August 2018

martes, 27 de diciembre de 2022 2:08 p.m.

① (a) In a finite abelian group, prove the order of each element divides the maximal order of all elements. (You may use the classification of finite abelian groups.)

Pf: Let G be a finite abelian group s.t. $|G| = n_1 n_2 \cdot \ldots \cdot n_k$.
Using the classification of finite abelian gps, we can write G as $\mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_k)$.
The order of an element $(a_1, a_2, \ldots, a_k)$ in G is $\operatorname{lcm}(|a_1|, |a_2|, \ldots, |a_k|)$.
Observe that $|(1,1,\ldots,1)| = \operatorname{lcm}(|1|, |1|, \ldots, |1|) = \operatorname{lcm}(n_1, n_2, \ldots, n_k) = n$
Note that $n \cdot (a_1, a_2, \ldots, a_k) = (\underset{\downarrow\, n_1|n}{na_1}, \underset{\downarrow\, n_2|n}{na_2}, \ldots, \underset{\downarrow\, n_k|n}{na_k}) = (0, 0, \ldots, 0)$ because n is the maximal order of all elements.
For any $(a_1, a_2, \ldots, a_k) \in G$, $n \cdot (a_1, a_2, \ldots, a_k) = 0$.
So $|(a_1, a_2, \ldots, a_k)| \leq n$ and $|(a_1, a_2, \ldots, a_k)| \mid n$.
Therefore, the order of each elt. divides the maximal order of all elts. □

(b) In a field F, use part (a) to prove every finite subgroup of $F^\times = F - \{0\}$ is cyclic.

Pf: Let G be a finite subgroup of $F^\times$, with $|G| = n$.
From part (a), if m is the maximal order of an element in G, then $|x| \mid m$ $\forall x \in G$. So $x^m = 1$ $\forall x \in G$.
$x^m = 1$ is a polynomial of degree m with (at least) n solutions in a field, so $n \leq m$.
We know $\exists y \in G$ with $|y| = m$, $m \mid n$, so $m \leq n$.
Therefore, $m = n$.
G has an element of order $n = |G|$, so G is cyclic. □

② Let R be a commutative ring w/ identity and $R[x]$ be the polynomial ring over R.

(a) Prove the ideal (x) in $R[x]$ is a prime ideal if and only if R is an integral domain.

Pf: • Let (x) be a prime ideal in $R[x]$. So if $a, b \in R$ and $ab \in (x)$, then either $a \in (x)$ or $b \in (x)$.
We know that $R[x]/(x) \cong R$.
If $\bar{a}, \bar{b} \in R[x]/(x) \cong R$, then $\overline{ab} \equiv 0 \bmod (x)$ means that $ab \in (x)$ b/c (x) is prime, so at least one of a, b is in (x), so $\bar{a} \equiv 0 \bmod (x)$ or $\bar{b} \equiv 0 \bmod (x)$. This is the definition of an integral domain (if $ab = 0$ in R, then $a = 0$ or $b = 0$ in R.).
Therefore, R is an integral domain.

• Let R be an integral domain. Then if $a, b \in R$ and $ab = 0$, then $a = 0$ or $b = 0$.
R is an integral domain $\Rightarrow$ $R[x]$ is an integral domain.
Consider the ideal (x).
Suppose $ab \in (x)$. Then $\overline{ab} \equiv 0 \bmod (x)$, so $\bar{a} \equiv 0 \bmod (x)$ or $\bar{b} \equiv 0 \bmod (x)$ since $R[x]$ is an integral domain (i.e., $a \in (x)$ or $b \in (x)$).
Therefore, (x) is a prime ideal in $R[x]$. □

(b) Let I be an ideal of R. Prove that the following set is an ideal in $R[x]$:
$I[x] := \{f(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x] : a_0, a_1, \ldots, a_n \in I\}$.

Pf: First we will show that $I[x]$ is a subring of $R[x]$.
Note that $I[x]$ is nonempty since $0 \in I[x]$ and $I \subset I[x]$.
Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in I[x]$ and
$g(x) = b_0 + b_1 x + \ldots + b_n x^n \in I[x]$.
Then $f(x) - g(x) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_n - b_n)x^n \in I[x]$ b/c $a_i, b_i \in I$ and I is an ideal.
Then $f(x)g(x) \in I[x]$ b/c $a_i b_j$ for $0 \leq i, j \leq n$ is in I since I is an ideal.
Therefore, $I[x]$ is a subring of $R[x]$.
Now to show $I[x]$ is an ideal, we will show that for any $r(x) \in R[x]$ and $f(x) \in I[x]$, that $r(x)f(x) \in I[x]$.
Let $r(x) = r_0 + r_1 x + \ldots + r_m x^m \in R[x]$.
Then $r(x)f(x) = \sum_{j=0}^{n} \sum_{i=0}^{m} r_i a_j x^{i+j} \in I[x]$ since $r_i a_j \in I$ b/c I is an ideal. □

(c) Prove that an ideal I of R is a prime ideal if and only if the ideal $I[x]$ of $R[x]$ from part (b) is a prime ideal.

