Question 4+: A polynomial has bounded number of roots

Lemma. *Let D be an integral domain and let $f(x) \neq 0 \in D[x]$. If $\alpha \in D$ is a root of f then $x - \alpha \mid f$.*

Proof. We first show that if $\alpha \in D$ is a root of f, then $x - \alpha \mid f$. By the division algorithm in $D[x]$ there exists $q(x), r(x) \in D[x]$ s.t. $\deg r < \deg x - \alpha = 1$ or $r = 0$ and

$$f(x) = (x - \alpha)q(x) + r(x).$$

1 possible because $x - \alpha$ is monic.

This tells us that $r(x)$ is either a constant or 0, so let $r(x) = c \in D$. Now, since α is a root of f we have that

$$f(\alpha) = 0 \cdot q(\alpha) + c = c = 0,$$

which implies that $r = 0$ and $x - \alpha \mid f$. ✓ □

Theorem. *Let D be an integral domain and let $f(x) \neq 0 \in D[x]$ where $\deg f = d$, then f has $\leq d$ roots.*

Proof. We proceed by induction on d. As a base case take $d = 0$ which means that f is a nonzero constant. Therefore, f has 0 roots. ✓

Now consider f a polynomial of degree $d > 0$. Let $\alpha \in D$ be a root of f (if no such α exists then f has less than d roots and we are happy). Then by the above lemma, we have that

$$f(x) = (x - \alpha)g(x) \qquad \text{where} \qquad \deg g = d - 1.$$

So by induction g has at most $d - 1$ roots. Take a root $\beta \in D$ of f that is not a root of g. Then

$$f(\beta) = (\beta - \alpha)g(\beta) = 0 \qquad \text{but} \qquad g(\beta) \neq 0.$$

Therefore, since we're in an integral domain with no zero divisors, we must have that $\beta - \alpha = 0$ which implies that $\beta = \alpha$ and thus f has at most d roots (at most $d - 1$ from g and α). □

5

NICELY DONE.