January 2016

martes, 25 de julio de 2023 8:12 p.m.

① Let $F$ be a field. Prove that $F[x]$ is a Euclidean domain.

Pf: We want to show that if $f, g \in F[x]$ with $g \neq 0$, then there are unique $q, r \in F[x]$ s.t.

① $f = qg + r$ and ② $r = 0$ or $\deg(r) < \deg(g)$.

· First we will show uniqueness of $q$ and $r$ in $F[x]$:

Suppose $f = gq_1 + r_1 = gq_2 + r_2$ with $q_i, r_i \in F[x]$, $\deg(r_i) < \deg(g)$, $i = 1,2$

Then $gq_1 + r_1 - (gq_2 + r_2) = 0 \Rightarrow g(q_1 - q_2) + (r_1 - r_2) = 0$

$$\underbrace{g(q_1 - q_2)} = \underbrace{r_2 - r_1}$$

If $q_1 \neq q_2$, then $q_1 - q_2 \neq 0$, then

If $r_2 \neq r_1$, then $r_2 - r_1 \neq 0$, then $\deg(r_2 - r_1) < \deg(g)$

$$\deg(g(q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2) \geq \deg(g)$$

So from $g(q_1 - q_2) = r_2 - r_1$, we get that the LHS $\geq \deg(g)$ and the RHS $< \deg(g)$. ↯

So $q_1 = q_2$, which gives us $g(q_1 - q_2) = 0 = r_2 - r_1 \Rightarrow r_1 = r_2$

Therefore, $q, r \in F[x]$ are unique.

· Now we will show existence of $q, r \in F[x]$:

Given $f, g \in F[x]$ with $g \neq 0$

If $f = 0$ or $\deg(f) < \deg(g)$, then $f = g \cdot 0 + f$, so $q = 0$, $r = f$.

Now suppose $\deg(f) \geq \deg(g)$.

We will induct on $\deg(f) = m$: the cases $0 \leq m \leq \deg(g) - 1$ are done.

When $m \geq \deg(g)$, write out

$$f = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0 \quad \text{and}$$

$$g = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0, \quad m \geq n, \ a_m, b_n \neq 0$$

Consider $f(x) = \frac{a_m}{b_n} x^{m-n} g(x)$, where we can use $\frac{a_m}{b_n} \cdot b_n = a_m$ b/c $F$ = field.

$$\Rightarrow f(x) - \frac{a_m}{b_n} x^{m-n} g(x) = (a_m x^m + a_{m-1} x^{m-1} + \dots +) - \frac{a_m}{b_n} x^{m-n} (b_n x^n + b_{n-1} x^{n-1} + \dots)$$

$$= (a_m x^m + a_{m-1} x^{m-1} + \dots) - a_m x^m - \frac{a_m b_{n-1}}{b_n} x^{m-1} - \dots$$

So the degree $m$ terms cancel out, and this poly. either has deg 0 or degree $< m$. If $f(x) - \frac{a_m}{b_n} x^{m-n} g(x) = 0$, then $f(x) = \frac{a_m}{b_n} x^{m-n} g(x) + 0$, so $q = \frac{a_m}{b_n} x^{m-n}$ and $r = 0$.

If $\tilde{f} = f - \frac{a_m}{b_n} x^{m-n} g \neq 0$, then since $\deg(\tilde{f}) < m$, by induction we know $\exists\, Q, R \in F[x]$ s.t. $\tilde{f} = gQ + R$, $R = 0$ or $\deg(R) < \deg(g)$.

$$\Rightarrow \tilde{f} = f = \frac{a_m}{b_n} x^{m-n} g + gQ + R = g\underbrace{\left(\frac{a_m}{b_n} x^{m-n} + Q\right)}_{q} + \underbrace{R}_{r}. \quad \square$$

③ Let $D_{2n}$ be the dihedral group of order $2n$, with $n \geq 3$.

(a) Let $p$ be an odd prime and let $H$ be a Sylow $p$-subgroup of $D_{2n}$. Prove that $H$ is a normal subgroup and cyclic.

Pf: Let $2n = p^k m$ for some prime $p$ and $m \in \mathbb{Z}$ s.t. $p \nmid m$, so $p^k \mid 2n$

$\Rightarrow p \mid n$ b/c $p$ is odd.

Let $|H| = p^k$ since $H$ is a Sylow $p$-subgp. of $D_{2n}$.

We want to show that $H$ contains no reflections.

A reflection $s$ has order 2 since $s^2 = 1$ and a reflection $r^k s$ also has order 2 since $(r^k s)^2 = r^k s r^k s = r^k s s r^{-k} = r^k s^2 r^{-k} = r^k r^{-k} = 1$.

But $|H| = p^k$, $p$ odd prime, so $H$ has no elements of order 2.

