Solutions to assignment 3 – MA542

Chapter 13:

58) $F^\times = \{x \in F : x \neq 0\}$ is a group under multiplication. It has $n-1$ elements, hence

$x^{n-1} = 1 \quad \forall x \in F^\times$ (since if G is a finite group & $g \in G$, then $g^{|G|} = 1$) ☐

Chapter 15:

46) F field, R a ring w/ at least two elements, $\varphi : F \to R$ a surjective homom.

Claim: $\ker \varphi \neq F$

proof: let $r \in R$, $r \neq 0$ (exist since R has at least two elements)

Then, since φ is surjective, $\exists\, x \in F$ s.t. $\varphi(x) = r$. Then $x \notin \ker \varphi$ ②

But $(0) \trianglelefteq F$ are the only two ideals $\trianglelefteq F$, so $\ker \varphi = (0)$ i.e. φ is injective.

Since φ is surjective, it is an isom. ☐

49) a) $\pi_1 : R \oplus S \to R$, $(a,b) \mapsto a$

- $\pi_1((a,b)+(c,d)) = \pi_1((a+c, b+d)) = a+c = \pi_1(a,b) + \pi_1(c,d)$
- $\pi_1((a,b)(c,d)) = \pi_1(ac, bd) = ac = \pi_1(a,b)\,\pi_1(c,d)$

b) $\iota_1 : R \to R \oplus S$, $a \mapsto (a,0)$

- $\iota_1(a+b) = (a+b, 0) = (a,0) + (b,0) = \iota_1(a) + \iota_1(b)$
- $\iota_1(ab) = (ab, 0) = (a,0)(b,0) = \iota_1(a)\,\iota_1(b)$
- $\iota_1(a) = (0,0)$ iff $(a,0) = (0,0)$ iff $a = 0$

  so $\ker \iota_1 = (0)$ so ι_1 is one-to-one.

c) $\varphi : R \oplus S \to S \oplus R$, $(r,s) \mapsto (s,r)$

- φ is a homom:
  - $\varphi((r_1,s_1)+(r_2,s_2)) = \varphi(r_1+r_2, s_1+s_2) = (s_1+s_2, r_1+r_2) = (s_1,r_1) + (s_2,r_2) = \varphi(r_1,s_1) + \varphi(r_2,s_2)$
  - $\varphi((r_1,s_1)(r_2,s_2)) = \varphi(r_1r_2, s_1s_2) = (s_1s_2, r_1r_2) = (s_1,r_1)(s_2,r_2) = \varphi(r_1,s_1)\,\varphi(r_2,s_2)$
- φ is surjective: given $(s,r) \in S \oplus R$, $\varphi(r,s) = (s,r)$
- φ is injective: If $\varphi(r,s) = (0,0)$ then $(s,r) = (0,0)$ so $s=0, r=0$

  so $(r,s) = (0,0)$ so $\ker \varphi = (0)$

☐

Questions:

(1)(a) $a, b \in \varphi(I) = \{y \in S : \exists\, x \in I \text{ with } \varphi(x) = y\}$ & $s \in S$. Then $\exists\, x, y \in I$ s.t. $\varphi(x) = a$, $\varphi(y) = b$

- $a-b$: $\varphi(x-y) = \varphi(x) - \varphi(y) = a-b$ & $x-y \in I$ so $a-b \in \varphi(I)$

(1)(a) cont'd: • sa: since φ is surjective $\exists\, r\in R$ s.t. $\varphi(r)=s$.
Then $\varphi(rx)=\varphi(r)\varphi(x)=sa$ & $rx\in I$ so $sa\in\varphi(I)$
similarly for as.
Hence, $\varphi(I)$ is an ideal in S. ∎

(b) let $\varphi: \mathbb{Z}\to\mathbb{Z}\oplus\mathbb{Z}$, $a\mapsto(a,a)$ — φ is a homom: • $\varphi(a+b)=(a+b,a+b)=(a,a)+(b,b)$
$=\varphi(a)+\varphi(b)$
• $\varphi(ab)=(ab,ab)=(a,a)(b,b)=\varphi(a)\varphi(b)$

Can take $I=\mathbb{Z}$, Then $\varphi(I)=\{(a,a)\in\mathbb{Z}\oplus\mathbb{Z} : a\in\mathbb{Z}\}$
Then $(2\cdot 3)(1,1)=(2,3)\notin\varphi(I)$ so $\varphi(I)$ is not an ideal.

