January 2019

sábado, 24 de diciembre de 2022 2:53 p.m.

① (a) For $n\geq 3$, determine with proof the conjugacy classes of the dihedral group of order $2n$. (Hint: separately consider even n and odd n.)

Pf: Every element of D_n is r^i or r^is for some $i\in\mathbb{Z}$.
In order to find the conjugacy classes of D_n, we want to compute r^igr^{-i} and $r^isg(r^is)^{-1}=r^isgsr^{-i}$ $\forall g\in D_n$.
Let $r^j\in D_n$, $j\in\mathbb{Z}$. Then $r^ir^jr^{-i}=r^j$ and $r^isr^jsr^{-i}=r^{-j}$.
So for $i\in\mathbb{Z}$, the only conjugates of r^j in D_n are r^j and r^{-j}.
For s, we have $r^isr^{-i}=r^{2i}s$ and $r^isssr^{-i}=r^isr^{-i}=r^{2i}s$.
So for $i\in\mathbb{Z}$, the only conjugates of s in D_n are the reflections $r^{2i}s$ with an even exponent.
If n is odd, then every integer mod n is a multiple of 2.
So when n is odd, s is conjugate to every reflection $\{r^ks : k\in\mathbb{Z}\}$.
If n is even, then we only get half of the reflections as conjugates of s.
The other half are conjugate to rs:
$r^i(rs)r^{-i}=r^{2i+1}s$ and $(r^is)(rs)(sr^{-i})=r^{2i-1}s$.
As i varies, this gives us $\{rs, r^3s,\dots,r^{n-1}s\}$.
So if n is odd, then the conjugacy classes are $\{1\}$, $\{r^{\pm i}\}$, $\{r^is\}$ for $0\leq i\leq n-1$.
If n is even, then the conjugacy classes are $\{1\}$, $\{r^{n/2}\}$, $\{r^is\}$, $\{r^{2i}s\}$, $\{r^{2i+1}s\}$ for $0\leq i\leq \frac{n}{2}-1$. □

(b) Let c_n be the number of conjugacy classes in the dihedral group of order $2n$. Compute $\lim\limits_{n\to\infty}\frac{c_n}{n}$.

Pf: When n is odd, $c_n=1+n+n=2n+1$.
So $\lim\limits_{n\to\infty}\frac{2n+1}{n}=2$.

When n is even, $c_n=1+1+\frac{n}{2}+\frac{n}{2}+\frac{n}{2}=2+n+\frac{n}{2}$.
So $\lim\limits_{n\to\infty}\frac{2+n+n/2}{n}=\lim\limits_{n\to\infty}\frac{4+2n+n}{2n}=\lim\limits_{n\to\infty}\frac{4+3n}{2n}=\frac{3}{2}$. □

---

② Let p be the smallest prime dividing the order of a finite group G. Prove that if H is a subgroup of G with index p, then H is a normal subgroup. (Hint: Look at the left multiplication action of G on the left cosets of H.)

Pf: Suppose $H\leq G$ and $[G:H]=p$.
Let π_H be the permutation representation afforded by multiplication on the set of left cosets of H in G.
Let $K=\ker(\pi_H)$ and let $[H:K]=k$.
Then $[G:K]=[G:H][H:K]=pk$.
Since H has p left cosets, G/K is isomorphic to a subgp. of S_p (namely, the image of G under π_H) by the first isom. thm.
By Lagrange's thm, $pk=|G/K|$ divides $p!$.
Thus, $k\mid\frac{p!}{p}=(p-1)!$. But all prime divisors of $(p-1)!$ are less than p and by the minimality of p, every prime divisor of k is greater than or equal to p. This forces $k=1$. So $H=K\trianglelefteq G$.
↳ $[H:K]=1$ □

---

③ View $\mathbb{Q}$ and $\mathbb{Z}$ as additive groups. For $a\in\mathbb{Z}$, set $\varphi_a:\mathbb{Q}\to\mathbb{Q}$ by $\varphi_a(t)=2^at$.

(a) Show that φ_a is an automorphism of (the additive group) $\mathbb{Q}$ for each $a\in\mathbb{Z}$ and show $\varphi:\mathbb{Z}\to\mathrm{Aut}(\mathbb{Q})$ given by $a\mapsto\varphi_a$ is a homomorphism of gps.

