① Let R be a commutative ring w. $1 \neq 0$, and suppose that for every $r \in R$ there is some $n > 1$ s.t. $r^n = r$. Prove: every prime ideal of R is maximal.

Pf P - prime ideal

P is maximal $\iff$ R/P is a field

Pick $a + P \in R/P$ s.t. $a \neq 0$. Then $\exists\, n > 1$ s.t.

$a^n = a \Rightarrow a^n - a = 0 \Rightarrow a(\underline{a^{n-1} - 1}) = 0.$ $\neq 0$

Note: $(a+P)(a^{n-2}+P) = a \cdot a^{n-2} + P = a^{n-1} + P$

Claim $a^{n-1} + P = 1 + P$

$\overline{a^{n-1} - 1} = \overline{0} \Rightarrow \overline{a^{n-1}} = \overline{1}$

② G - gp. of order $132 = 11 \cdot 12$

Show: G has a normal sbgp. of order 11 or a normal sbgp. of order 12.

Sylow 3 $n_{11} \equiv 1 \bmod 11$

$n_{11} \mid 12$ $n_{11} \in \{1, 12\}$ ✓

If $n_{11} = 12$, we have 12 sbgps, each w. 11 elements.

have 120 elements of order 11 + identity

left: 11 elements

$n_3 \in \{1, 4\}$

$n_2 \in \{1, 3\}$

Cases $n_2=1, n_3=1$ fills up 12 elts ✓

$n_2=1, n_3=4$ ✓

$n_2=3, n_3=1$ ✓

~~$n_2=3, n_3=4$~~ counting argument

Let H be a normal Sylow 2-sbgp,

K Sylow 3-sbgp

H normal $\Longrightarrow$ HK is a sbgp. of order 12 ✓

(Hung. I.5.3)

$\Longrightarrow$ HK is unique,

hence normal $\square$

③ Let $g = x^2+2x-1 \in \mathbb{F}_5[x]$.

(a) Let $\mathcal{E}$ be the quotient ring $\mathbb{F}_5[x]/(g)$. Show that $\mathcal{E}$ is a field. What is $|\mathcal{E}|$ and why?

$\Longrightarrow$ Show (g) is maximal.

Suffices to show (g) is irreducible.

$$\left.\begin{matrix} g(0) \\ g(1) \\ g(2) \\ g(3) \\ g(4) \end{matrix}\right\} \neq 0 \bmod 5$$

hence (g) is irred.

$|\mathcal{E}| = 25$ Hung. I.V.6

(b) $\alpha := x + (g) \in \mathcal{E}$

What is the order of α in $\mathcal{E}^\times$?

$(x+(g))^{12} = 1 + (g)$ (check: 1, 2, 3, 4, 6, 8, 12)

(4) R - UFD

(a) Show π is irreducible in R iff (π) in R is prime.

($\Leftarrow$) See Hungerford

(π) prime $\Leftrightarrow$ π is prime (nonzero, nonunit)

Suppose $\pi = ab$ $a, b \in R$

$\Rightarrow \pi \mid ab \Rightarrow \pi \mid a$ or $\pi \mid b$

wlog, $\pi \mid a \Rightarrow \exists c \in R$ st. $\pi c = a$

$\Rightarrow \pi = ab = \pi c b \Rightarrow 1 = cb$:)

so b is a unit!

($\Rightarrow$) Assume π is irreducible. Show (π) is prime.

nonzero & nonunit

Suffices to show π is prime.

$a, b \in R$ st. $\pi \mid ab$ Goal: $\pi \mid a$ or $\pi \mid b$

at least one of a, b is a nonunit

(UFD) $a = p_1 \cdots p_n$, p_i irred.

$b = q_1 \cdots q_m$, q_i irred.

$\Rightarrow$ $ab = p_1 \cdots p_n q_1 \cdots q_m$

$\pi \mid ab$, so $\exists c \in R$ s.t. $\pi c = ab$

$\pi c = p_1 \cdots p_n q_1 \cdots q_m$

$\pi c_1 \cdots c_\ell = p_1 \cdots p_n q_1 \cdots q_m$

UFD $\Rightarrow$ π must be associate to some p_i or q_j

$\Longrightarrow \pi \mid a$ or $\pi \mid b$ $\square$

(b) π irred.

$Q \subset (\pi)$, Q is a nonzero prime ideal

Show $Q = (\pi)$.

Show $(\pi) \subset Q$

Q prime $\Rightarrow$ $\exists$ nonunit, nonzero $q \in Q$

UFD $\Rightarrow q = q_1 \cdots q_n$, q_i irred.

Q is prime $\Longrightarrow \exists q_i$ s.t. $q_i \in Q \subset (\pi)$

Hence, $(q_i) \subset Q \subset (\pi)$, q_i irred.

