July 28

Friday, 24 July 2020 16:11

August 2016:

⑧ - $R = \mathbb{Z}[x]$: $0 \longrightarrow R \xrightarrow{f} R \xrightarrow{g} \mathbb{Z} \longrightarrow 0$

For $P \in R$ then $f(P) = x \cdot P$, $g(P) = P(0)$. Action $\begin{aligned} R \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, 1) &\longmapsto 0 \end{aligned}$

(a) Show that is exact as R-mods.

(i) f is injective : if $f(P) = 0$ then $x \cdot P(x) = 0$, and since $\mathbb{Z}[x]$ is integral domain we must have $P = 0$.

(ii) g is surjective : for each $n \in \mathbb{Z}$ take $P(x) = n$, now $g(P) = n$.

(iii) $\operatorname{im}(f) = \ker(g)$:

$\subseteq$) $P \in R$, then $g(f(P)) = g(x \cdot P(x)) = 0 \cdot P(0) = 0$.

$\supseteq$) $P \in R$ with $g(P) = P(0) = 0$, then P has no constant term, so we can factor x. Then there is $Q \in R$ with $x \cdot Q = P$, then $f(Q) = P$.

(b) Does it split as R-mods?

If it splits, then there exists a section $h: \mathbb{Z} \longrightarrow R$ with $gh = 1_{\mathbb{Z}}$. Hungerford IV 1.18.

Since h cannot be zero, we have $h(j) = j h(1) \neq 0$ for all $j \in \mathbb{Z}$.

But then using the R-mod action : $x \cdot h(j) = h(x \cdot j) = h(0) = 0$.

This is a contradiction with $x \neq 0$, $h(j) \neq 0$, so since R is an integral domain : $x \cdot h(j) \neq 0$.

Thus the sequence does not split.

(c) Does it split as $\mathbb{Z}$-mods?

Define: $\begin{aligned} h: \mathbb{Z} &\longrightarrow R \\ 1 &\longmapsto 1 \end{aligned}$. Now: $gh(j) = g(j) = j$ for all $j \in \mathbb{Z}$; so $gh = 1_{\mathbb{Z}}$.

Hungerford IV.1.18. The sequence splits. Detail: why is h a $\mathbb{Z}$-homomorphism.

Alternatively: $\mathbb{Z}$ is free, hence projective, as $\mathbb{Z}$-mod, so the sequence splits.

January 2017:

①- Prove that S_4 / K_4 is isomorphic to S_3.

Since everything is finite: $\left| S_4/K_4 \right| = \dfrac{|S_4|}{|K_4|} = \dfrac{4!}{4} = 6$.

[illegible] S_3. Hungerford II.6

Since everything is finite: $\left|S_4/K_4\right| = \frac{|S_4|}{|K_4|} = \frac{24}{4} = 6$.

We know that there are only two groups of order 6: $\mathbb{Z}_6$ and S_3. Hungerford II.6.

If we show that S_4/K_4 is <u>not</u> abelian, then $S_4/K_4 \cong S_3$.

We will show $S_4/K_4 \not\cong \mathbb{Z}_6$ by showing that it does <u>not</u> contain an element of order 6. Let $\sigma \in S_4$, then $|\sigma|$ is the least common multiple of the orders of the disjoint cycles into which it decomposes. Since σ acts on four elements, the decomposition must be:

σ is a 4-cycle ; σ is a 3-cycle, σ is two disjoint 2-cycles, σ is a 2-cycle.

But all of these have order less than six.

An element of S_4/K_4 is of the form σK_4 where $\sigma \in S_4$. Now $|\sigma K|$ divides $|\sigma|$, so $|\sigma K| < 6$. So S_4/K_4 has no element of order 6, so $S_4/K_4 \cong S_3$.

② - How many Sylow 2 and Sylow 5 subgroups are there in a non-commutative group of order 20?

$|G| = 2^2 \cdot 5$, so by the Third Sylow Theorem: $n_5 = 1$, $n_2 = 1, 5$.

