August 2019

sábado, 24 de diciembre de 2022 2:27 p.m.

① For a ring R, write $GL_3(R)$ for the group of 3×3 matrices with entries in R and determinant in the units $R^\times$.

(a) Give, with reasoning, a matrix in $GL_3(\mathbb{Z})$ with first row (6 10 15).

Pf: Note that $GL_3(\mathbb{Z}) = \{A \in M_3(\mathbb{Z}) : \det(A) = \pm 1\}$.
Consider M being the matrix in $GL_3(\mathbb{Z})$ w/ first row (6 10 15).
Then $\det(M) = 6A - 10B + 15C = \pm 1$, where A, B, C are determinants of 2×2 matrices
Then $A=1, B=-1, C=-1$ gives $6(1) - 10(-1) + 15(-1) = 6 + 10 - 15 = 1$ ✓
Let $M = \begin{pmatrix} 6 & 10 & 15 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Then $\det(M) = 6(1) - 10(-1) + 15(-1) = 1$

So the matrix $\begin{pmatrix} 6 & 10 & 15 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{Z})$ as desired. □

(b) Let $\mathbb{Z}[x]$ be the polynomial ring with coefficients in $\mathbb{Z}$. Show that no matrix in $GL_3(\mathbb{Z}[x])$ has first row $(6\ 2x\ 3x)$.

Pf: Recall that $GL_3(\mathbb{Z}[x]) = \{A \in M_3(\mathbb{Z}[x]) : \det(A) = \pm 1\}$.
Consider $M \in GL_3(\mathbb{Z}[x])$ w/ first row $(6\ 2x\ 3x)$.
Then $\det(M) = 6 \cdot A(x) - 2x \cdot B(x) + 3x \cdot C(x) = \pm 1$
($A(x), B(x), C(x)$ are the determinants of 2×2 matrices (minors).)
Evaluate at $x=0$: $6 \cdot A(0) - 2 \cdot 0 \cdot B(0) + 3 \cdot 0 \cdot C(0) = \pm 1$

$\Rightarrow 6 \cdot A(0) = \pm 1$

$\Rightarrow A(0) = \frac{\pm 1}{6} \in \mathbb{Q}$, $\notin \mathbb{Z}$ } this means that the det. of the matrix of $A(x)$ evaluated at $x=0$ is $\pm 1/6$, which is not an integer.

Therefore, there does not exist such a matrix in $GL_3(\mathbb{Z}[x])$. □

---

② (a) For prime p, define a p-Sylow subgroup of a finite group G.

Pf: Let G be a finite group s.t. $|G| = p^k m$, p prime, $p \nmid m$.
A subgroup of order p^k is called a p-Sylow subgroup.
(in other words, a p-Sylow subgp. is a subgp. of G w/ order the highest power of p that divides $|G|$.) □

(b) Prove that if a p-group H acts on a finite set X, then $\#X \equiv \#\mathrm{Fix}_H(X) \bmod p$, where $\mathrm{Fix}_H(X)$ is the set of points in X fixed by all of H.

Pf: Let the different orbits in X be represented by $x_1, \dots, x_n$, so we can write $|X| = \sum_{i=1}^{n} |\mathrm{Orb}_{x_i}|$. By the orbit-stabilizer thm, we have that $|\mathrm{Orb}_{x_i}| = [H : \mathrm{Stab}_{x_i}]$. We also have that $|H|$ is a power of p, so $|\mathrm{Orb}_{x_i}| \equiv 0 \bmod p$, unless $H = \mathrm{Stab}_{x_i} \Rightarrow [H : \mathrm{Stab}_{x_i}] = 1 = |\mathrm{Orb}_{x_i}|$, i.e., the orbit of x_i has length 1, which means that x_i is a fixed pt.
If we reduce $|X| = \sum_{i=1}^{n} |\mathrm{Orb}_{x_i}| \bmod p$, we get that all terms on the RHS vanish except for a contribution of 1 for each fixed point.
So we have $|X| \equiv |\mathrm{Fix}_H(X)| \bmod p$. □

(c) For each prime p, prove that if P and Q are p-Sylow subgroups of a finite group G, then P and Q are conjugate in G. (That is, prove the second part of the Sylow theorems.) You may use part (b).

Pf: $P, Q \in \mathrm{Syl}_p(G)$, let $|G| = p^k m$, $p \nmid m$, and $|P| = |Q| = p^k$.
Let Q act on G/P by left multiplication.
By fixed-point congruence,
$\underbrace{|G/P|}_{|G|/|P| = p^k m/p^k = m \not\equiv 0 \bmod p} \equiv |\mathrm{Fix}_Q(G/P)| \bmod p$ } $\Rightarrow |\mathrm{Fix}_Q(G/P)| \not\equiv 0 \bmod p$ $\Rightarrow \mathrm{Fix}_Q(G/P) \neq \emptyset$

Let $gP \in G/P$ be the fixed point in $\mathrm{Fix}_Q(G/P)$.
Then $qgP = gP$ for all $q \in Q \Rightarrow g^{-1}qgP = P \Rightarrow g^{-1}qg \in P \Rightarrow qg = gP$
Equivalently, $qg \in gP$ for all $q \in Q$, so $Q \subset gPg^{-1}$. Therefore, $Q = gPg^{-1}$, since Q and gPg^{-1} have the same size, we are done. □

---

③ Let F be a field.

(a) Prove that if $f(x) \neq 0$ in $F[x]$, then it has at most $\deg f$ different roots in F.