Pf: Observe that $R[x]/I[x] \cong (R/I)[x]$.
Let $\varphi: R[x] \longrightarrow (R/I)[x]$, so φ is the reduction on coeffs.
Since φ is a redn. map, we know it is a homomorphism and onto.
Observe that $\ker(\varphi) = \{f(x) \in R[x] : f(x) \equiv 0 \bmod I\} = I[x]$.
So by the first isom. thm., we have that $R[x]/I[x] \cong (R/I)[x]$.
If I is a prime ideal, then R/I is an integral domain, so $(R/I)[x]$ is an integral domain $\Rightarrow$ $R[x]/I[x]$ is an integral domain $\Rightarrow$ $I[x]$ is a prime ideal.
If $I[x]$ is a prime ideal, then $R[x]/I[x]$ is an integral domain, so $(R/I)[x]$ is an integral domain $\Rightarrow$ R/I is an integral domain $\Rightarrow$ I is a prime ideal. □

③ Let G be a group and H be a subgroup.

(a) Define the normalizer of H in G.

Pf: The normalizer of H in G is defined as follows:
$N_G(H) = \{g \in G : gHg^{-1} = H\}$. □

(b) Prove conjugate subgroups have conjugate normalizers: if N is the normalizer of H in G, then for each $g \in G$, gNg^{-1} is the normalizer of gHg^{-1} in G.

Pf: Let $N = N_G(H) = \{g \in G : gHg^{-1} = H\}$.
Let $K = gHg^{-1}$ be an arbitrary conjugate of H, and then compute the normalizer of K:

$$\begin{aligned} N_G(K) &= \{x \in G : xKx^{-1} = K\} \\ &= \{x \in G : xgHg^{-1}x^{-1} = gHg^{-1}\} \\ &= \{x \in G : g^{-1}xgHg^{-1}x^{-1}g = H\} \\ &= \{x \in G : g^{-1}xgH(g^{-1}xg)^{-1} = H\} \\ &= \{x \in G : g^{-1}xg \in N_G(H)\} \end{aligned}$$

$$\begin{aligned} N_G(N) &= \{x \in G : xNx^{-1} = N\} \\ &= \{x \in G : xN_G(H)x^{-1} = N_G(H)\} \\ &= \{x \in G : xgHg^{-1}x^{-1} = gHg^{-1}\} \\ &= \{x \in G : g^{-1}xgH(g^{-1}xg)^{-1} = H\} \\ &= \{x \in G : g^{-1}xg \in N_G(H)\}. \end{aligned}$$

Therefore, if N is the normalizer of H in G, then for each $g \in G$, gNg^{-1} is the normalizer of gHg^{-1} in G. □

(c) Let $G = GL_2(\mathbb{R})$ and $H = \left\{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x, y \in \mathbb{R}^\times\right\}$. Prove the normalizer of H in G is $\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : a, b, c, d \in \mathbb{R}^\times\right\}$.

Pf: Recall that $GL_2(\mathbb{R}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}^\times, ad - bc \neq 0\right\}$.
$N_G(H) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} H \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = H\right\}$.
Let $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in H$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$. Then we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} ax & by \\ cx & dy \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\frac{1}{ad-bc} = \begin{pmatrix} adx - bcy & -abx + aby \\ cdx - cdy & ady - cbx \end{pmatrix}\frac{1}{ad-bc}$$

$$= \begin{pmatrix} \frac{adx - bcy}{ad-bc} & ab(y-x) \\ cd(x-y) & \frac{ady - cbx}{ad-bc} \end{pmatrix} \in H \text{ if } \left.\begin{matrix} ab(y-x) = 0 \\ cd(x-y) = 0 \end{matrix}\right\}$$

Let $a = d = 0$ $(ad - bc \neq 0)$ or let $c = b = 0$ $(ad - bc \neq 0)$

(consider $x = 2, y = 1$, then the above holds.)

So we have $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ and $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ that normalize H.
Therefore, $N_G(H) = \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : a, b, c, d \in \mathbb{R}^\times\right\}$. □

④ The Fibonacci numbers $\{f_n\}$ are determined recursively for $n \geq 0$ by $f_0 = 0$, $f_1 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for all $n \geq 0$.