Suppose $n_2 = 1$, we prove that G is abelian. Let H_2 H_5 be the only Sylow 2-subgroup, 5-subgroup by the Second Sylow Theorem, $H_2 \trianglelefteq G$, $H_5 \trianglelefteq G$. Also $|H_2| = 4$, $|H_5| = 5$, and $H_2 \cap H_5 = \{e\}$.

Hungerford I.5.3. By normality and trivial intersection: H and K commute.

Also $\underline{HK = H \times K} < G$. Now: $|H \times K| = 20 = |G|$ so $H \times K = G$.

<u>Alternatively</u>: Hungerford I.8.6. $H, K \trianglelefteq G$, $H \cap K = \{e\}$ so $H \times K = G$.

Now H is commutative, K is commutative, and H and K commute with each other, so G is commutative.

Hence G has 5 Sylow 2-subgroups and 1 Sylow 5-subgroup.

③ - Let $T = \{z \in \mathbb{C} \mid |z| = 1\}$ group with respect to multiplication. Prove that $G < T$ finite means G cyclic.

Let $G < T$ finite subgroup, if $G = \{1\}$ then it is cyclic. Let G non-trivial. We can write elements of T as: $e^{\theta i}$ for $0 \leq \theta < 2\pi$. Consider:

$$G = \{e^{\theta i} \in T \mid \theta \in J \subseteq \mathbb{N} \text{ finite}\}.$$

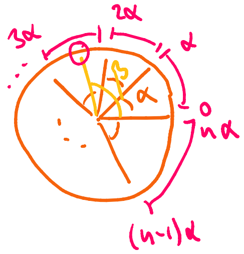
Let: $\alpha := \min\{\theta \in J \mid e^{\theta i} \neq 1\}$, which exists because J is finite. Then we have:

$e^{\alpha i} \in G$, so it has some order $|e^{\alpha i}| = n$, i.e. $e^{n\alpha i} = 1$.

$e^{\alpha i} \in G$, so it has some order $|e^{\alpha i}| = n$, i.e. $e^{n\alpha i} = 1$.

Suppose G is <u>not</u> cyclic, then there is $\beta \in J$ with $e^{\beta i} \notin \langle e^{\alpha i} \rangle = \{1, e^{\alpha i}, \dots, e^{(n-1)\alpha i}\}$.

Now $\beta \in (k\alpha, (k+1)\alpha)$ for some $k = 0, \dots, n-1$. Hence: $e^{\beta i - k\alpha i} = \underbrace{e^{\beta i}}_{\overset{\cap}{G}} \cdot \underbrace{e^{-k\alpha i}}_{\overset{\cap}{G}} \in G$ for



that specific $k = 0, \dots, n-1$. But now $\beta - k\alpha \in J$, and $k\alpha < \beta < (k+1)\alpha$ means $\beta - k\alpha < \alpha$. This contradicts the minimality of α. So $G = \langle e^{\alpha i} \rangle$ must be cyclic.

<u>Alternatively</u>: Use the clasification theorem for finitely generated abelian groups, pick element of maximal order, get contradiction.

④ - Prove that every two sided ideal of $M_n(\mathbb{Z})$ is of the form $M_n(k\mathbb{Z})$ for some $k \in \mathbb{N}$.

Note that $k\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal. All ideals of $\mathbb{Z}$ are of this form.

<u>Claim:</u> Let R commutative ring (with unit), then every two sided ideal of $M_n(R)$ is of the form $M_n(I)$ for some ideal $I \subseteq R$.

Let $J \subseteq M_n(R)$ a two sided ideal. Let: $I := \{a \in R \mid \text{there is } A \in J \text{ with } a_{11} = a\}$.

This is an ideal: if $a, b \in I$ then there are $A, B \in J$ with $a_{11} = a$, $b_{11} = b$, so:

$a - b = a_{11} - b_{11} = c_{11}$ for $C = A - B \in J$. If further $r \in R$, then:

$r \cdot a = d_{11}$ for $D = \begin{bmatrix} r & 0 & \cdots & 0 \\ 0 & & & \vdots \\ \vdots & & & \\ 0 & \cdots & \cdots & 0 \end{bmatrix} A \in J$.

