MAT401H1S Homework 5

16.22 To show that Z[x] is not a principal ideal domain.

To construct an ideal in Z[x] that is not generated by a single element. (There are many.)

Let $A=\{a(x)(x^2+c)+b(x)(x^3) \mid a(x),b(x) \in Z[x]\}$ for some $c>0$.

Clearly $A \neq 0$ (eg. $x^2+c \in A$)

To show that this is in fact an ideal is trivial (show that ra and ar are in A for all r(x) in Z[x] and a(x) in A). Note that Z[x] is commutative and therefore it needs only be shown on one side.

Therefore A is an ideal by definition.

Assume A=<g(x)> for some g(x) in Z[x].

Then $\exists$ f(x) e Z[x] such that:

$f(x)g(x) = x^2+c$

and there exists $h(x) \in Z[x]$ such that:

$h(x)g(x)=x^3$

x^2+c is irreducible over Z[x]

Therefore $g(x)=1$ or $g(x)=x^2+c$.

x^3 is only reducible to $1x^3$ or xx^2.

Therefore $g(x)=1$.

Therefore A=<1>.

Therefore A=Z[x].

Therefore $x \in A$.

But then there exist a(x),b(x) in Z[x] such that $a(x)(x^2+c)+b(x)(x^3)=x$.

Therefore:

$(a_0+a_1x+\ldots+a_nx^n)(x^2+c)+(b_0+b_1x+\ldots+b_mx^m)(x^3)=x$

The only term in x on the left side is a_1cx and therefore $a_1c=1$, $a_1=1/c$.

But if we take $c\neq1$, then $a_1 \notin Z$ and $a(x) \notin Z[x]$.

Therefore $A\neq Z[x]$ and A is not generated by a single element.

Therefore there are ideals in Z[x] that are not generated by a single element.

Therefore Z[x] is not a principal ideal domain.

16.27 Let F be a field, $I \subseteq F[x]$, $I=\{a_0+a_1x+\ldots+a_nx^n \mid (i=0\rightarrow n)\Sigma a_i=0,\ a_i \in F\}$

I is nonempty: $f(x)=0 \in I$ (Trivial.)

If $a(x), b(x) \in I$:

$a(x)-b(x)= (i=0\rightarrow m)\Sigma(a_i-b_i)x^i + (i=m+1\rightarrow n)\Sigma a_ix^i$

Note: Without loss the assumption that deg b=m<n=deg a.

$a(x)-b(x)=(i=0\rightarrow n)\Sigma c_ix^i$

Therefore $\Sigma c_i=(i=0\rightarrow m)\Sigma(a_i-b_i)+(i=m+1\rightarrow n)\Sigma(a_i)=(i=0\rightarrow n)\Sigma a_i - (i=0\rightarrow m)\Sigma b_i = 0-0=0$ and a(x)-b(x) is in I.

Since F is a field, p(x)q(x)=q(x)p(x) for all p, q in F[x]. (Therefore need only check one side)

To check that for all $p(x) \in F[x]$, $a(x) \in I$, $p(x)a(x) \in I$:

Let $p(x)=cx^m$ for some c e F, $m >0 \in Z$.

Then $p(x)a(x)=cx^m(\Sigma a_ix^i)=\Sigma ca_ix^{i+m}=(i=m\rightarrow m+n)\Sigma ca_{i-m}x^i$

Then let $d_i=0$ for all $i \in \{0,1,\ldots,m-1\}$ and let $d_i=ca_{i-m}$ for all $i \in \{m, m+1,\ldots, m+n\}$

Then $p(x)a(x)=(i=0\rightarrow m+n)\Sigma d_ix^i$

And therefore $\Sigma d_i=(i=0\rightarrow m-1)\Sigma d_i + (i=m\rightarrow m+n)\Sigma d_i=(i=0\rightarrow m-1)\Sigma(0)+(i=0\rightarrow n)\Sigma ca_i$

$= c(i=0 \rightarrow n)\Sigma a_i = c(0) = 0$ and $p(x)a(x) \in I$.