Pf: First we will show that φ_a is an aut. of $\mathbb{Q}$ for each $a\in\mathbb{Z}$:
Let $x,y\in\mathbb{Q}$, then $\varphi_a(x+y)=2^a(x+y)=2^ax+2^ay=\varphi_a(x)+\varphi_a(y)$
Therefore, φ_a is a homomorphism.
φ is onto: Let $y\in\mathbb{Q}$, then $\varphi_a(x)=2^ax=y\Rightarrow x=\frac{y}{2^a}\in\mathbb{Q}$.

φ is 1-1: Let $x\neq y$, then $\varphi_a(x)=2^ax\neq\varphi_a(y)=2^ay$
$2^ax=2^ay$
$2^{-a}2^ax=y\Rightarrow x=y$ ↯
Therefore, φ_a is a bijective hom.. Thus, φ_a is an automorphism.
Now we will show that φ is a hom. of gps. We WTS
$\varphi(a+b)=\varphi(a)+\varphi(b)\Rightarrow\varphi_{a+b}=\varphi_a\circ\varphi_b$:
$\varphi_{a+b}(x)=2^{a+b}x=2^a2^bx=2^a\varphi_b(x)=\varphi_a(\varphi_b(x))=(\varphi_a\circ\varphi_b)(x)$.
Therefore, φ is a homomorphism of groups. □

(b) Set $G=\mathbb{Q}\rtimes_\varphi\mathbb{Z}$, a semidirect product. In G, let $H=\{(m,0): m\in\mathbb{Z}\}$ and $x=(0,1)$. Prove that $xHx^{-1}\subset H$.

Pf: Let $(m,0)\in H$. Note that $(0,1)^{-1}=(0,-1)$ b/c $(0,1)(0,-1)=(0,0)$.
We have that $x(m,0)x^{-1}$ is
$(0,1)(m,0)(0,1)^{-1}=(0+\varphi_1(m),1+0)(0,-1)=(2^1m,1)(0,-1)$
$=(2m+\varphi_1(0),1+(-1))=(2m+2^1\cdot0,0)=(2m,0)\in H$.
Therefore, $xHx^{-1}\subset H$. □

(c) Show that $x=(0,1)$ is not an element of the normalizer $N_G(H)$ of H in G.

Pf: $N_G(H)=\{y\in G: yHy^{-1}=H\}$.
We WTS that for $x=(0,1)$, $xHx^{-1}\not\supset H$.
From part (b), xHx^{-1} is always going to be of the form $(2k,0)$ for $k\in\mathbb{Z}$.
Consider $(1,0)\in H$. $(1,0)\notin xHx^{-1}$.
Therefore, $x=(0,1)$ is not an element of $N_G(H)$. □

---

④ (a) Define a Euclidean domain and prove all ideals in a Euclidean domain are principal.

Pf: An integral domain R is a Euclidean domain if there exists a Euclidean function $N: R-\{0\}\to\mathbb{N}$ s.t. for $a,b\in R$ there exists $q,r\in R$ s.t. $a=bq+r$ and $r=0$ or $N(r)<N(b)$.

Now we are going to prove that all ideals in a Euclidean domain R are principal. Let I be an ideal of R. If $I=(0)$, then I is principal. Let $I\neq(0)$. Let $m\in I$ be the element w/ least possible norm in I (so $N(m)=\min\limits_{\substack{a\neq0\\a\in I}}N(a)$). For any $a\in I$, we can write $a=mq+r$ w/ $r=0$ or $N(r)<N(m)$ since R is a Euclidean domain.

Then $a-mq=r\in I\Rightarrow r=0$ b/c of the minimality of the norm of m.
So we have $a=mq\Rightarrow m\mid a$. So $I=(m)$.
Therefore, all ideals in a Euclidean domain are principal. □

(b) Prove $F[x]$ is a Euclidean domain when F is a field.

Pf: We will prove that when F is a field, for $f(x),g(x)\in F[x]$, there exist $q(x),r(x)\in F[x]$ s.t. $f(x)=g(x)q(x)+r(x)$ where $r=0$ $(\deg(r)=0)$ or $\deg(r)<\deg(g)$.

