Mathematics 546 Homework.

In this assignment F always is a field.

Proposition 1 (Remainder Theorem)**.** *Let $f(x) \in F[x]$ be a polynomial of degree ≥ 1 over the field F and let $a \in F$. Then the reminder when $f(x)$ is divided by $x - a$ is $f(a)$. A little more explicitly if*

$$f(x) = q(x)(x - a) + r$$

where $r \in F$, then $r = f(a)$.

Problem 1. Prove this. □

Corollary 2. *If $f(x) \in F[x]$ where F is a field and $a \in F$, then $f(a) = 0$ if and only if $f(x)$ is divisible by $(x - a)$.*

Problem 2. Prove this. □

Theorem 3. *Let $f(x) \in F[x]$ and let $n = \deg(f(x)) \geq 1$. Then $f(x)$ has at most n roots in F. (That is there are at most n elements $a \in F$ such that $f(a) = 0$.)*

Problem 3. Prove this. *Hint:* Use induction of $n = \deg(f(x))$.

(a) *Base case.* This is $n = 1$. If $\deg(f(x)) = 1$, then $f(x) = a_1x + a_0$ with $a_1 \neq 0$. Show that in this case $f(x)$ has exactly one roots and give a formula for it.

(b) *Induction step.* The induction hypothesis is that any polynomial of degree n has at most n roots. Let $\deg(f(x)) = n + 1$ and we wish to show it has at most $n+1$ roots. If it has no roots are are done. So assume $f(x)$ has at least one root a_1. Then explain why $f(x) = (x - a_1)f_1(x)$ where $\deg(f_1(x)) = n$ and use this and the induction hypothesis to finish the proof. □

Problem 4. Prove this. □

Definition 4. Let $f(x)$ and $g(x)$ be polynomials in $F[x]$ not both zero. Then $d(x) \in F[x]$ is a ***greatest common divisor*** of $f(x)$ and $g(x)$ if and only if

(a) $d(x) \mid f(x)$ and $d(x) \mid g(x)$ (that is it divides both $f(x)$ and $g(x)$), and

(b) If $c(x) \mid f(x)$ and $c(x) \mid g(x)$, then $c(x) \mid d(x)$. (That is $d(x)$ is divides any polynomial that divides both $f(x)$ and $g(x)$.) □

Theorem 5 (Bézout's Theorem for polynimials)**.** *Let $f(x)$ and $g(x)$ be elements of $F[x]$ not both zero. Then $f(x)$ and $g(x)$ have a greatest common divisor, $d(x)$, it is unique up to multiplication by a constant, and $d(x)$ is a linear combination of $f(x)$ and $g(x)$. That is there are $p(x), q(x) \in F[x]$ such that*

$$p(x)f(x) + q(x)g(x) = d(x).$$

Outline of the proof. Let

$$I = \{A(x)f(x) + B(x)g(x) : A(x), B(x) \in F[x]\}$$

be the set of all linear combinations of $f(x)$ and $g(x)$. Then it is not hard to show that I is an ideal in $F[x]$. We know that all ideals in $F[x]$ are principle, that is there is a polynomial $d(x)$ such that

$$I = \langle d(x) \rangle = \{h(x)d(x) : h(x) \in F[x]\} = \text{ set of all multiples of } d(x).$$

Then, as $f(x), g(x) \in I$ we have that $d(x) \mid f(x)$ and $d(x) \mid g(x)$. And as $d(x) \in I$ it is a linear combination of $f(x)$, and $g(x)$, that is

$$d(x) = p(x)f(x) + q(x)g(x)$$

for some polynomials $p(x)$ and $q(x)$. From this we see that if $c(x)$ divides both $f(x)$ and $g(x)$ then we can factor $c(x)$ out of $p(x)f(x)+q(x)g(x) = d(x)$ which shows that $c(x) \mid d(x)$. □

