Solutions to assignment 4 - MAS42

Chapter 14:

6a) I'll jump straight to part d). There are several ways to do this, here's one way. Another, shorter way on page 2
(I abuse notation & write $a \in \mathbb{Z}/n\mathbb{Z}$ but still consider a to be an integer $0 \le a < n$)

Claim: If $d = \gcd(a,n)$, then $(\mathbb{Z}/n\mathbb{Z})/(a) \cong \mathbb{Z}/d\mathbb{Z}$

proof: If $d=1$, then a is a unit in $\mathbb{Z}/n\mathbb{Z}$ so $aa^{-1}=1 \in (a)$ so $(a) = \mathbb{Z}/n\mathbb{Z}$ & $(\mathbb{Z}/n\mathbb{Z})/(a) = \{0\} = \mathbb{Z}/\mathbb{Z}$

suppose $d>1$. Since $d=\gcd(a,n)$ $\exists t,s,b,m$ s.t. $ab+nm=d$
$dt=a$ & $ds=n$

define $\varphi: \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$ by taking $\alpha \in \mathbb{Z}/n\mathbb{Z}$, using the division algorithm
$\exists! q, r$, $r<d$ or $r=0$ s.t. $\alpha = qd+r$. define $\varphi(\alpha)=r$

φ is well-defined: if $\beta = \alpha$ in $\mathbb{Z}/n\mathbb{Z}$ then $\exists k$ s.t. $\beta = \alpha + kn$

so $\beta = qd+r+kn = qd+r+kds = (q+ks)d+r$ ($q+ks$) & r unique

so $\varphi(\beta) = r = \varphi(\alpha)$

φ is a homom: exercise

φ is surjective: note that $d \le n$ so $\gamma \in \mathbb{Z}/d\mathbb{Z}$ w/ $0 \le \gamma < d$. Then
$\varphi(\gamma) = \gamma$

$\ker\varphi$: $a = td$ so $\varphi(a) = 0$ so $(a) \subseteq \ker\varphi$

let $\alpha \in \ker\varphi$, then $\alpha = qd+0$. $d = ab+nm$

so $\alpha = qba + qmn \equiv qba \bmod n$

so $\alpha \in (a)$ so $\ker\varphi \subseteq (a)$ QED

Furthermore every ideal $I \subseteq \mathbb{Z}/n\mathbb{Z}$ is principal: indeed, $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group under addition, so any subgroup is cyclic, so I is a cyclic subgroup under addition, say $I = \langle a \rangle$. Then $I = (a)$.

so $I=(a) \subseteq \mathbb{Z}/n\mathbb{Z}$ is max'l iff $(\mathbb{Z}/n\mathbb{Z})/I$ is a field iff $\gcd(a,n) =$ prime

write $n = p_1^{m_1} p_2^{m_2} \cdots p_\ell^{m_\ell}$ the unique factorization of n into primes p_i;

Suppose $a = a_1 a_2$ where $a_1 | n$ & $\gcd(a_2, n) = 1$. Then $(a) = (a_1)$ (indeed, clearly $(a) \subseteq (a_1)$. also, $a_1 = a a_2^{-1}$ so $(a_1) \subseteq (a)$) a_2^{-1} exists in $\mathbb{Z}/n\mathbb{Z}$

so can assume $a | n$. Then $\gcd(a,n) =$ prime iff $a = p_i$ for some i

so $I \subseteq \mathbb{Z}/n\mathbb{Z}$ is max'l iff $I = (p)$ for some prime $p | n$.

6) Alternative solution: · show every $I \trianglelefteq \mathbb{Z}/n\mathbb{Z}$ is principal as above.
· show can assume $a|n$ as above
· show $a = p_i$ for some i as above.

62) R is the set of all infinite sequences of integers. Addition & multiplication is componentwise.
Suppose $I = (\underline{a})$ for some $\underline{a} \in I$. $\underline{a} = (a_1, a_2, a_3, \ldots)$ & $\exists N$ s.t. $\forall i \geq N$ $a_i = 0$.
let $\underline{b} \in I$ be the sequence $b_1 = 1, b_2 = 1, \ldots, b_N = 1, b_i = 0 \ \forall i > N$
Then $\underline{b} \notin (\underline{a})$: indeed, given $\underline{r} = (r_1, r_2, \ldots) \in R$, $\underline{r}\,\underline{a} = (r_1 a_1, r_2 a_2, \ldots)$
so $r_i a_i = 0 \ \forall i \geq N$. but $b_N \neq 0$ QED

(Aside: in fact, I is not "finitely generated", i.e. $I \neq (\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n)$ for any finite number of elements $\underline{a}_i \in I$ (where $(\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n)$ is the ideal generated by $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n$)))

Chapter 16:

2) not $0^3 = 0$, $1^3 = 1$ & $2^3 = 2$ in $\mathbb{Z}/3\mathbb{Z}$
so $\alpha^3 = \alpha \ \forall \alpha \in \mathbb{Z}/3\mathbb{Z}$ so $\alpha^4 = \alpha^2 \ \forall \alpha \in \mathbb{Z}/3\mathbb{Z}$
so $\alpha^4 + \alpha = \alpha^2 + \alpha \ \forall \alpha \in \mathbb{Z}/3\mathbb{Z}$