Now we prove $J = M_n(I)$.

$\subseteq$) Pick $A \in J$, then:

$$\begin{bmatrix} 0 \cdots 0 \overset{j}{1} 0 \cdots 0 \\ \\ 0 \\ \\ \end{bmatrix} \underbrace{\begin{bmatrix} & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{bmatrix}}_{\overset{\cap}{J}} \begin{matrix} \\ i \\ \\ \end{matrix}\!\begin{bmatrix} 0 & \\ \vdots & \\ 0 & \\ 1 & 0 \\ 0 & \\ \vdots & \\ 0 & \end{bmatrix} = \begin{bmatrix} a_{ij} & \\ & * \\ & \end{bmatrix} \in J$$

so $a_{ij} \in I$ for all $i, j = 1, \dots, n$.

Hence $A \in M_n(I)$.

$\supseteq$) Pick $B \in M_n(I)$. Since $b_{ij} \in I$ for all $i, j = 1, \dots, n$, there are matrices $A_{ij} \in J$ such that $(a_{ij})_{11} = b_{ij}$. Now:

such that $(a_{ij})_{11} = b_{ij}$. Now:

$$B_{ij} := \underbrace{\begin{array}{c} \\ \\ \\ i \\ \\ \\ \\ \end{array}\!\!\begin{bmatrix} 0 & & \\ \vdots & & \\ 0 & & \\ 1 & & 0 \\ 0 & & \\ \vdots & & \\ 0 & & \end{bmatrix}}_{X} \underbrace{\begin{bmatrix} 1 & \\ & 0 \end{bmatrix} A_{ij} \begin{bmatrix} 1 & \\ & 0 \end{bmatrix}}_{\begin{bmatrix} b_{ij} & \\ & 0 \end{bmatrix}} \underbrace{\begin{array}{c} \quad\quad j \\ \begin{bmatrix} 0 \cdots 0\ 1\ 0 \cdots 0 \\ \\ 0 \\ \\ \end{bmatrix} \end{array}}_{Y} = \begin{array}{c} \\ i \end{array}\!\!\begin{array}{c} j \\ \begin{bmatrix} b_{ij} \end{bmatrix} \end{array} \in J \text{ since } A_{ij} \in J.$$

So: $B = \sum_{i,j=1}^{n} B_{ij} \in J$.

Alternatively: use linear transformations for the matrices X, Y.

5 - Are $\mathbb{Z}[x]/(x^2-2)$ and $\mathbb{Z}[x]/(x^2-3)$ isomorphic?

Suppose: $\phi : \mathbb{Z}[x]/(x^2-2) \longrightarrow \mathbb{Z}[x]/(x^2-3)$ is an isomorphism. We must have $\phi(1) = 1$, so

$\phi(j) = j$ for all $j \in \mathbb{Z}$. Now let's look at $\phi(x)$:

$\phi(x)^2 = \phi(x^2) = \phi(2) = 2$, since $x^2 \equiv 2 \mod x^2-2$.

Since ϕ is surjective, we must have $\phi(x) = ax+b$ for some $a \neq 0$ (otherwise $\mathrm{im}(\phi) \subseteq \mathbb{Z}$).

Now: $(ax+b)^2 = a^2x^2 + b^2 + 2axb = 3a^2 + b^2 + 2axb \mod x^2-3$.

And: $(ax+b)^2 = \phi(x)^2 = 2 \mod x^2-3$.

For this, we need: $2ab = 0$, hence $b=0$ since $a \neq 0$ and $b \in \mathbb{Z}$. Then: $3a^2 = 2$ which has no solution in $\mathbb{Z}$. Contradiction.

Hence $\mathbb{Z}[x]/(x^2-2)$ and $\mathbb{Z}[x]/(x^2-3)$ are not isomorphic.

6 - R ring, M an R-mod Noetherian. Let $\phi : M \to M$ surjective R-hom. Show ϕ is an isomorphism.