Pf: If $f(x) \neq 0$ had more than $n = \deg f$ roots, then by the division algorithm we can write $f(x) = (x-a_1)(x-a_2)\cdots(x-a_m)$ where $m > n$.
But then the RHS is a polynomial of degree m and the LHS is a polynomial of degree n. ↯
Therefore, $f(x)$ must have at most $n = \deg f$ different roots in F. □

(b) If $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ where F is infinite and $f(a_1, \dots, a_n) = 0$ for all $a_1, \dots, a_n \in F$, then prove $f = 0$ in $F[x_1, \dots, x_n]$. You may use part (a).

Pf: We will use induction. The case $n=1$ is part (a).
Now suppose the claim holds for all j s.t. $1 \le j \le n$.
Let $f(x_1, \dots, x_{n+1}) \in F[x_1, \dots, x_{n+1}]$ and $f(a_1, a_2, \dots, a_{n+1}) = 0$ for all $a_1, a_2, \dots, a_n, a_{n+1} \in F$.
We may assume f contains all $n+1$ indeterminants $x_1, x_2, \dots, x_{n+1}$ or else we could invoke the induction by hypothesis.
Write f as a polynomial in $(F[x_1, \dots, x_n])[x_{n+1}]$.
That is, $f(x_1, \dots, x_n, x_{n+1}) = g_k(x_1, \dots, x_n) x_{n+1}^k + \dots + g_1(x_1, \dots, x_n) x_{n+1}^1 + g_0(x_1, \dots, x_n)$.
If for any tuple $(a_1, a_2, \dots, a_n) \in F^n$ we have $f(a_1, \dots, a_n, a_{n+1}) = 0$, then $g_j(a_1, \dots, a_n) = 0$ for all $0 \le j \le k$.
Since $g_j \in F[x_1, \dots, x_n]$, we conclude by induction that $g_j \equiv 0$ for all $0 \le j \le k$.
Hence, $f \equiv 0$ which would prove the claim for the $n+1$ case.
We claim that this must be the case.
If $\exists (a_1, a_2, \dots, a_n) \in F^n$ s.t. $f(a_1, \dots, a_n, x_{n+1}) \neq 0$, then define $g(x) = f(a_1, \dots, a_n, x_{n+1})$. Note that $g(x) \in F[x_{n+1}]$, a poly. in one variable and since $f(a_1, \dots, a_n, a) = 0$ for any $a \in F$ by hypothesis, we see that $g(a) = 0$ for all $a \in F$.
Since f is infinite, this would imply that $g(x)$ has infinitely many roots. By part (a), $g \equiv 0$.
But this means $g_j(x_1, \dots, x_n) \equiv 0$ for each $0 \le j \le k$. ↯
Since $f(a_1, \dots, a_n, x_{n+1}) \not\equiv 0$.
Therefore, we verified the claim for the $n+1$ case. Now apply induction to show it's true for all $n \in \mathbb{N}$. □

---

⑤ Let R be a commutative ring with identity.

(a) Define what it means for R to be a principal ideal domain.

Pf: R is a PID if every ideal in R is principal. □

(b) Prove that if R is a principal ideal domain, then every nonzero prime ideal in R is a maximal ideal.

Pf: Since R is a PID, it is also a UFD, so in R {primes} = {irred.}.
We want to show that if (a) is a nonzero prime ideal, then for an ideal I, $(a) \subset I \subset R$, either $I = (a)$ or $I = R$.
Let $(a) \in R$ be a nonzero prime ideal. Then a is irred. in R, so $a = uv$ where u or v is a unit in R.
Suppose $\exists (b) \in R$ s.t. $(a) \subset (b) \subset R$.
Then $b \mid a \Rightarrow b \mid uv$, so b is either a unit or an associate of a.
If b is a unit, then $(b) = R$.
If b is an associate of a, then $(b) = (a)$.
Therefore, we conclude that (a) is a maximal ideal. □

---

⑥ Give examples as requested, with justification.

(a) A noncyclic group that is not isomorphic to a semidirect product of nontrivial groups.

Pf: Consider A_5. The gp. A_5 is noncyclic and it does not have any normal subgroups. Therefore, it cannot be isom. to a semidirect product of nontrivial groups (b/c this requires a normal subgp.) □

(b) A prime p such that the ideal (p, x^2-3) in $\mathbb{Z}[x]$ is maximal.

Pf: The maximal ideals in $\mathbb{Z}[x]$ are of the form $(p, f(x))$ where p prime and $f(x)$ is monic, irred. mod p.
Consider the prime $p=5$. Then
$0^2 - 3 \equiv -3 \equiv 2\ (5)$
$1^2 - 3 \equiv -2 \equiv 3\ (5)$
$2^2 - 3 \equiv 1\ (5)$
$3^2 - 3 \equiv 1\ (5)$
$4^2 - 3 \equiv 3\ (5)$
Therefore, $x^2 - 3$ is irred. mod 5.
Thus, $p=5$ is a prime s.t. $(5, x^2-3)$ in $\mathbb{Z}[x]$ is maximal. □

(c) A UFD that is not a Euclidean domain.

Pf: Consider $\mathbb{Z}[x]$.
It is a UFD since $\mathbb{Z}$ is a UFD.
$\mathbb{Z}[x]$ is not a Euclidean domain b/c it is not a PID.
Consider the ideal $(2, x)$ in $\mathbb{Z}[x]$. It is not principal.
Therefore, $\mathbb{Z}[x]$ is a UFD that is not a Euclidean domain. □