(a) Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. For all integers $n \geq 1$, show $A^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$.

Pf: Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix}$, $f_0 = 0$, $f_1 = 1$, $f_2 = 1$
Base case: $n = 2$: $A^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} f_3 & f_2 \\ f_2 & f_1 \end{pmatrix}$ $(f_3 = \underset{f_2}{1} + \underset{f_1}{1} = 2)$

Ind. hyp.: Suppose this holds for all $0 \leq k \leq n-1$, so $A^{n-1} = \begin{pmatrix} f_n & f_{n-1} \\ f_{n-1} & f_{n-2} \end{pmatrix}$. We WTS this holds for $k = n$.
Observe that

$$A^n = A^{n-1}A = \begin{pmatrix} f_n & f_{n-1} \\ f_{n-1} & f_{n-2} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_n + f_{n-1} & f_n \\ f_{n-1} + f_{n-2} & f_{n-1} \end{pmatrix} = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

Therefore, $A^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$. □

(b) Show the group $GL_2(\mathbb{Z}/p\mathbb{Z})$, for prime p, has order $(p^2-1)(p^2-p)$.

Pf: Consider the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z})$. Recall that $ad - bc \neq 0$.
For the first vector in the matrix $\begin{pmatrix} a \\ c \end{pmatrix}$, there are $p^2 - 1$ options b/c we cannot have $a = c = 0$, $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ or else $ad - bc = 0$.
For the second vector in the matrix $\begin{pmatrix} b \\ d \end{pmatrix}$, there are $p^2 - p$ options b/c we cannot have $\begin{pmatrix} b \\ d \end{pmatrix}$ be a scalar multiple of $\begin{pmatrix} a \\ c \end{pmatrix}$, and there are p different scalars.
Therefore, $GL_2(\mathbb{Z}/p\mathbb{Z})$ has order $(p^2-1)(p^2-p)$. □

(c) Use parts (a) and (b) to help you find, with proof, some integer $n \geq 1$ such that $f_n \equiv 0 \bmod 10$ while $f_{n+1} \equiv 1 \bmod 10$. (Hint: Use the prime factorization of 10.)

Pf: We know that $10 = 2 \cdot 5$.
We want to find n s.t. $A^n \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 10$
(by part (a), $f_{n+1} = f_n + f_{n-1} \Rightarrow f_{n-1} = f_{n+1} - f_n = 1 - 0 = 1$)
want: $A^n \bmod 2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $A^n \bmod 5 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow A^n \bmod 10 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\mathbb{Z}/10 \cong \mathbb{Z}/2 \times \mathbb{Z}/5$, $(2,5) = 1$ (CRT)
Using part (b), $|GL_2(\mathbb{Z}/2\mathbb{Z})| = (2^2-1)(2^2-2) = 3 \cdot 2 = 6$ and
$|GL_2(\mathbb{Z}/5\mathbb{Z})| = (5^2-1)(5^2-5) = 24 \cdot 20 = 480$.
$A^{6 \cdot 480} = A^{2880} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 10$.
Therefore, $n = 2880$. □

⑤ An abelian group A is called divisible if, for each $a \in A$ and $n \in \mathbb{Z}^+$, there is $a, b \in A$ (maybe not unique) such that $nb = a$. (Formally it says we can "divide" a by n, but the choice may not be unique so do not write $b = \frac{1}{n}a$.) For example, $(\mathbb{R}, +)$ is divisible. Also $(\mathbb{C}^\times, \times)$ is divisible since, for all $n \in \mathbb{Z}^+$, a number in $\mathbb{C}^\times$ has an n^{th} root in $\mathbb{C}^\times$ (not unique if $n > 1$).
Prove a nonzero divisible group can't be finitely generated.

See Keith's notes.

⑥ Give examples as requested, with justification.

(a) Two nonconjugate elements of S_4 that have the same order.

Pf: Two elements of S_n are conjugate if and only if they have the same cycle type.
Consider (12) and $(12)(34)$ in S_4.
The two elements have diff. cycle types, so they are not conjugate.
The order of an element in S_n is the lcm of the cycle lengths, so the order of (12) is 2 and the order of $(12)(34)$ is $\operatorname{lcm}(2,2) = 2$.
Therefore, (12) and $(12)(34)$ are two nonconjugate elts. of S_4 that have the same order. □

(b) Two commutative rings that are not isomorphic as rings, but are isomorphic as additive groups.