We want to show that ϕ is injective. Suppose not, that is, suppose $\mathrm{Ker}(\phi) \neq \{0\}$.

Claim: $\mathrm{Ker}(\phi) \subsetneq \mathrm{Ker}(\phi^2) \subsetneq \cdots \subsetneq \mathrm{Ker}(\phi^n) \subsetneq \mathrm{Ker}(\phi^{n+1}) \subsetneq \cdots$.

Remark: ϕ surjective means ϕ^n is also surjective. details.

Now if $\mathrm{Ker}(\phi) \neq \{0\}$, we show $\mathrm{Ker}(\phi^n) \subsetneq \mathrm{Ker}(\phi^{n+1})$. For $m \in \mathrm{Ker}(\phi^n)$, then $\phi^{n+1}(m) = \phi(\phi^n(m)) = 0$, so indeed $\mathrm{Ker}(\phi^n) \subseteq \mathrm{Ker}(\phi^{n+1})$. Pick $x \in M$ non-zero, $x \in \mathrm{Ker}(\phi)$. Since ϕ^n is surjective, there is $y \in M$ with $\phi^n(y) = x$, and now $\phi(\phi^n(y)) = \phi(x) = 0$. Hence $y \in \mathrm{Ker}(\phi^{n+1})$

there is $y \in M$ with $\phi^n(y) = x$, and now $\phi(\phi^n(y)) = \phi(x) = 0$. Hence $y \in \mathrm{Ker}(\phi^{n+1})$ but $y \notin \mathrm{Ker}(\phi^n)$. Then $\mathrm{Ker}(\phi^n) \subsetneq \mathrm{Ker}(\phi^{n+1})$.

We found:

$\mathrm{Ker}(\phi) \subsetneq \mathrm{Ker}(\phi^2) \subsetneq \cdots \subsetneq \mathrm{Ker}(\phi^n) \subsetneq \mathrm{Ker}(\phi^{n+1}) \subsetneq \cdots$ an ascending chain of submodules that doesn't stabilize, a contradiction with M being Noetherian.

(7)- R I.D. Show that R field iff every R-mod is projective.

$\Rightarrow$) Suppose R field, the R-mods are R-vector spaces, so they are free, so projective.

$\Leftarrow$) Suppose every R-mod is projective.

<u>Claim 1:</u> R cannot contain a proper ideal that is <u>not</u> prime.

<u>Claim 2:</u> If R is <u>not</u> a field, then R contains a proper ideal that is <u>not</u> prime.

<u>Proof 1:</u> Suppose $I \subseteq R$ is a proper ideal that is <u>not</u> prime. Since R is an integral domain, $I \neq \{0\}$ since otherwise we would have zero divisors. Consider R/I an R-mod. Then by hypothesis R/I is projective.

We have: $\pi : R \longrightarrow R/I$, $r \longmapsto r+I$, $1_{R/I} : R/I \longrightarrow R/I$, $r+I \longmapsto r+I$.

We can fit them:

$$\begin{tikzcd} & R/I \arrow[dl, dashed, "f"'] \arrow[d, "1_{R/I}"] & \\ R \arrow[r, "\pi"] & R/I \arrow[r] & 0 \end{tikzcd}$$

Since R/I is projective, there exists some R-hom: $f : R/I \longrightarrow R$ such that $\pi f = 1_{R/I}$.

Since I is <u>not</u> prime, there are $r, s \in R \setminus I$ such that $rs \in I$ and $r, s \notin I$. Now:

$\pi f(s+I) = s+I \neq I$, so $s+I \neq 0$, also since R is an integral domain and $r \neq 0$, $f(s+I) \neq 0$, then $r f(s+I) \neq 0$.

But:

$r f(s+I) = f(r(s+I)) = f(rs+I) = f(I) = 0$, a contradiction.

This proves Claim 1.

<u>Proof 2:</u> Let R <u>not</u> be a field, we want a proper, not-prime, ideal.

Pick $r \in R$ that is <u>not</u> a unit, which exists because R is <u>not</u> a field.

