January 2010

martes, 8 de agosto de 2023 6:21 p.m.

① Prove the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are isomorphic when n and m are relatively prime (positive) integers. Discuss whether these rings are ever isomorphic when m and n are not relatively prime.

Pf: Let $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $\varphi(a) = (a \bmod m, a \bmod n)$.

This is a homomorphism:

Let $a,b \in \mathbb{Z}$, then $\varphi(a+b) = (a+b \bmod m, a+b \bmod n)$
$= (a \bmod m, a \bmod n) + (b \bmod m, b \bmod n)$
$= \varphi(a) + \varphi(b)$

Let $a,b \in \mathbb{Z}$, then $\varphi(ab) = (ab \bmod m, ab \bmod n)$
$= (a \bmod m, a \bmod n)(b \bmod m, b \bmod n)$
$= \varphi(a)\varphi(b)$.

Lastly, $\varphi(1) = (1 \bmod m, 1 \bmod n)$.

Now we WTS $\ker(\varphi) = mn\mathbb{Z}$. $\ker(\varphi) = \{a \in \mathbb{Z} : \varphi(a) = (0,0)\}$:

$\varphi(a) = (a \bmod m, a \bmod n) = (0 \bmod m, 0 \bmod n) \Rightarrow \begin{matrix} a \equiv 0 \bmod m \\ a \equiv 0 \bmod n \end{matrix}$

$\Rightarrow m|a$ and $n|a$, but $(m,n)=1 \Rightarrow mn|a$.

So $\ker(\varphi) = mn\mathbb{Z}$.

Now we WTS that φ is surjective: Let $(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

We want α s.t. $\varphi(\alpha) = (a \bmod m, b \bmod n)$.

Since $(m,n)=1$, we know $\exists x,y \in \mathbb{Z}$ s.t. $xm + yn = 1$

Consider $\alpha = xmb + yna$. Then (Note $yn = 1 - xm$ and $xm = 1 - yn$)

$xmb + yna \bmod m \equiv yna \bmod m \equiv (1-xm)a \bmod m$
$\equiv a - xma \bmod m \equiv a \bmod m$

$xmb + yna \bmod n \equiv xmb \bmod n \equiv (1-yn)b \bmod n$
$\equiv b - ynb \bmod n \equiv b \bmod n$

Therefore, $\forall (a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $\exists\, \alpha = xmb + yna$ s.t. $\varphi(xmb+yna) = (a \bmod m, b \bmod n)$.

Thus, φ is surjective.

Therefore, φ is an isom. $\Rightarrow \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by the 1^{st} isom. thm.

The order of $(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is $\text{lcm}(m,n)$, where $|a| = m$, $|b| = n$.

If $(m,n) = 1$, then $|(a,b)| = mn$.

If $(m,n) \neq 1$, then $|(a,b)| = k < mn$, $k \in \mathbb{Z}$

So $\mathbb{Z}/mn\mathbb{Z}$ has an elt. of order mn, but $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ does not if $(m,n) \neq 1$.

Therefore, $\mathbb{Z}/mn\mathbb{Z} \not\cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if $(m,n) \neq 1$. □

② Let $S = \{(z,w) \in \mathbb{C} \times \mathbb{C} : |z|^2 + |w|^2 = 1\}$. For a positive integer m, let $\mathbb{Z}/m\mathbb{Z}$ act on the set S by $(a \bmod m)\cdot(z,w) = (e^{2\pi i a/m} z, e^{8\pi i a/m} w)$.

(a) Show this is a group action of $\mathbb{Z}/m\mathbb{Z}$ on S.

Pf: Let $a \bmod m$, $b \bmod m \in \mathbb{Z}/m\mathbb{Z}$ and let $(z,w) \in S$.

$(a \bmod m)\cdot[(b \bmod m)\cdot(z,w)] = (a \bmod m)\cdot(e^{2\pi i b/m} z, e^{8\pi i b/m} w)$
$= (e^{2\pi i a/m} e^{2\pi i b/m} z, e^{8\pi i a/m} e^{8\pi i b/m} w)$
$= (e^{2\pi i (a+b)/m} z, e^{8\pi i (a+b)/m} w)$

the gp. operation of $\mathbb{Z}/m\mathbb{Z}$ is addition ↓

$[(a \bmod m) + (b \bmod m)]\cdot(z,w) = (a+b \bmod m)\cdot(z,w)$
$= (e^{2\pi i (a+b)/m} z, e^{8\pi i (a+b)/m} w)$

$\Rightarrow$ so $(a \bmod m)[(b \bmod m)\cdot(z,w)] = [(a \bmod m) + (b \bmod m)]\cdot(z,w)$ $\forall a,b \in \mathbb{Z}/m\mathbb{Z}$, $(z,w) \in S$.

$(0 \bmod m)\cdot(z,w) = (e^{2\pi i 0/m} z, e^{8\pi i 0/m} w) = (z,w)$ $\forall (z,w) \in S$. □

(b) If m is odd, show every orbit in this group action has m elements.