- First, we will show uniqueness of $q(x),r(x)$ described above.
Suppose $f(x)=g(x)q_1(x)+r_1(x)=g(x)q_2(x)+r_2(x)$, $r_i(x),q_i(x)$ a stated above, $i=1,2$.
Then $g(x)(q_1(x)-q_2(x))=r_2(x)-r_1(x)$. $\Rightarrow\deg(g(q_1-q_2))=\deg(r_2-r_1)$
If $r_2(x)\neq r_1(x)$, then $r_2-r_1\neq0$, so $\deg(r_2-r_1)<\deg(g)$
If $q_1(x)\neq q_2(x)$, then $q_1-q_2\neq0$,
so $\deg(g(q_1-q_2))=\deg(g)+\deg(q_1-q_2)\geq\deg(g)$. ↯
This is not possible: RHS has deg. $<\deg(g)$ and LHS has deg $\geq\deg(g)$.
Therefore, $q(x),r(x)$ are unique.
- Now we will show existence of $q(x),r(x)\in F[x]$: Let $f(x),g(x)\in F[x]$, $g\neq0$.
Suppose $\deg(f)<\deg(g)$. Then $f(x)=g(x)\cdot0+r(x)$, so $q(x)=0$, $r(x)=f(x)$.

Now suppose $\deg(f)\geq\deg(g)$. Then we will induct on $\deg(f)=m$: the cases $0\leq m\leq\deg(g)-1$ are done. When $m\geq\deg(g)$ write
$f(x)=a_mx^m+a_{m-1}x^{m-1}+\dots+a_1x+a_0$ and
$g(x)=b_nx^n+b_{n-1}x^{n-1}+\dots+b_1x+b_0$, $a_m,b_n\neq0$, $m\geq n$.
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.
Then $f(x)-\frac{a_m}{b_n}x^{m-n}g(x)=(a_mx^m+\dots+a_0)-\frac{a_m}{b_n}x^{m-n}(b_nx^n+\dots+b_0)$
$=a_mx^m+\dots+a_0-a_mx^m-\frac{a_mb_{n-1}}{b_n}x^{m-n}-\dots$

So the degree m terms cancel out, and this poly. either has degree 0 or $\deg<m$. If $f(x)-\frac{a_m}{b_n}x^{m-n}g(x)=0$, then $f(x)=\frac{a_m}{b_n}x^{m-n}g(x)$, so $q(x)=\frac{a_m}{b_n}x^{m-n}$ and $r(x)=0$.
If $\tilde{f}=f-\frac{a_m}{b_n}x^{m-n}g\neq0$, then since $\deg(\tilde{f})<m$, by induction we know $\exists\,Q(x),R(x)\in F[x]$ s.t. $\tilde{f}(x)=Q(x)g(x)+R(x)$, $R(x)\neq0$ or $\deg(R)<\deg(g)$.
$\Rightarrow\tilde{f}=f=\frac{a_m}{b_n}x^{m-n}g+gQ+R=g\underbrace{\left(\frac{a_m}{b_n}x^{m-n}+Q\right)}_{q(x)}+\underbrace{R}_{r(x)}$.

Therefore, we conclude that if F is a field, then $F[x]$ is a Euclidean domain. □

(c) Prove $\mathbb{Z}[x]$ is not a Euclidean domain.

Pf: Consider the ideal $(2,x)$ in $\mathbb{Z}[x]$. $(2,x)$ is not principal.
Suppose $(2,x)=(f(x))$ for $f(x)\in\mathbb{Z}[x]$.
Then $2\in(f(x))\Rightarrow 2=f(x)g(x)$ for $g(x)\in\mathbb{Z}[x]$
Then $\deg(2)=\deg(f(x)g(x))\Rightarrow 0=\deg(f)+\deg(g)$
$\Rightarrow\deg(f(x))=\deg(g(x))=0$.
Since 2 is prime $f(x)=\pm1$ or ±2.
$f(x)\neq\pm1$ b/c if $(f(x))=(\pm1)=\mathbb{Z}[x]$ which is not true since $(2,x)\subset\mathbb{Z}[x]$.
Let $f(x)=2y$ for some $y\in\mathbb{Z}$.
Then $x\in(f(x))=(2y)\Rightarrow x=2y\cdot h(x)$ for $h(x)\in\mathbb{Z}[x]$.
This cannot happen b/c the coeff. of x is 1 and the coeff. of the RHS is not 1, so $h(x)=\frac{x}{2y}$ which cannot happen in $\mathbb{Z}$.
Therefore, $(2,x)$ cannot be a principal ideal.
Thus, $\mathbb{Z}[x]$ is not a PID, but every Euclidean domain is a PID (by part (a)), so $\mathbb{Z}[x]$ is not a Euclidean domain. □

---

⑥ Give examples as requested, with justification.