(2) Define $f: I\to(I+J)/J$, $a\mapsto a+J$

Claim: f is surjective
proof: let $x\in(I+J)/J$. Then $\exists\, a\in I,\ b\in J$ s.t. $x=(a+b)+J$
since $b\in J$, $b+J=0+J$ so $x=(a+b)+J=a+J$. Then $x=f(a)$ ∎

Claim: $\ker f=I\cap J$
proof: ($\supseteq$): let $a\in I\cap J$, Then $f(a)=a+J=0+J$ (since $a\in J$)
($\subseteq$): Suppose $a\in I$ & with $f(a)=0+J$. Then $a+J=0+J$. This happens iff $a\in J$
so $a\in I$ & $a\in J$ so $a\in I\cap J$ ∎

Then, by the first Isom Thm, $I/\ker f\cong \operatorname{im} f$
$\|$ $\|$
$I/I\cap J$ $(I+J)/J$ ∎

(3)(a) $I/J=\{a+J : a\in I\}\subseteq R/J$ (Indeed, if $a\in I$ & $b\in J$, $a+b\in I$ (since $J\subseteq I$), so the set of all elements in R equivalent to a mod J is a subset of I).

To be clearer (about the fact that $I/J\subseteq R/J$), in principal, $a+J$ contains all elements $r\in R$ s.t. $a-r\in J$ & so could contain elements not in I, however, as an element of I/J, $a+J$ would only contain elements in I. But because of this, these two concepts of coset are the same.

$I/J\subseteq R/J$: $a+J, b+J\in I/J$ & $r+J\in R/J$
• $(a+J)-(b+J)=a-b+J$. since $a-b\in I$, $a-b+J\in I/J$
• $(r+J)(a+J)=ra+J$. since $ra\in I$, $ra+J\in I/J$
similarly for $(a+J)(r+J)$ ∎

(3) (b) define $\varphi: R/J \longrightarrow R/I$
$a+J \longmapsto a+I$

Claim: φ is well-defined

proof: suppose $a+J = b+J$. Then $\exists x \in J$ s.t. $a = b+x$

$\varphi(a+J) = \varphi(b+x+J) = b+x+I = b+I$ (since $x \in I$)
$= \varphi(b+J)$

so φ is indep of choice of representative of the coset $a+J$ ☒

Claim: φ is a homom:

proof: • $\varphi((a+J)+(b+J)) = \varphi(a+b+J) = a+b+I = (a+I)+(b+I) = \varphi(a+J)+\varphi(b+J)$

• $\varphi((a+J)(b+J)) = \varphi(ab+J) = ab+I = (a+I)(b+I) = \varphi(a+J)\varphi(b+J)$ ☒

☒

Claim: φ is surjective: let $a+I \in R/I$, then $\varphi(a+J) = a+I$

Claim: $\ker\varphi = I/J$

proof: $\supseteq$: let $a+J \in I/J$, then $a \in I$ so $\varphi(a+J) = a+I = 0+I$

$\subseteq$: let $a+J \in R/J$ s.t. $\varphi(a+J) = 0+I$, then $a+I = 0+I$, so $a \in I$

Hence $a+J \in I/J$ ☒

The first isom Thm $\Rightarrow (R/J)/\ker\varphi \cong \operatorname{im}\varphi$

$(R/J)/(I/J) = R/I$ (QED)

(4) Suppose $\psi: R[x] \to S$ is s.t. $\psi(r) = \varphi(r)$ $\forall r \in R$ & $\psi(x) = \varphi(x)$ & ψ a homom.