Pf: The orbit of $x \in S$ is $\{gx : g \in \mathbb{Z}/m\mathbb{Z}\}$

Let $a \bmod m \in \mathbb{Z}/m\mathbb{Z}$, m odd, and $(z,w) \in S$

Then $(a \bmod m)(z,w) = (e^{2\pi i a/m} z, e^{8\pi i a/m} w)$ $\forall a \in \mathbb{Z}/m\mathbb{Z}$

Since m is odd, $(2,m) = 1$, so a has m distinct options $\{0,1,\dots,m-1\}$

Therefore, the order of every orbit in this gp. action is m, i.e., every orbit in this gp. action has m elements since (z,w) was chosen arbitrarily. □

(c) If m is even, show the orbit of some point in S has less than m elements.

Pf: Let $m = 2k$ for $k \in \mathbb{Z}$, $k < m$.

Let $a \in \mathbb{Z}/m\mathbb{Z}$, $(z,w) \in S$. Then

$(a \bmod m)\cdot(z,w) = (e^{2\pi i a/m} z, e^{8\pi i a/m} w)$
$= (e^{2\pi i a/2k} z, e^{8\pi i a/2k} w)$
$= (e^{\pi i a/k} z, e^{4\pi i a/k} w)$

Now a has k distinct options $\{0,1,\dots,k-1\}$, $k < m$

Therefore, the orbit of some point $(z,w) \in S$ has less than m elts.

→ a still has m options, but some of them will produce the same angle, so a really has $<m$ options. □

③ Use Zorn's lemma to show every nontrivial finitely generated group contains a maximal subgroup. (A maximal subgroup is a proper subgroup contained in no other proper subgroup.) Do not assume this group is abelian.

Pf: [If H is a proper subgp. of G, then there is a maximal proper subgp. M of G s.t. $H \subset M \subset G$.

Let G = nontrivial fin. gen. gp.

Let $S = \{$proper subgps. of $G\}$

$S \neq \emptyset$: $\{e\} \subset G$ (since $G \neq 0$)

Partially order S by containment

If $\{H_\alpha\}$ is totally ordered subset of S, then it has an upper bound in S:

$H = \bigcup_\alpha H_\alpha$

H is a subgp.: $x,y \in H \Rightarrow x \in H_\alpha$, $y \in H_\beta$

Tot. ordering $\Rightarrow H_\alpha \subset H_\beta$ or $H_\beta \subset H_\alpha$
$\Rightarrow xy^{-1} \in H_\beta \subset H$ or $x^{-1}y \in H_\alpha \subset H$

H is a proper subgp: $H_\alpha \subset H \subset S$ and all subgps. in S are proper subgps. of G. So by Zorn's lemma, S has a maximal subgp. M.

That means
- M is a proper ideal of G
- $M \subset H \subset G$, $H \neq G \Rightarrow H = M$ (subgp.)

So M is a maximal subgp.

Therefore, every nontrivial fin. gen. group G contains a maximal subgp. □

④ (a) Let a be any complex number. Prove that the map $\phi : \mathbb{R}[x] \to \mathbb{C}$ defined by $\phi(f(x)) = f(a)$ is a homomorphism of rings.

Pf: First we will show that $\phi(f(x)+g(x)) = \phi(f(x)) + \phi(g(x))$:

Let $f(x), g(x) \in \mathbb{R}[x]$. Then

$\phi(f(x)+g(x)) = f(a)+g(a) = \phi(f(x)) + \phi(g(x))$ ✓

Now we will show that $\phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$:

$\phi(f(x)g(x)) = f(a)g(a) = \phi(f(x))\phi(g(x))$ ✓

Lastly, $\varphi(1) = 1$. ✓

Therefore, ϕ is a homomorphism of rings. □

(b) Prove that $\mathbb{R}[x]/(x^2+1)$ is a field which is isomorphic to $\mathbb{C}$.

Pf: $(x^2+1) = (x+i)(x-i)$

Let $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ by $\varphi(f(x)) = f(i)$.

By part (a), this is a ring homomorphism.

We want to show that $\ker(\varphi) = (x^2+1)$.

- Let $g(x) \in (x^2+1)$.
  Then $g(i) = (i^2+1) = 0$, so $g(x) \in \ker(\varphi)$.
  Therefore, $(x^2+1) \subseteq \ker(\varphi)$.
- Let $g(x) \in \ker(\varphi)$.
  Then $g(i) = 0 \Rightarrow (x-i) | g(x)$ and
  $g(-i) = 0 \Rightarrow (x+i) | g(x)$.
  Therefore, $(x-i)(x+i) = (x^2+1) | g(x) \Rightarrow g(x) \in (x^2+1)$.

Thus, $\ker(\varphi) \subseteq (x^2+1)$.

We conclude that $\ker(\varphi) = (x^2+1)$.

The evaluation map $g(x) \mapsto g(i)$ is onto: $a+bi \in \mathbb{C}$ is the image of $a+bx \in \mathbb{R}[x]$.

Therefore, by the first isom. thm., we have that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$. □

⑤ (a) Let R be a commutative ring with identity and I be an ideal in R. Show that R/I is a field if and only if I is a maximal ideal.