Definition 6. A polygonal $p(x) \in F[x]$ is ***irreducible*** if and only if $\deg(p(x)) \geq 1$ and if $p(x) = f(x)g(x)$ then at least one of $f(x)$ or $g(x)$ is a constant. (That is $f(x) = c \in F$ or $g(x) = c \in F$ for some $c \in F$.) □

Definition 7. If $f(x), g(x) \in F[x]$, then $f(x)$ and $g(x)$ are ***relatively prime*** if and only if 1 is a greatest common divisor of $f(x)$ and $g(x)$. We write this as $\gcd(f(x), g(x)) = 1$. □

Theorem 8. *If $f(x), g(x) \in F[x]$ are relatively prime and $f(x) \mid g(x)h(x)$ for some $h(x) \in F[x]$, then $f(x) \mid h(x)$.*

Problem 5. Prove this. *Hint:* The proof looks almost exactly like the analogous fact for the integers. Start noting that by the definition of $f(x) \mid g(x)h(x)$ there is a polynomial $k(x)$ with

$$g(x)h(x) = k(x)f(x).$$

By Bézout's Theorem there are $p(x), q(x) \in F[x]$ with

$$1 = p(x)f(x) + q(x)g(x).$$

Multiple this by $h(x)$ and use $g(x)h(x) = k(x)f(x)$ to rewrite things so that it is possible to factor $f(x)$ out of the resulting formula for $h(x)$. □

Proposition 9. *If $p(x)$ is irreducible and $p(x)$ does not divide $f(x)$, then* $\gcd(p(x), f(x)) = 1$.

Problem 6. Prove this. □

Theorem 10. *If $p(x) \in F[x]$ is irreducible and $p(x) \mid f(x)g(x)$, then $p(x) \mid f(x)$ or $p(x) \mid g(x)$. (That is if an irreducible polynomial divides a product, then it divides one of the factors.)*

Problem 7. Prove this. *Hint:* If your are having trouble with this go back and see what we did in the case of integers. □

We can now prove the analogue of the Fundamental Theorem of Arithmetic (which is that a positive integer $n \geq 2$ has a unique factorization into primes).

Theorem 11 (Unique factorization in polynimial rings)**.** *Let $f(x) \in F[x]$ with $\deg(f(x)) \geq 1$. Then $f(x)$ factors into irreducible polynimials*

$$f(x) = p_1(x)p_2(x)\cdots p_k(x)$$

and this factorization is unique up to the reordering the factors and multiplying them by constants.

Proof. The proof is almost exactly the same as the one we gave for factoring integers into primes. So we are going to skip it. □

If a polynomial $f(x)$ with $\deg(f(x)) \geq 1$ is not irreducible, then it is ***reducible***. That if $f(x)$ is reducible if and only if $f(x) = g(x)h(x)$ where $\deg(g(x)) \geq 1$ and $\deg(h(x)) \geq 1$.

Proposition 12. *If $f(x) \in F[x]$ has $\deg(f(x)) \geq 2$ and $f(x)$ has a root in F (that is $f(a) = 0$ for some $a \in F$), then $f(x)$ is reducible.*

Problem 8. Prove this. *Hint:* Use $f(a) = 0$ to show $f(x)$ has factor of degree 1. □

Problem 9. Show that if $f(x) \in F[x]$ has $\deg(f(x)) = 2$ or $\deg(f(x)) = 3$ then it is reducible if and only if if has a root in F. *Hint:* One direction follow from Proposition 12. In the other direction assume that $\deg(f(x)) = 2$ or $\deg(f(x)) = 3$ and that $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ where $\deg((x)) + \deg(h(x)) = \deg(x)$ and so $\deg(g(x)) + \deg(f(x)) = 2$ or $\deg(g(x)) + \deg(f(x)) = 3$. Use this to show that at least one of $g(x)$ or $h(x)$ has degree $= 1$. And a degree on polynomial always has a root (why?).