UFD $\Rightarrow q_i$ and π are associates

hence $(\pi) = (q_i) \subset Q$

(5) R comm. ring w. $1 \neq 0$, I, J ideals of R

Show $\exists$ R-module isomorphism

$$\varphi : R/I \otimes_R R/J \longrightarrow R/(I+J) \text{ s.t.}$$

$$\varphi(\bar{x} \otimes \bar{y}) = \overline{xy}$$ universal ppty :)

Pf $\cdot\ f : R/I \times R/J \longrightarrow R/(I+J)$

<u>well-def</u> $(\bar{x},\bar{y}) = (\bar{a},\bar{b})$ $\quad x+I = a+I,\ y+J = b+J$

$$f((\bar{x},\bar{y})) = \overline{xy} = xy + (I+J)$$

$$f((\bar{a},\bar{b})) = \overline{ab} = ab + (I+J)$$

$$xy - ab \in I+J$$

$$xy \to (a+i)(b-j)$$

$$ab - aj + ib - ij - ab = -aj + ib - ij \in I+J \quad \checkmark$$

Hence, $\overline{xy} = \overline{ab}$

<u>f bilinear</u>

- $f((\overline{x_1+x_2},\bar{y})) = \overline{(x_1+x_2)y} = \overline{x_1y} + \overline{x_2y} = f((\bar{x}_1,\bar{y})) + f((\bar{x}_2,\bar{y}))$
- $f((\bar{x},\overline{y_1+y_2}))$ in a similar manner
- $r \in R$, $r \cdot f((\bar{x},\bar{y})) = r \cdot \overline{xy} = r(x+I)(y+J)$

$$= (rx+I)(y+J) = (x+I)(ry+J)$$

$$= f((\overline{rx},\bar{y})) = f((\bar{x},\overline{ry})) \quad \text{bilinear!}$$

$\overline{xr}$ if R is not comm.

- Universal ppty:

$$\begin{tikzcd}
R/I \times R/J \arrow[rr, "f"] \arrow[dr, "i"'] & \arrow[d, phantom, "\circ"] & R/(I+J) \\
& R/I \otimes_R R/J \arrow[ur, "\exists!\ \varphi \text{ homom.}"'] &
\end{tikzcd}$$

- Show φ is injective & surjective

<u>Surjective</u>

let $\bar{d} \in R/(I+J)$ $\qquad \bar{d} = d + (I+J)$

$\varphi(\bar{d} \otimes \bar{1}) = \bar{d}$ ✓

$r \in R$

$r \otimes 1 - 1 \otimes r = 0$

<u>injective</u>

$$\varphi\left(\sum_{i=1}^{n} \overline{a_i \otimes b_i}\right) = \sum_{i=1}^{n} \overline{a_i b_i} = 0$$

so $\displaystyle\sum_{i=1}^{n} a_i b_i \in I + J$

$\displaystyle\sum_{i=1}^{n} a_i b_i = \alpha + \beta$, $\alpha \in I$, $\beta \in J$

$\displaystyle\sum_{i=1}^{n} a_i b_i - \beta = \alpha \in I$

$\displaystyle\sum_{i=1}^{n} \bar{a}_i \otimes \bar{b}_i = \sum_{i=1}^{n} \overline{a_i b_i} \otimes \bar{1}$ $\qquad \bar{1} \otimes \beta = 0$

hence, $\sum_{i=1}^{n} \overline{a_i b_i} \otimes \overline{1} + \overline{1} \otimes \overline{\beta}$

$(\overline{\alpha} + \overline{\beta}) \otimes \overline{1}$
$=$
$\overline{\alpha} \otimes \overline{1} + \overline{1} \otimes \overline{\beta}$
$=$
$\overline{0}$

$$\sum_{i=1}^{n} \overline{a_i b_i} \otimes \overline{1} - \overline{\beta} \otimes \overline{1}$$

$$= \left(\sum_{i=1}^{n} \overline{a_i b_i - \beta}\right) \otimes \overline{1}$$

$$= \overline{\alpha} \otimes \overline{1} = \overline{0}$$

$$= \overline{0} \otimes \overline{1} = \overline{0}$$

$\square$

⑥ Let p be an odd prime number, and

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$$

ⓐ Show f is irreducible in $\mathbb{Q}[x]$ using Einsestein.

