COMMUTATIVE ALGEBRA HW 1 SOLUTIONS

JC

Due in class Fri 2 September. Uses the ideas in the proof of the theorem "R UFD implies $R[x]$ UFD".

(1) Let R be a PID, let $X \subseteq R$ be a set with at least one nonzero element and (X) the ideal generated by X. Show that $a \in R$ is a gcd for X iff $(a) = (X)$.
Since R is a PID we know $(X) = (b)$ for some b. Now since $b \in (X)$ every common divisor of X divides b, and since $X \subseteq (b)$ every element of X is divisible by b. So b is a gcd for X. gcd's are unique up to associates so a is a gcd iff a is an associate of b iff $(a) = (b)$ iff $(a) = (X)$.

(2) Let R be a UFD, let F be the field of fractions of R. Show that
  (a) If f and g are primitive and irreducible in $R[x]$ and f divides g in $F[x]$, then f and g are associates in $R[x]$.
  Let $f = gH$ for $H \in F[x]$ and let $h \in R[x]$ be a primitive $F[x]$-associate of H. Then fH and fh are primitive $F[x]$-associates so are $R[x]$-associates, so without loss $h = H$ and h must thus be a unit of R.
  (b) If f and g are non-associate irreducibles in $R[x]$ then
    (i) f and g have no common irreducible factor in $F[x]$.
    Suppose that h is a common irreducible factor in $F[x]$. Without loss $h \in R[x]$ and h is primitive, so by the previous result h is an $R[x]$-associate of both f and g. Contradiction!
    (ii) There exist $A, B \in R[x]$ and $c \in R$ such that $Af + Bg = c$, $c \neq 0$.
    Hint: what can you say about the ideal generated by f and g in the PID $F[x]$?
    Taking the hint we just showed that f and g are coprime in $F(x)$. So they have gcd 1 in the PID $F[x]$ and thus they generate (1), in particular $1 = Xf + Yg$ for $X, Y \in F[x]$. Clearing fractions in the coefficients of X and Y we get $AF + Bg = c \neq 0$ as required.

(3) Let k be a field and let $A = k[x, y]$ be the ring of polynomials in two variables x and y with coefficients from k.
  (a) Prove that A is a UFD (Hint: $A \simeq k[x][y]$).
  $k[x]$ is a PID so $k[x]$ is a UFD so $k[x][y]$ is a UFD.
  Cultural note: it is not a PID for example (x, y) is non-principal.
  (b) Let $f, g \in A$ be non-associate irreducible polynomials. Show that there are only finitely many $(c, d) \in k^2$ such that $f(c, d) = g(c, d) = 0$.
  Hint: let $R = k[x]$, let $F = k(x)$ (the field of fractions of R) and appeal to the preceding question.
  By the preceding questiion there are $A, B \in R[y] = k[x][y] = A$ (cheating a bit here by identifying isomorphic polynomial rings) such that $Af + Bg = h$ for some non-zero $h \in R = k[x]$. In particular

$f(c,d) = g(c,d) = 0 \rightarrow h(c) = 0$ so there are only finitely many candidates for c. By symmetry the same is true for d and we are done. Hint: what do you know about the number of roots of a nonzero polynomial in $k[x]$?

Cultural note: we just showed that two "irreducible curves" in the 2D affine space k^2 have a finite intersection. Later on we discuss the question of how big this finite set must be and show that counting in the right way there are $deg(f)deg(g)$ points.