[illegible] prime then $\langle r \rangle$ is <u>not</u> prime, proper, ideal.

Pick $r \in R$ that is not a unit, which exists because R is not a field.

If r is not prime then $\langle r \rangle$ is not prime, proper, ideal.
If r is prime, then $r^2 | r \cdot r$, but if $r^2 | r$ then $r = s \cdot r^2$ for some $s \in R$. Since R is integral domain, we can cancel: $1 = s \cdot r$, so in fact r is a unit. Hence r^2 is not prime, so $\langle r^2 \rangle$ is not prime, proper, ideal.
This prover claim 2.

To put everything together: by contrapositive of Claim 2, if R does not contain a proper, not-prime, ideal, then R is a field, and by Claim 1 we have that R indeed cannot contain a proper ideal that is not prime.

Alternatively: $\Leftarrow$) Suppose R not a field, consider R/M as R-mod, where M is any proper non-trivial ideal. Then:

$$0 \to M \to R \to R/M \to 0$$

splits because R/M is projective.

Then: $\underset{\text{integral domain.}}{\underset{\sim}{R}} \cong M \oplus \underbrace{R/M}_{\text{has torsion}}$, a contradiction.

(8)- k field, $a \in k$, p prime. Prove that $x^p + a$ is either irreducible or has a root in k.

If $p=2$ then x^2+a doesn't have a root in k iff it is irreducible, it works.

Assume $p \geq 3$ (is odd). In $\bar{k}$, factor: $x^p + a = (x-a_1)\cdots(x-a_p)$. Suppose x^p+a is not irreducible in k. Then: $x^p + a = f(x)g(x)$ for $f(x), g(x) \in k[x]$ and $\deg(f), \deg(g) \geq 1$.

Since p is odd, either f or g has even degree, let's say f. Now:

$f(x) = (x-a_1)\cdots(x-a_r)$ with $1 \leq r < p$, maybe reordering the roots.

Set: $b = a_1 \cdots a_r$, the constant term of f, so $b \in k$. Moreover: $a_i^p + a = 0$ because a_i are roots of x^p+a, so $a_i^p = -a$. Hence:

$$b^p = a_1^p \cdots a_r^p = (-a) \overset{r}{\cdots} (-a) = (-a)^r = a^r.$$

Since p is prime, it is coprime with r, so there are $m, n \in \mathbb{Z}$ such that:

$1 = mp + nr$. Thus:

$$a = a^1 = a^{mp+nr} = a^{mp} a^{nr} = (a^m)^p (a^r)^n = (a^m)^p (b^p)^n = (a^m)^p (b^n)^p = (a^m b^n)^p.$$

By p odd:

$a = a = a^{1} = a^{1}a = (a\ )\cdot(a\ ) = (a\ )\cdot(\ ) = (\ $

By p odd:

$$-a = -(a^m b^n)^p = (-a^m b^n)^p.$$ So $-a^m b^n$ is a root of $x^p + a$.

Since $a, b \in k$, we have $-a^m b^n \in k$.

⑨ - $g(x) = (x^2-2)(x^2+3) \in \mathbb{Q}[x]$, E the splitting field of g over $\mathbb{Q}$.

(a) What is $[E:\mathbb{Q}]$?

The roots of g are $\pm\sqrt{2}$ and $\pm i\sqrt{3}$, so $E = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$. Thus:

$$[E:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\cdot 2 = 4$$ because:

(i) x^2-2 is the minimal poly. of $\sqrt{2}$ over $\mathbb{Q}$ (irreducible).

(ii) x^2+3 is the minimal poly of $i\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ (irreducible).

(b) Construct $\mathrm{Gal}(E/\mathbb{Q}) = G$.

We have $|G| = [E:\mathbb{Q}] = 4$, so either $G \cong \mathbb{Z}_4, \mathbb{Z}_2\times\mathbb{Z}_2$.