Pf $\quad f(x+1)x = (x+1)^p - 1$

$$= x^p + \binom{p}{1} x^{p-1} + \cdots + 1 - 1$$

$$= x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1} x$$

$$\Rightarrow f(x+1) = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1}$$

Choose prime p for Einsestein

$p \mid \binom{p}{k}$ done :)

but $p^2 \nmid \binom{p}{p-1} = p$

(b) Let $\zeta = e^{2\pi i/p} \in \mathbb{C}$, and let $K = \mathbb{Q}(\zeta)$. Show K is the splitting field of f over $\mathbb{Q}$.

$$f = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{p-1})$$

$$f(x)(x-1) = x^p - 1 \quad \text{so} \quad f(\zeta^n)(\zeta^n - 1) = 0$$

$$\zeta^n - 1 \neq 0 \text{ for } n = 1, \dots, p-1$$

$$\Rightarrow f(\zeta^n) = 0$$

(c) Let $G = \mathrm{Gal}(K/\mathbb{Q})$. For $\sigma \in G$, show $\exists!$ integer $m(\sigma) \in \{1, \dots, p-1\}$ s.t. $\sigma(\zeta) = \zeta^{m(\sigma)}$.

Let $\sigma, \tau \in G$ s.t. $m(\sigma) = m(\tau)$.

Let $k \in \mathbb{Z}$

$$\sigma(\zeta^k) = \sigma(\zeta)^k = (\zeta^{m(\sigma)})^k$$

$$= (\zeta^{m(\tau)})^k = \tau(\zeta^k)$$

$$\Rightarrow \sigma = \tau$$

(d) Prove that $m: G \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ defined in (c) is a gp. isomorphism.

(showed injectivity in (c))

<u>homom</u> $\sigma, \tau \in G$

$$m(\sigma \circ \tau) \overset{?}{=} m(\sigma) m(\tau)$$

$$(\sigma \circ \tau)(\zeta) = \zeta^{m(\sigma \circ \tau)}$$

$$\sigma(\zeta) = \zeta^{m(\sigma)}, \quad \tau(\zeta) = \zeta^{m(\tau)}$$

$$\sigma(\tau(\zeta)) = \sigma(\zeta^{m(\tau)}) = \zeta^{m(\sigma) m(\tau)}$$

For each $k \in \{1, \dots, p-1\}$, one have a different σ sending $\zeta \longmapsto \zeta^k$

surjectivity

(7) (a) surjective ; R-mod homom. $g \circ h = f$

(b) property of your choice in Hungerford (sec. 3 & 4) or Dummit Foote

(c) Show that if M_i, $i \in I$, are projective left R-modules, then the direct sum $\bigoplus_{i \in I} M_i$ is a projective left R-mod.

Pf universal ppty for direct sum (coproduct) (IV.I.13 Hungerford)

Also see projective modules in Hungerford

or use the characterization of direct summands of free modules (mention Axiom of Choice)

(8) G group, V a 2-dim vector space over field K

Suppose we have an action of G on V, $(g,v) \mapsto g \cdot v$

s.t. $\forall g \in G$, $c \in K$, $v, w \in V$

$$g \cdot (cv) = c(g \cdot v)$$

$$g \cdot (v+w) = g \cdot v + g \cdot w$$

(a) Use the action of G to define a gp. hom.

$\varphi : G \to GL_2(K)$

$\varphi : G \to M_2(K)$, show φ is multiplicative

let $\{e_1, e_2\}$ be a basis of V

$$(g, e_1) \mapsto g \cdot e_1 = \lambda_{11} e_1 + \lambda_{21} e_2 \qquad \lambda_{ij} \in K$$

$$(g, e_2) \mapsto g \cdot e_2 = \lambda_{12} e_1 + \lambda_{22} e_2$$

$$\varphi(g) = \begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix}$$

straightforward to show it is multiplicative ($\varphi(gh) = \varphi(g)\varphi(h)$)

$$\varphi(h) = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix}, \text{ for } \gamma_{ij} \in K$$

$$(gh, e_1) \mapsto (gh) \cdot e_1 = g \cdot (h \cdot e_1) = g(\gamma_{11} e_1 + \gamma_{21} e_2)$$

$$= (\gamma_{11}\lambda_{11} + \cancel{\gamma_{21}}\lambda_{12})e_1 + (\gamma_{11}\lambda_{12} + \gamma_{21}\lambda_{22})e_2$$

$$(gh, e_2) \mapsto (\gamma_{12}\lambda_{11} + \gamma_{22}\lambda_{12})e_1$$
$$+ (\gamma_{12}\lambda_{21} + \gamma_{22}\lambda_{22})e_2$$

hence ρ is multiplicative

ρ is invertible: $\rho(e) = I_2$

$$\rho(e) = \rho(g^{-1}g) = \rho(g^{-1})\rho(g) = I_2$$
$$\text{''}\ \rho(gg^{-1}) = \rho(g)\rho(g^{-1})$$

Hence codomain is $GL_2(K)$ so

$\rho: G \to GL_2(K)$ is a homom

(b) Show V has a 1-dim subspace W that is fixed by G.

$g(e_1) = e_1$ so $g(\lambda e_1) = \lambda e_1$