Now let $q(x)$ be arbitrary in $F[x]$ and let $a(x) \in I$ as before.
Then $q(x)a(x)=(q_0+q_1x+\ldots+q_mx^m)a(x)=q_0a(x)+q_1xa(x)+\ldots+q_mx^ma(x)$
From above, if $a(x)$ is in I, then $cx^ka(x)$ is in I.
Therefore $q_ix^ia(x) \in I$.
Since I is closed under subtraction, it is also closed under addition.
Therefore $q(x)a(x)$ is in I.
By the Ideal Test (14.1), I is an ideal in $F[x]$.

A generator for I is (x-1)
To show:

x-1 e I, (1-1=0)

If $g(x)$ is a generator for I, $x-1=g(x)h(x)$ for some $h(x)$ e $F[x]$. But deg $(x-1)=1$ and therefore $g(x)$ has degree one or zero. If $g(x)$ has degree one, then $h(x)$ is a unit (clearly nonzero) and $g(x)$ can be generated by x-1 (i.e. $<x-1>=<g(x)>$). If deg $g(x)=0$, then $g(x)=g_0$. But $g(x)$ is in I and therefore $g_0=0$. Impossible.
Therefore $g(x)$ has degree one and $<g(x)>=<x-1>$ and x-1 generates I.

16.31 To show that $x^{p-1}-1=(x-1)(x-2)\ldots(x-(p-1))$ in $Z_p[x]$ for all primes p.
Fermat's Little Theorem:
Let p be a prime and let $a \in N$, $0<a<p$.
Let $Ap=\{1a,2a,\ldots,(p-1)a\}$
No two elements in Ap are congruent modulo p:

If they were: $ra \equiv sa \pmod p$

$ra-sa\equiv 0 \pmod p$

$(r-s)a\equiv 0 \pmod p$

$p|a$ or $p|r-s$ (p prime by Euclid's Lemma)

But $0<a<p$ and so $p|r-s$, but $0<r,s<p$ and therefore $-p<r-s<p$

Therefore $r-s=0$ and $r=s$ no two elements are congruent modulo p.

Therefore the elements of Ap are distinct modulo p.
Therefore $Ap=\{1,2,\ldots,p-1\}$ modulo p
Therefore $(1a)(2a)\ldots((p-1)a) \equiv (1)(2)\ldots(p-1) \pmod p$

$(a^{p-1})(p-1)! \equiv (p-1)! \pmod p$

$(a^{p-1}-1)(p-1)! \equiv 0 \pmod p$

Clearly p does not divide $(p-1)!$ and so $p|(a^{p-1}-1)$

Therefore $a^{p-1}-1 \equiv 0 \pmod p$ for all a such that $\gcd(a,p)=1$.

By the Factor Theorem (16.2 Cor 2) a is a zero of $f(x) \in F[x]$ if and only if x-a is a factor and by the Remainder Theorem (16.2 Cor 1) $f(a)$ is the remainder in the division of $f(x)$ by x-a.

Therefore let $f(x)=x^{p-1}-1 \in Z_p[x]$
For all $a \in \{1,2,\ldots,p-1\}$, $f(a) = 0$ (By Fermat's Little Theorem)
For all a as above, $(x-a)$ divides $f(x)$

Therefore $f(x)=x^{p-1}-1=(x-1)(x-2)\ldots(x-(p-1))$
Note that f has at most (p-1) zeroes so there are no more.

16.39 Let F be a field, $f(x), g(x) \in F[x]$ and let f(x) and g(x) be relatively prime.
Then apply the division algorithm (without loss assume that deg f(x) ≥ deg g(x)).

$f(x) = q_0(x)g(x)+r_0(x)$ and by 16.2, $\deg r_0(x) < \deg g(x)$

Note: $r_0(x) \neq 0$ because then $g(x)|f(x)$ and they are not relatively prime.
Reapplying the algorithm:

$g(x)=q_1(x)r_0(x)+r_1(x)$ and $\deg r_1(x)<\deg r_0(x)$

Note: Similarly, $r_1(x)\neq 0$.
Repeatedly applying the algorithm yields:

$r_i(x)=q_{i+2}(x)r_{i+1}(x) +r_{i+2}$ with $\deg r_{i+2}(x)<\deg r_{i+1}(x)$

Therefore:

Deg $r_0(x)>\deg r_1(x)>\ldots>\deg r_n(x) \geq 0$.