Pf: Consider the commutative rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$.
These two rings are not isomorphic as rings:
Suppose $\varphi: \mathbb{Z}[i] \longrightarrow \mathbb{Z}[\sqrt{2}]$
Let $\varphi(i) = x + y\sqrt{2}$.
Observe that $-1 = \varphi(i^2) = (x + y\sqrt{2})^2 = x^2 + 2xy\sqrt{2} + 2y^2$
$\Rightarrow -1 = (x^2 + 2y^2) + \underbrace{2xy\sqrt{2}}_{x=0 \text{ or } y=0}$: if $x = 0 \Rightarrow -1 = 2y^2 \Rightarrow$ no $\mathbb{Z}$-soln; if $y = 0 \Rightarrow -1 = x^2 \Rightarrow$ no $\mathbb{Z}$-soln
Therefore, $\mathbb{Z}[i] \ncong \mathbb{Z}[\sqrt{2}]$ as rings.
These two are isomorphic as additive groups:
Let $\varphi: \mathbb{Z}[i] \to \mathbb{Z}[\sqrt{2}]$ by $a + bi \mapsto a + b\sqrt{2}$
φ is a hom: $\varphi((a+bi) + (c+di)) = \varphi((a+c) + (b+d)i) = (a+c) + (b+d)\sqrt{2}$
$= a + b\sqrt{2} + c + d\sqrt{2} = \varphi(a+bi) + \varphi(c+di)$.
φ is onto: for all $a, b \in \mathbb{Z}$, $a + bi \mapsto a + b\sqrt{2}$
φ is 1-1: $\ker(\varphi) = \{\varphi(\alpha) \in \mathbb{Z}[i] : \varphi(\alpha) = 0\}$
Let $\alpha = a + bi$. $\varphi(\alpha) = \varphi(a + bi) = a + b\sqrt{2} = 0 \Rightarrow a = b = 0$.
Therefore, the $\ker(\varphi)$ is trivial.
By the first isom. thm., $\mathbb{Z}[i] \cong \mathbb{Z}[\sqrt{2}]$.
Therefore, $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$ are two comm. rings that are not isomorphic as rings, but are isom. as additive groups. □

(c) A formula for a ring isomorphism $\mathbb{R}[x]/(x^2-1) \to \mathbb{R} \times \mathbb{R}$.

Pf: Observe that $x^2 - 1 = (x+1)(x-1)$, and $(x+1) + (x-1) = \mathbb{R}[x]$.
By the CRT, $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R}[x]/(x+1) \times \mathbb{R}[x]/(x-1) \cong \mathbb{R} \times \mathbb{R}$ by eval. @ $x = 1, x = -1$
Let $\varphi: \mathbb{R}[x] \longrightarrow \mathbb{R} \times \mathbb{R}$ by $f(x) \longmapsto (f(1), f(-1))$.
The evaluation map is a homomorphism and it is onto, so it remains to show that φ is 1-1.
We WTS $\ker(\varphi) = (x^2 - 1)$:
• Let $f(x) \in (x^2-1)$ s.t. $f(x) = (x^2-1)g(x)$, $g(x) \in \mathbb{R}[x]$.
Then $\varphi(f(x)) = (f(1), f(-1)) = ((1^2-1)g(1), ((-1)^2-1)g(-1)) = (0, 0)$.
So $(x^2-1) \subseteq \ker(\varphi)$.
• Let $f(x) \in \ker(\varphi)$. Then by the division algorithm in $\mathbb{R}[x]$, we have $q(x), r(x) \in \mathbb{R}[x]$ s.t. $f(x) = (x^2-1)q(x) + r(x)$ where $\deg(r) = 0$ or 1.
Since $f(x) \in \ker(\varphi)$,

$$\begin{aligned} 0 &= \varphi(f(x)) \\ &= \varphi(q(x))\underbrace{\varphi((x^2-1))}_{=0} + \varphi(r(x)) \\ &= \varphi(r(x)) \\ &= (r(1), r(-1)) \end{aligned}$$

So ± 1 are roots of $r(x)$ in $\mathbb{R}[x]$, which means that $r(x) = (x+1)(x-1)r_1(x) \Rightarrow \deg(r) \geq 2$ ↯
Therefore, $r(x) = 0 \Rightarrow f(x) = (x^2-1)q(x)$
$\Rightarrow f(x) \in (x^2-1)$.
Thus, $\ker(\varphi) \subseteq (x^2-1)$.
Therefore, $\ker(\varphi) = (x^2-1)$.
By the first isom. thm., $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R} \times \mathbb{R}$. □