Alternatively: send $\sqrt{2} \longmapsto \pm\sqrt{2}$, $i\sqrt{3} \longmapsto \pm i\sqrt{3}$. These are all in G by cardinality reasons. $\sigma : \begin{array}{l}\sqrt{2} \longmapsto -\sqrt{2}\\ i\sqrt{3} \longmapsto i\sqrt{3}\end{array}$; $\tau : \begin{array}{l}\sqrt{2} \longmapsto \sqrt{2}\\ i\sqrt{3} \longmapsto -i\sqrt{3}\end{array}$ have order 2.

Now: $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is $\mathbb{Z}_2$, given by: $\gamma : \sqrt{2} \longmapsto -\sqrt{2}$.
$\mathrm{id} : \sqrt{2} \longmapsto \sqrt{2}$.

This is good enough to claim: $G \cong \mathbb{Z}_2\times\mathbb{Z}_2$.

Then by the Extension Theorem, since $[\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ we have two possible ways of extending γ, id (for each): $i\sqrt{3} \mapsto \pm i\sqrt{3}$.

$\gamma_+ : \begin{array}{l}\sqrt{2} \longmapsto -\sqrt{2}\\ i\sqrt{3} \longmapsto i\sqrt{3}\end{array}$; $\delta : \begin{array}{l}\sqrt{2} \longmapsto \sqrt{2}\\ i\sqrt{3} \longmapsto -i\sqrt{3}\end{array}$; $\gamma_- : \begin{array}{l}\sqrt{2} \longmapsto -\sqrt{2}\\ i\sqrt{3} \longmapsto -i\sqrt{3}\end{array}$; $\mathrm{id} : \begin{array}{l}\sqrt{2} \longmapsto \sqrt{2}.\\ i\sqrt{3} \longmapsto i\sqrt{3}\end{array}$

$|\gamma_+| = 2$ $\quad |\delta| = 2$ $\quad |\gamma_-| = 2$

So $G \xrightarrow{\cong} \mathbb{Z}_2\times\mathbb{Z}_2$ is an explicit isomorphism.

$$\begin{array}{lcl}
\gamma_+ & \longmapsto & (1,0)\\
\delta & \longmapsto & (0,1)\\
\gamma_- & \longmapsto & (1,1)\\
\mathrm{id} & \longmapsto & (0,0)
\end{array}$$

(c) Show explicitly the correspondence between the intermediate fields $\mathbb{Q} \subseteq F \subseteq E$ and the subgroups $H \leq G$.

The subgroups of $G \cong \mathbb{Z}_2\times\mathbb{Z}_2$ are $\langle(1,0)\rangle, \langle(0,1)\rangle, \langle(1,1)\rangle, G, \langle(0,0)\rangle$.

The intermediate fields are: $\mathbb{Q}$, $\underbrace{\mathbb{Q}(\sqrt{2}, i\sqrt{3})}_{E}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{3})$, $\mathbb{Q}(i\sqrt{6})$.

$E^{\langle \mathrm{id}\rangle} = E$ so: $\mathbb{Q}(\sqrt{2}, i\sqrt{3}) \longleftrightarrow \langle \mathrm{id}\rangle$.

$E^{G} = \mathbb{Q}$ so: $\mathbb{Q} \longleftrightarrow G$.

$E^{\langle \mathrm{id} \rangle} = E$ so: $\mathbb{Q}(\sqrt{2}, i\sqrt{3}) \longleftrightarrow \langle \mathrm{id} \rangle$.

$E^{G} = \mathbb{Q}$ so: $\mathbb{Q} \longleftrightarrow G$.

$E^{\langle \gamma_+ \rangle} = \mathbb{Q}(i\sqrt{3})$ so: $\mathbb{Q}(i\sqrt{3}) \longleftrightarrow \langle \gamma_+ \rangle$.

$E^{\langle \delta \rangle} = \mathbb{Q}(\sqrt{2})$ so: $\mathbb{Q}(\sqrt{2}) \longleftrightarrow \langle \delta \rangle$.

$E^{\langle \gamma_- \rangle} = \mathbb{Q}(i\sqrt{6})$ so: $\mathbb{Q}(i\sqrt{6}) \longleftrightarrow \langle \gamma_- \rangle$.