(a) A group isomorphism from $(\mathbb{Z}/7\mathbb{Z})^\times$ to $(\mathbb{Z}/9\mathbb{Z})^\times$.

Pf: Note that $|(\mathbb{Z}/7\mathbb{Z})^\times|=6$, $(\mathbb{Z}/7\mathbb{Z})^\times=\{1,2,3,4,5,6\}$.
Note that $|(\mathbb{Z}/9\mathbb{Z})^\times|=6$, $(\mathbb{Z}/9\mathbb{Z})^\times=\{1,2,4,5,7,8\}$.
$(\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic since 7 is prime.
$(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic since $9=3^2$ is a prime squared.
Suffices to map generators to generators.
Observe that $\langle3\rangle\cong(\mathbb{Z}/7\mathbb{Z})^\times$:
$3\cdot3=9\equiv2(7)$, $2\cdot3=6(7)$, $6\cdot3=18\equiv4(7)$, $4\cdot3=12\equiv5(7)$, $5\cdot3=15\equiv1(7)$.
So 3 generates $(\mathbb{Z}/7\mathbb{Z})^\times$. $(|3|=6)$
Observe that $\langle2\rangle\cong(\mathbb{Z}/9\mathbb{Z})^\times$:
$2\cdot2=4(9)$, $4\cdot2=8(9)$, $8\cdot2=16\equiv7(9)$, $7\cdot2=14\equiv5(9)$, $5\cdot2=10\equiv1(9)$.
So 2 generates $(\mathbb{Z}/9\mathbb{Z})^\times$. $(|2|=6)$
Let $\varphi:(\mathbb{Z}/7\mathbb{Z})^\times\longrightarrow(\mathbb{Z}/9\mathbb{Z})^\times$ by $\varphi(3)=2$, so we map generator to gen.
$\varphi(3)=2$, $\varphi(3)^2=\varphi(3^2)=2^2$, $\varphi(3)^3=\varphi(3^3)=2^3,\dots$
$(3\mapsto2, 2\mapsto4, 6\mapsto8, 4\mapsto7, 5\mapsto5, 1\mapsto1)$
Thus, φ is a group isomorphism. □

(b) A cyclic group with 20 generators. (Also $\mathbb{Z}/25\mathbb{Z}$, $\varphi(25)=20$)

Pf: We want to find $\mathbb{Z}/n\mathbb{Z}$ s.t. $\varphi(n)=20$.
Notice that $20=2\cdot10$ and φ is multiplicative for $n=ab$ when $(a,b)=1$, so $\varphi(n)=\varphi(a)\varphi(b)$ where $\varphi(a)=2$ and $\varphi(b)=10$.
Let $a=3$ and $b=11$. Then $\varphi(3)\varphi(11)=2\cdot10=20$ and $\varphi(3)\varphi(11)=\varphi(33)$.
Therefore, $\mathbb{Z}/33\mathbb{Z}$ is a cyclic group w/ 20 generators. □

(c) A unit in $\mathbb{Z}[\sqrt{11}]$ other than ±1.

Pf: Let $x+y\sqrt{11}\in\mathbb{Z}[\sqrt{11}]$. So $N(x+y\sqrt{11})=(x+y\sqrt{11})(x-y\sqrt{11})=x^2-11y^2=\pm1$.
Consider $x^2=1+11y^2$.
Let $y=3$, $x=10$. Then $10^2=100$ and $1+11(3)^2=1+11\cdot9=1+99=100$.
Therefore, $10+3\sqrt{11}\in\mathbb{Z}[\sqrt{11}]$ is a unit other than ±1. □

(d) A prime element of $\mathbb{Z}[i]$.

Pf: Consider $1+i\in\mathbb{Z}[i]$.
$N(1+i)=(1+i)(1-i)=2$ which is prime, so $1+i$ is irreducible.
Since $\mathbb{Z}[i]$ is a Euclidean domain, it is a PID, and hence a UFD.
In UFD's $\{\text{primes}\}=\{\text{irred.}\}$.
In a PID, every irred. is prime.
Therefore, $1+i$ is a prime element of $\mathbb{Z}[i]$. □