4) $\operatorname{char} R$ = least $n \in \mathbb{Z}_{>0}$ s.t. $nr = 0 \ \forall r \in R$ ($= 0$ if no such n)
$\operatorname{char} R = 0$: suppose $\exists n \in \mathbb{Z}_{>0}$ s.t. $\forall f(x) \in R[x]$, $n f(x) = 0$
Then, in particular, $nr = 0 \ \forall r \in R$ (r the constant polynomial)
contradiction, hence $\operatorname{char} R[x] = 0$
$\operatorname{char} R = n > 0$: let $m = \operatorname{char} R[x]$:
Then $m \geq n$: let r be constant polynomial, Then $mr = 0 \ \forall r \in R$ so $m \geq n$
$n \geq m$: let $f(x) = \sum_{i=0}^{k} r_i x^i \in R[x]$, Then $n f(x) = \sum_{i=0}^{k} n r_i x^i = 0$ so $n \geq m$
QED

12)
$$\begin{array}{r} 4x^2+3x+6 \\ 3x^2+2x+1 \overline{)\,5x^4+3x^3+1} \\ -(5x^4+x^3+4x^2) \\ \hline 2x^3+3x^2+1 \\ -(2x^3+6x^2+3x) \\ \hline 4x^2+4x+1 \\ -(4x^2+5x+6) \\ \hline 6x+2 \end{array}$$

so $\boxed{q(x) = 4x^2+3x+6}$ & $\boxed{r(x) = 6x+2}$

A much nicer, slicker proof is on page (5)

40) Suppose $f(x)=\sum_{i=0}^{n} a_i x^i$ & $g(x)=\sum_{j=0}^{m} b_j x^j \in R[x]$ s.t. $f(x)g(x)\in I[x]$ with $a_n\neq 0$, $b_m\neq 0$, $h(x)=\sum c_k x^k$

$c_{n+m}=a_n b_m \in I$ so one of a_n or $b_m \in I$. wlog $a_n \in I$ & b_m isn't

$I \ni c_{n+m-1}=a_n b_{m-1}+a_{n-1}b_m$ & $a_n \in I$ so $a_n b_{m-1} \in I$ so $c_{n+m-1}-a_n b_{m-1} \in I$

$\parallel$

$a_{n-1}b_m \Rightarrow a_{n-1}\in I$ (since)

$\vdots$

If $m \geq n$: $I \ni c_{n+m-n}=\sum_{i+j=m} a_i b_j = \sum_{i\geq 1} a_i b_{m-i} + a_0 b_m$ & know that $a_i \in I$ for $i \geq 1$

so $c_{n+m-n}-\sum_{i\geq 1} a_i b_{m-i} \in I$

$\parallel$

$a_0 b_m \Rightarrow a_0 \in I$ (since)

so $f(x)\in I[x]$

If $m<n$:

$I \ni c_{m+n-m}=c_n=\sum_{i+j=n} a_i b_j = \sum_{i\geq n-m+1} a_i b_{n-i} + a_{n-m}b_m$ & know $a_i \in I$ for $i \geq n-m+1$

so $c_n-\sum_{i\geq n-m+1} a_i b_{n-i} \in I$

$\parallel$

$a_{n-m}b_m \Rightarrow a_{n-m}\in I$ (since)

$\vdots$

$I \in c_m=\sum_{i+j=n} a_i b_j = \sum_{i\geq 1} a_i b_{m-i} + a_0 b_m$ & know $a_i \in I$ for $i \geq 1$

so $c_m-\sum_{i\geq 1} a_i b_{m-i} \in I$

$\parallel$

$a_0 b_m \Rightarrow a_0 \in I$ (since)

so $f(x)\in I[x]$ QED

42) Use 1st isom thm (like we did in class to show $\mathbb{R}[x]/(x^2+1) \xrightarrow{\sim} \mathbb{C}$)

Define: $\varphi: \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\sqrt{2}]$

$f(x) \longmapsto f(\sqrt{2})$

φ is a homom: exercise

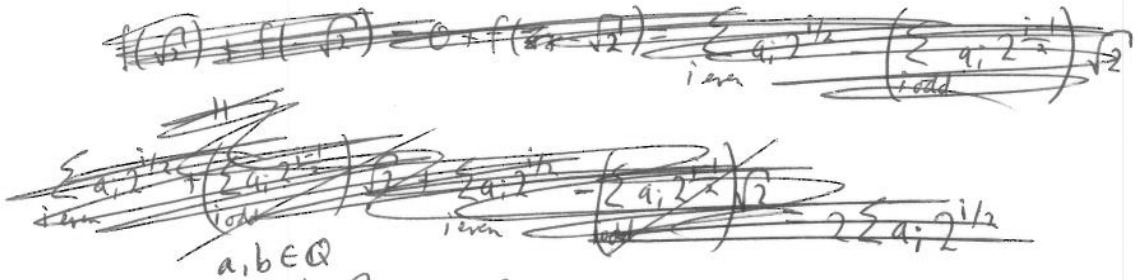
φ is surjective: let $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, then $a+b\sqrt{2}=\varphi(a+bx)$