Show $\psi(f(x)) = \varphi(f(x))$ $\forall f(x) \in R[x]$

$f(x) = \sum_{i=0}^{n} a_i x^i$. Since ψ is a homom, $\psi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \psi(a_i)\psi(x)^i$

Then $= \sum_{i=0}^{n} \varphi(a_i)\varphi(x)^i$

$= \varphi\left(\sum_{i=0}^{n} a_i x^i\right)$ (QED)

(5) (a) • $\varphi\left(\sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i\right) = \varphi\left(\sum_{i=0}^{l} (a_i+b_i) x^i\right)$ (where $l = \max(m,n)$ & $a_i = 0$ for $i > m$, $b_i = 0$ for $i > n$)

$= \sum_{i=0}^{l} (a_i+b_i)(y+1)^i = \sum_{i=0}^{m} a_i(y+1)^i + \sum_{i=0}^{n} b_i(y+1)^i = \varphi\left(\sum_{i=0}^{m} a_i x^i\right) + \varphi\left(\sum_{i=0}^{n} b_i x^i\right)$

• $\varphi\left(\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right)\right) = \varphi\left(\sum_{i,j} a_i b_j x^{i+j}\right) = \sum_{i,j} a_i b_j (y+1)^{i+j} = \left(\sum_{i=0}^{m} a_i (y+1)^i\right)\left(\sum_{j=0}^{n} b_j (y+1)^j\right)$

(5)(a) (cont'd): so φ is a ring homom.

Claim: φ is surjective:

proof: let $\sum_{i=0}^{n} b_i y^i \in (\mathbb{Z}/2\mathbb{Z})[y]$, Then $\varphi\left(\sum_{i=0}^{n} b_i (x+1)^i\right) = \sum_{i=0}^{n} b_i (y+2)^i$

$= \sum_{i=0}^{n} b_i y^i$ (since $2=0$)

so $\sum_{i=0}^{n} b_i y^i \in \operatorname{im}\varphi$ ☑

Claim: φ is injective:

proof: let $\sum_{i=0}^{n} a_i x^i \in \ker\varphi$, so $\sum_{i=0}^{n} a_i (y+1)^i = 0$

$a_n y^n + (n a_n + a_{n-1}) y^{n-1} + \cdots$

$\Rightarrow a_n = 0$ ↯ Then $\Rightarrow a_{n-1} = 0$ & on & on ... ☑

(b) let $\pi: (\mathbb{Z}/2\mathbb{Z})[y] \to (\mathbb{Z}/2\mathbb{Z})[y]/(y^3+y^2+1)$ & let $\bar{\varphi} = \pi \circ \varphi$. Then $\bar{\varphi}$ is a homom since it is the composition of two homoms.

↳ the natural homom.

$\bar{\varphi}$ is surjective since it is the composition of two surjective maps

Claim: $\ker\bar{\varphi} = (x^3+x+1)$

proof: ($\supseteq$): $\bar{\varphi}(x^3+x+1) = (y+1)^3 + (y+1) + 1 + J$ (where $J = (y^3+y^2+1)$)

$= y^3 + 3y^2 + 3y + 1 + y + 1 + 1 + J$

$= y^3 + y^2 + y + 1 + y + 1 + 1 + J$ (coefficients are in $\mathbb{Z}/2\mathbb{Z}$)

$= y^3 + y^2 + 1 + J$

$= 0 + J$

($\subseteq$): [illegible]

Since φ is injective, $\ker\bar{\varphi} = \varphi^{-1}(\ker\pi) = \varphi^{-1}((y^3+y^2+1))$

Claim: $(x^3+x+1) = \varphi^{-1}((y^3+y^2+1))$

proof: ($\subseteq$) $\varphi(x^3+x+1) = y^3+y^2+1$ by above calculation so $(x^3+x+1) \subseteq \varphi^{-1}(J)$

($\supseteq$): suppose $f(x) \notin (x^3+x+1)$, Then $\exists\, q(x), r(x) \in (\mathbb{Z}/2\mathbb{Z})[x]$ with $\deg r \le 2$ & $r(x) \neq 0$ s.t. $f(x) = (x^3+x+1)\,q(x) + r(x)$

$\varphi(f(x)) = (y^3+y^2+1)\,\varphi(q(x)) + \varphi(r(x))$. Since $\varphi(r(x))$ has degree ≤ 2 any, $\varphi(r(x)) \notin J$ so $\varphi(f(x)) \notin J$ so $f(x) \notin \varphi^{-1}(J)$ ☑ ☑

Then, First Isom Thm $\Rightarrow (\mathbb{Z}/2\mathbb{Z})[x]/(x^3+x+1) \cong (\mathbb{Z}/2\mathbb{Z})[y]/(y^3+y^2+1)$