Pf:
- Suppose that R/I is a field and $I \subset J \subset R$ where J is an ideal.
  We WTS $J = I$ or $J = R$ (defn. of a max. ideal).
  Assume $J \neq I$.
  Let $j \in J - I$, so in R/I we have $j \not\equiv 0 \bmod I$.
  Since R/I is a field, there is a $k \in R$ s.t. $jk \equiv 1 \bmod I$, so $jk = 1 + x$ for some $x \in I$.
  Thus, $1 = jk - x$.
  Since $j \in J$, we have that $jk \in J$, and since $x \in I \subset J$, we have that $1 = jk - x \in J$. (so $1 \in J$)
  Therefore, J contains 1, so $J = R$.
  Thus, I is a maximal ideal.
- Suppose that I is a maximal ideal.
  Then I is a proper ideal of R s.t. the only ideals J satisfying $I \subset J \subset R$ are $J = I$ or $J = R$.
  Let $a \neq 0$, $a \in R/I$.
  We WTS a has an inverse.
  Consider the sum $I + Ra = \{x + ra : x \in I, r \in R\}$.
  This is an ideal in R: $\forall r \in R$ and $x + ra \in I + Ra$, we have $r(x+ra) = rx + r^2a \in I + Ra$ $(rx \in I, r^2a \in Ra)$.
  The ideal $I + Ra$ contains I (use $r=0$) and it contains a (use $x=0$ and $r=1$), so the ideal $I+Ra$ is larger than I.
  Therefore, $I + Ra = R$ since I is a maximal ideal.
  That implies $1 = x + ra$ for some $x \in I$ and $r \in R$, so $ra \equiv 1 \bmod I$, and thus $a \bmod I$ has an inverse.
  Therefore, R/I is a field. □

(b) Let R be a PID and P be a nonzero prime ideal in R. Show that P is a maximal ideal.

Pf: Since R is a PID, the prime ideal P is principal, i.e., $P = (p) \subset R$.

Let $I = (a)$ be an ideal s.t. $P \subset I \subset R$, so $(p) \subset (a) \subset R$.

$(p) \subset (a) \Rightarrow a|p$, so $\exists b \in R$ s.t. $p = ab$.

Since P is prime, $a \in P$ or $b \in P$.

If $a \in P$, then $(a) \subset (p) \Rightarrow I = P$

If $b \in P$, then $\exists c \in R$ s.t. $b = pc$.

Then $p = ab = apc \Rightarrow p = pac$
$\Rightarrow 1 = ac$
$\Rightarrow a$ is invertible.
Thus, $I = R$.

Therefore, for $P \subset I \subset R$, we have $I = P$ or $I = R$.

Thus, we conclude that P is a maximal ideal. □

⑥ Give examples as requested, with brief justification.

(a) A nonabelian group which is not isomorphic to a semidirect product of nontrivial groups.

Pf: Q_8 (the quaternions) is a nonabelian gp. that is not isom. to a semidirect prod. of nontrivial gps.

Q_8 is not abelian b/c $ij = k$, but $ji = -k$ and $k = -k$, so $ij \neq ji$.

Suppose $Q_8 \cong G = N \rtimes H$ ($N \trianglelefteq G$, $H < G$, N & H are nontrivial).

- If $|N| = 4$, then $H = \{1, h\}$ where h is an elt. of order 2 in Q_8.
  Therefore, $h = -1$, which is the only elt. of order 2 in Q_8.
  But $-1 \in N$ since $i^2 = j^2 = k^2 = -1$.
  We get the contradiction that $N \cap H \neq \{1\}$.
- If $|N| = 2$, then $|H| = 4$ and $H \trianglelefteq G$.
  Noting $N = \{1, n\}$, we have $h^{-1}nh = n$ for $h \in H$.
  Therefore, $nh = hn$.
  This proves that $G = NH$.
  Also N is abelian as a cyclic gp. of order 2.
  H is also cyclic since $|H| = 2^2$ and H is abelian.
  This would make G abelian. ↯ □

(b) A 2-Sylow subgroup of S_4.

Pf: (Needs work)

(c) A PID other than $\mathbb{Z}$.

Pf: $\mathbb{Q}$ is a field other than $\mathbb{Z}$.

The only ideals in $\mathbb{Q}$ are (0) and $(1) = \mathbb{Q}$.

Therefore, $\mathbb{Q}$ is a PID since all of its ideals are principals. □

(d) A unit other than ± 1 in $\mathbb{Z}[\sqrt{7}]$.

Pf: Let $x + y\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$.

$N(x+y\sqrt{7}) = (x+y\sqrt{7})(x-y\sqrt{7}) = x^2 - 7y^2$

$x^2 - 7y^2 = \pm 1 \Rightarrow x^2 - 7y^2 = 1 \Rightarrow x^2 = 1 + 7y^2$

Let $x = 8$, $y = 3$.

Then $N(8 + 3\sqrt{7}) = 1$

Therefore, $8 + 3\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$ is a unit other than ± 1. □