Notice that $r_i(x) \neq 0$ for any i because then we could show that f(x) and g(x) are not relatively prime. I.e. Assume that $r_2(x)=0$:

Then $r_0(x)=q_2(x)r_1(x)+0$

Therefore $r_1(x)|r_0(x)$; but also we know that $g(x)=q_1(x)r_0(x)+r_1(x)$ and therefore r1(x)|g(x) and so on to show that it also divides f(x).

Therefore the degrees of the $r_i(x)$'s is always decreasing and $r_i(x)$ is never zero.
Therefore there exists $n \in N$ such that $\deg r_n(x)=0$.
Therefore let $r_n(x)=r_n$, $r_n \in F$.
From the algorithm we will have $r_{n-2}(x)=q_n(x)r_{n-1}(x)+r_n(x)$
Rearranging yields: $r_n(x)=r_{n-2}(x)=q_n(x)r_{n-1}(x)$ and substituting from the previous line for $r_{n-1}(x)$ and then repeating this procedure will eventually yield:

$r_n(x)=f(x)h(x)+g(x)k(x)$

Since F is a field, $r_n\neq 0$, r_n is a unit.
Therefore $r_nr_n^{-1}=f(x)h(x)r_n^{-1}+g(x)k(x)r_n^{-1}$
Therefore $1=f(x)h'(x)+g(x)k'(x)$
Note: This is the Euclidean Algorithm for integers.)

16.41 Let $f(x) \in \mathbf{R}[x]$ and let $f(a)=f'(a)=0$.
Then $f(x)=f_0+f_1x+\ldots+f_nx^n$
f(a)=0 implies: (x-a) is a factor of f(x) (By the Factor Theorem 16.2 Cor 2)
Therefore $f(x)=(x-a)g(x)$ for some $g(x) \in \mathbf{R}[x]$, $\deg g(x)+1=\deg f(x)$.
Note: The above line can be found from an analysis of leading terms.
From above:
$f(x)=xg(x)-ag(x)$
$f'(x)=g(x)+xg'(x)-ag'(x)=g(x)+(x-a)g'(x)$
Therefore: $f'(a)=g(a)+(a-a)g'(a)=g(a)=0$
Therefore $g(x)=(x-a)h(x)$ for some $h(x) \in \mathbf{R}[x]$.
Therefore $f(x)=(x-a)g(x)=(x-a)(x-a)h(x)=(x-a)^2h(x)$.
Therefore $(x-a)^2$ divides f(x).

17.4 Let $f(x)=x^k+a_{k-1}x^{k-1}+\ldots+a_1x+a_0 \in Z[x]$.

Assume that r $\in$ **Q** such that x-r is a factor of f(x). In particular, r $\in$ **R** and f(x) $\in$ **R**[x] and therefore by the factor and remainder theorems (16.2 Cor 1,2) if x-r is a factor of f(x) then r is a zero and f(r)=0.

Therefore let r=m/n; m,n $\in$ Z, gcd(m,n)=1, n≠0

$f(r)=0 \rightarrow r^k+a_{k-1}r^{k-1}+\ldots+a_1r+a_0=0$

$(m/n)^k+a_{k-1}(m/n)^{k-1}+\ldots+a_1(m/n)+a_0=0$

Multiply by nk:

$m^k+a_{k-1}m^{k-1}n+\ldots+a_1mn^{k-1}+a_0n^k=0$

$-m^k=a_{k-1}m^{k-1}n+\ldots+a_1mn^{k-1}+a_0n^k$

Since n divides every term on the right hand side, n must divide the left hand side by the Fundamental Theorem of Arithmetic,

Therefore $n|m^k$. But gcd(m,n)=1 and therefore n=1

Therefore r=m $\in$ Z.

Therefore if x-r is a factor and r $\in$ **Q**, then r $\in$ Z.