Now we want to show that any subgp. containing only rotations is normal.

Let $H$ be a subgp. only containing rotations, so $H = \langle r^d \rangle$, $d \in \mathbb{Z}$.

Let $r^k s \in D_{2n}$, then $r^k s r^d (r^k s)^{-1} = r^k s r^d s r^{-k} = r^{k-d} s^2 r^{-k} = r^{-d} \in H$,

and for $r^k \in D_{2n}$, then $r^k r^d r^{-k} = r^{k+d-k} = r^d \in H$

Therefore, $H$ is normal.

Since $H$ only contains rotations, we know that $H$ is cyclic b/c the set of rotations is $\{1, r, r^2, \dots, r^{n-1}\} = \langle r \rangle$, is cyclic.

Since $H$ is a subgp. of a cyclic gp., it is cyclic. $\square$

(b) Writing $2n = 2^e \cdot m$ with $m$ odd and $e \geq 1$, prove that the number of Sylow 2-subgroups of $D_{2n}$ is $m$.

Pf: By the first Sylow thm, we know there exists a Sylow 2-subgp. $P$ s.t. $|P| = 2^e$, for $e \geq 1$.

· If $N \trianglelefteq G$ and $P$ is a $p$-Sylow subgp. of $G$, then $P \cap N$ is a $p$-Sylow subgp. of $N$.

(Needs work)

④ Find (with proof) a product of cyclic groups that is isomorphic to the group $(\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z})/\langle (2,6) \rangle$.

Pf: By Lagrange's theorem, we have that

$$|(\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z})/\langle (2,6) \rangle| = \frac{12 \cdot 12}{6} = 24.$$

$|\langle (2,6) \rangle| = 6$ because:
order of 2 in 12 is 6
order of 6 in 12 is 2
$\Rightarrow |\langle (2,6) \rangle| = \mathrm{lcm}(2,6) = 6$

We can think of this group as

$H = (\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z})/(2n, 6n)$.

The prime factorization of $24 = 2^3 \cdot 3$.

By the fund. thm. of fin. gen. abelian gps., we know that a group of order 24 is isomorphic to

$$\underset{*}{\mathbb{Z}/24\mathbb{Z}}, \quad \underset{**}{\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}, \quad \underset{***}{\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$$

$|(a,b)| = \mathrm{lcm}(|a|, |b|)$

In the original gp. there is no elt. of order 24, so can't be *

The only possible order of elts. is factors of 12.

** has an elt. of order 12, but *** does not.

$\langle (2,6) \rangle = \{(2,6), (4,0), (6,6), (8,0), (10,6), (0,0)\}$

want $(a,b)$ s.t. $|(a,b)| = 12$ in $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

We don't want $n(a,b) \in \langle (2,6) \rangle$ unless $n = 12$

nonex: $(1,0)$ b/c $4(1,0) = (4,0) \in \langle (2,6) \rangle$

$|(1,0)| = 12$ in $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and it still has order 12 in $H$

$\Rightarrow \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\square$

⑤ For each integer $d$ that's not a perfect square, let $R_d$ be the set of all 2-by-2 matrices of the form $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$ with $a, b \in \mathbb{Z}$. Show that $R_d$ is a subring of the ring of integral 2-by-2 matrices $M_2(\mathbb{Z})$ and that $R_d$ is isomorphic to the ring $\mathbb{Z}[\sqrt{d}]$.

Pf: First we will show that $R_d$ is a subring of $M_2(\mathbb{Z})$:

Let $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \begin{pmatrix} c & ed \\ e & c \end{pmatrix} \in R_d$, so $a, b, c, d, e \in \mathbb{Z}$

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix} + \begin{pmatrix} c & ed \\ e & c \end{pmatrix} = \begin{pmatrix} a+c & bd+ed \\ b+e & a+c \end{pmatrix} = \begin{pmatrix} a+c & (b+e)d \\ b+e & a+c \end{pmatrix} \in R_d$$

b/c $\mathbb{Z} + \mathbb{Z} = \mathbb{Z}$
$a + c \in \mathbb{Z}$
$b + e \in \mathbb{Z}$

So $R_d$ is closed under addition.

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix} \begin{pmatrix} c & ed \\ e & c \end{pmatrix} = \begin{pmatrix} ac+bde & aed+bcd \\ bc+ae & bde+ac \end{pmatrix} = \begin{pmatrix} ac+bed & (ae+bc)d \\ ae+bc & ac+bed \end{pmatrix} \in R_d$$

b/c $\mathbb{Z} \cdot \mathbb{Z} = \mathbb{Z}$
$ac + bed \in \mathbb{Z}$
$ae + bc \in \mathbb{Z}$

So $R_d$ is closed under multiplication.

