$\langle d \rangle = r_1 d,\ \forall r_i \in R;\ \langle a, b \rangle = r_a a + r_b b,\ \forall r_i \in R$$

Proving $d = \gcd(a, b) \implies \langle a, b \rangle = \langle d \rangle$:
If $d = \gcd(a, b) \implies d \mid a \land d \mid b$; we need to show $\forall r_a, r_b \in R, \exists r_d \in R,\ r_a a + r_b b = r_d d$

$$r_a a + r_b b = r_d d = (r_a(d_a * d)) + (r_b(d_b * d)) = (r_d d)$$

$$= (r_a d_a)d + (r_b d_b)d = (r_a d_a + r_b d_b)d = (r_d)d$$

So if we pick $r_d := (r_a d_a + r_b d_b) \in R$ this holds
Proving $\langle a, b \rangle = \langle d \rangle \implies d = \gcd(a, b)$:
If $\langle a, b \rangle = \langle d \rangle \implies \forall r_a, r_b \in R, \exists r_d \in R, r_a a + r_b b = r_d d$; since

$$d \mid (r_d d) \implies d \mid (r_a a + r_b b) \implies d \mid (r_a a) \land d \mid (r_b b)$$

Since R is a PID, that means that it is also a PID

Admitted

Problem 5:
Let $R = \mathbb{Q}[x, y]$ be the polynomial ring in two variables over $\mathbb{Q}$. Show that 1 is a GCD of x and y, but there is no equation of the form $1 = f \cdot x + g \cdot y$ for $f, g \in R$
Solution:
We know fundamentally that $1 \mid x \land 1 \mid y$ as we can write $x = 1 * x \land y = 1 * x$.
To show it is the *greatest* common divisor, let us assume some divisor $\exists d \in R$, s.t. $d > 1$.

$$\implies d_x \mid x \land d_y \mid y \implies x = d_x * x' \land y = d_y * y' \land d_x = d_y$$

We have two cases for each variable x', y':
Assume that a, b are constants in R and f, f', g, g' are functions comprised solely of their respective variables. We also assume that any $f(x) + g(y)$ sum is not a constant (as it would fall into the constant case instead).

x'	y'	d_x	d_y
Constant a	Constant b	$\frac{x}{a}$	$\frac{y}{b}$
Constant a	$f'(x) + g'(y)$	$\frac{x}{a}$	$\frac{y}{f'(x)+g'(y)}$
$f(x) + g(y)$	Constant b	$\frac{x}{f(x)+g(y)}$	$\frac{y}{a}$
$f(x) + g(y)$	$f'(x) + g'(y)$	$\frac{x}{f(x)+g(y)}$	$\frac{y}{f'(x)+g'(y)}$

It is straightforward to see from this table that we can never reconcile $d_x = d_y$ unless we are in the case where $x' = f(x) + g(y) = x$ and $y' = f'(x) + g'(y) = y$ in which case

$$d_x = \frac{x}{x} = 1 = \frac{y}{y} = d_y$$

Besides this, these are just polynomials so we cannot have d with $f(x) + g(y)$ in the denominator.

$$\therefore \gcd(x, y) = 1$$

Now, to show that no equation can be formed.
Let us presume that $\exists f, g$ s.t. $1 = fx + gy$, however we need either fx, gy or both to have a constant term.
However, neither fx or gy can have a constant term, so $1 = fx + gy$ cannot have a constant term

$$\therefore \nexists f, y \in R,\ s.t\ 1 = fx + gy$$