$(x^2-2)\subseteq \ker\varphi$: If $f(x)=(x^2-2)g(x)$, then $\varphi(f(x))=(\sqrt{2}^2-2)g(\sqrt{2})=(2-2)g(\sqrt{2})=0$

$\ker\varphi \subseteq (x^2-2)$: If $\varphi(f(x))=0$ then $f(\sqrt{2})=0$ so $\sqrt{2}$ is a root of $f(x)$, want to show $-\sqrt{2}$ is also a root (b/c then $(x-\sqrt{2})(x+\sqrt{2})=(x^2-2)\mid f(x)$)

Let $f(x)=\sum_{i=0}^{n} a_i x^i \in$ $f(-\sqrt{2})=\sum_{i\text{ even}} a_i 2^{i/2} - \left(\sum_{i\text{ odd}} a_i 2^{\frac{i-1}{2}}\right)\sqrt{2}$

4.2)(cont'd) & $f(\sqrt{2}) = \sum_{i \text{ even}} a_i 2^{i/2} + \left(\sum_{i \text{ odd}} a_i 2^{\frac{i-1}{2}}\right)\sqrt{2} = 0$



$a, b \in \mathbb{Q}$

Remark: $a + b\sqrt{2} = 0$ iff $a = 0$ & $b = 0$

proof: $a + b\sqrt{2} = 0 \Leftrightarrow \sqrt{2} = \frac{-a}{b} \Leftrightarrow \sqrt{2}$ is rational contradiction QED

so $f(\sqrt{2}) = 0 \Rightarrow \sum_{i \text{ even}} a_i 2^{i/2} = 0$ & $\left(\sum_{i \text{ odd}} a_i 2^{\frac{i-1}{2}}\right) = 0$

$\Rightarrow f(-\sqrt{2}) = 0$ QED

Remark: Given what we did in class on Wednesday there's now a much nicer, simpler proof of $\ker\varphi \subseteq (x^2-2)$ as follows:

~~$\mathbb{Q}$~~ $\mathbb{Q}[x]$ is a PID & $\ker\varphi = (g(x))$ where $g(x) \in \ker\varphi$ is of minimal degree.

Claim: $x^2 - 2$ is of minimal degree in $\ker\varphi$.

proof: if not $\exists f(x) = ax + b$ s.t. $a\sqrt{2} + b = 0$, then $\sqrt{2} = \frac{-b}{a} \in \mathbb{Q}$ contrad QED.

Problems:

(1) Several ways. Here's one: define $\varphi: \mathbb{Z} \oplus \mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z}$ & use 1st Isom Thm

$(a,b) \longmapsto a \bmod 5$

φ is a homom: exercise

$\ker\varphi$: $\varphi(a,b) = 0$ iff $a \equiv 0 \bmod 5$ iff $a = 5x$ for some $x \in \mathbb{Z}$ iff $(a,b) \in I$ QED

(2) Remember that in $\mathbb{Z}$, $(m) \cap (n) = (\text{lcm}(m,n))$ so e.g. $(2) \cap (3) = (6)$

(3) Let $I \trianglelefteq R$ prime $\Rightarrow R/I$ is an int domain. show it's a field. Let $a + I \neq 0 + I$ in R/I. since $a^n = a$ in R, $(a+I)^n = a + I$ in R/I. Use cancellation law in R/I. Then $(a+I)^{n-1} = 1 + I$

so $(a+I)^{-1} = (a+I)^{n-2} \in R/I$ QED

Chapter 16: #40: Alternative solution:

define $\varphi : R[x] \longrightarrow (R/I)[x]$

$f(x) = \sum_{i=0}^{n} r_i x^i \longmapsto \sum_{i=0}^{n} \overline{r_i} x^i$ (where for $r \in R$, we denote the coset $r+I \in R/I$ by $\overline{r}$)

φ is a homom: exercise

φ is surjective: given $\overline{f} = \sum_{i=0}^{n} \overline{r_i} x^i \in (R/I)[x]$, $\overline{f} = \varphi\left(\sum_{i=0}^{n} r_i x^i\right)$

$\ker\varphi \supseteq I[x]$: let $f(x) \in I[x]$, then $r_i \in I \ \forall i$ so $\overline{r_i} = 0 \ \forall i$

$I[x] \subseteq \ker\varphi$: If $\varphi(f(x)) = 0$, then $\overline{r_i} = 0 \ \forall i$ so $r_i \in I \ \forall i$

so $f(x) \in I[x]$.

By 1st isom Thm, $R[x]/I[x] \cong (R/I)[x]$

R/I is a domain so $(R/I)[x]$ is a domain so $I[x] \trianglelefteq R[x]$ is prime

QED