Let $a = b = 0$, then $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R_d$ and let $a = 1, b = 0$, then $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R_d$

So $R_d$ contains the additive and multiplicative identities of $M_2(\mathbb{Z})$. (just need mult. id.)

Therefore, $R_d$ is a subring of $M_2(\mathbb{Z})$.

Now we will show that $R_d \cong \mathbb{Z}[\sqrt{d}]$.

Let $\varphi: \mathbb{Z}[\sqrt{d}] \to R_d$ s.t. $\varphi(a + b\sqrt{d}) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$

· $\varphi$ is a homomorphism: let $a + b\sqrt{d}, c + e\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Then

$$\varphi((a+b\sqrt{d}) + (c+e\sqrt{d})) = \varphi((a+c) + (b+e)\sqrt{d}) = \begin{pmatrix} a+c & (b+e)d \\ b+e & a+c \end{pmatrix} = \begin{pmatrix} a & bd \\ b & a \end{pmatrix} + \begin{pmatrix} c & ed \\ e & c \end{pmatrix}$$
$$= \varphi(a+b\sqrt{d}) + \varphi(c+e\sqrt{d})$$

and

$$\varphi((a+b\sqrt{d})(c+e\sqrt{d})) = \varphi((ac+bed) + (ae+bc)\sqrt{d}) = \begin{pmatrix} ac+bed & (ae+bc)d \\ ae+bc & ac+bed \end{pmatrix}$$
$$= \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \begin{pmatrix} c & ed \\ e & c \end{pmatrix} = \varphi(a+b\sqrt{d})\varphi(c+e\sqrt{d}).$$

· $\varphi$ is injective: Let $a_1 + b_1\sqrt{d} \neq a_2 + b_2\sqrt{d}$. Then

$$\varphi(a_1 + b_1\sqrt{d}) = \begin{pmatrix} a_1 & b_1 d \\ b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 d \\ b_2 & a_2 \end{pmatrix} = \varphi(a_2 + b_2\sqrt{d}) \Rightarrow a_1 = a_2, \ b_1 = b_2$$

so $\varphi(a_1 + b_1\sqrt{d}) \neq \varphi(a_2 + b_2\sqrt{d})$

Therefore, $\varphi$ is injective.

· $\varphi$ is surjective: Let $\begin{pmatrix} a & bd \\ b & a \end{pmatrix} \in R_d$. Take $a + b\sqrt{d} \in R_d$. Then $\varphi(a + b\sqrt{d}) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$. Therefore, $\varphi$ is surjective.

Therefore, $\varphi$ is an inj., surj., hom. $\Rightarrow \varphi$ is an isom.

Thus, $R_d \cong \mathbb{Z}[\sqrt{d}]$. $\square$

⑥ Give examples as requested, with brief justification.

(b) A commutative ring $R$ and an element $a \neq 0$ or $1$ such that $a^2 = a$.

Pf: Let $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Then $(1,0)^2 = (1,0)(1,0) = (1,0) \neq 0$ or $1$

$(0,0)^2 = (0,0)$

$(1,1)^2 = (1,1)$

$(0,1)^2 = (0,1)$

So $R$ is a comm. ring and $(1,0)$ is an element $\neq 0, 1$ s.t. $(1,0)^2 = (1,0)$. $\square$

(c) A non-trivial group with trivial center, $Z(G) = \{e\}$.

Pf: Consider the nontrivial gp. $D_3 = \{1, r, r^2, s, rs, r^2 s\}$

$Z(D_n) = \{z \in D_n : \forall g \in D_n, zg = gz\}$

We know that $r^k s = s r^{-k}$, so this only commutes if $r^k = r^{-k}$, which is not the case. $(s, r, r^2 \notin Z(D_3))$

Show $rs, r^2 s \notin Z(D_3)$: $rs(r^2 s)(rs)^{-1} = rsr^2 ssr^{-1} = rsr = s$

Therefore, $Z(D_3) = \{e\}$. $\square$

(d) A nonabelian group of order 12 constructed by an explicit semidirect product.

Pf: Consider the semidirect product $\mathbb{Z}/(3) \rtimes \mathbb{Z}/(4)$

$\varphi: \mathbb{Z}/(4) \to \mathrm{Aut}(\mathbb{Z}/(3)) = (\mathbb{Z}/(3))^\times$ by $k \bmod 4 \mapsto (-1)^k \bmod 3$

We use the group law $(a,b)(c,d) = (a + (-1)^b c, b + d)$.

This can only be abelian if $\varphi$ is trivial ($\varphi(k) = \mathrm{id}.\ \forall k$).

Since $\varphi$ is nontrivial, $\mathbb{Z}/(3) \rtimes_\varphi \mathbb{Z}/(4)$ is nonabelian. $\square$