# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo de orden $|G| = p^2q^2$ donde $p$ y $q$ son primos distintos. Muestre que $G$ no es simple.
2. Sea $G$ un grupo actuando en el conjunto $X$. Suponga que $|G| = p^n$ donde $p$ es un primo y suponga también que $\text{mcd}(|X|, p) = 1$. Muestre que existe $x \in X$ tal que $gx = x$ para todo $g \in G$.
3. Sea $R$ un anillo comutativo con 1 y sea $a \in R$. Sean $m$ y $n$ números naturales con máximo común divisor $d$. Sea $I \subseteq R$ el ideal en $R$ generado por $a^m - 1$ y $a^n - 1$ y sea $J \subseteq R$ el ideal generado por $a^d - 1$.
   (a) Muestre que $(a^d - 1) \mid (a^n - 1)$.
   (b) Muestre que $I \subseteq J$.
   (b) Muestre que $J \subseteq I$ y concluya que $I = J$.
4. Sea $I = \langle 5, X^3 + X + 1 \rangle$ el ideal de $\mathbb{Z}[X]$ generado por 5 y $X^3 + X + 1$. Determine si $I$ es un ideal primo.
5. Sea $f(x) = x^3 - 5 \in \mathbb{Q}[x]$ y sea $E$ el cuerpo de descomposición de $f$ sobre $\mathbb{Q}$.
   (a) Encuentre $E$ explicitamente.
   (b) Determine $[E : \mathbb{Q}]$.
   (c) Encuentre $Gal(E/\mathbb{Q})$.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo de orden $|G| = pq$ donde $p$ y $q$ son primos. Suponiendo que $p < q$ y que $p \nmid (q-1)$, muestre que $G$ es cíclico.

2. Sea $G$ un grupo finito y sea $H \leq G$ un subgrupo. Muestre que $H$ tiene el mismo número de coclases por la izquierda que por la derecha.

3. Sea $R$ un anillo comutativo con 1 y sea $a \in R$. Sean $m$ y $n$ números naturales con máximo común divisor $d$. Sea $I \subseteq R$ el ideal en $R$ generado por $a^m - 1$ y $a^n - 1$ y sea $J \subseteq R$ el ideal generado por $a^d - 1$.

   (a) Muestre que $(a^d - 1) \mid (a^n - 1)$.

   (b) Muestre que $I \subseteq J$.

   (b) Muestre que $J \subseteq I$ y concluya que $I = J$.

4. Sea $\mathbb{F}_3$ el cuerpo con 3 elementos. Encuentre un polinomio $f \in \mathbb{F}_3[X]$ tal que el anillo $\mathbb{F}_3[X]/(f)$ sea un cuerpo con 27 elementos.

5. Sea $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ y sea $E$ el cuerpo de descomposición de $f$ sobre $\mathbb{Q}$.

   (a) Encuentre $E$ explicitamente.

   (b) Determine $[E : \mathbb{Q}]$.

   (c) Encuentre $Gal(E/\mathbb{Q})$.

 

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo finito y sea $\sigma : G \to G$ un automorphismo de $G$ tal que $\sigma(g) = g$ si y solo si $g = 1$ es la identidad de $G$.

   (a) Muestre que la función $f(g) = g^{-1}\sigma(g)$ de $G$ en $G$ es inyectiva, y por lo tanto biyectiva.

   Suponga ahora que $\sigma(\sigma(g)) = g$ para todo $g \in G$.

   (b) Usando (a) muestre que $\sigma(g) = g^{-1}$ para todo $g \in G$.

   (c) Muestre que $G$ es abeliano de orden impar.

2. Sea $R$ un anillo comutativo. Se define

$$N(R) = \{a \in R \,|\, a^n = 0 \text{ para algún } n \in \mathbb{N}\}$$

   (a) Muestre que $N(R)$ es un ideal de $R$.

   (b) Sea $P \subseteq R$ un ideal primo de $R$. Muestre que $N(R) \subseteq P$.

3. Sea $K$ un cuerpo tal que $\mathrm{char}(K) = p$ (primo) y sea $F/K$ una extensión cíclica de grado $p$. Sea $\sigma$ un generador del grupo de Galois de $F/K$.

   (a) Pruebe que la transformación $K$-lineal $S : F \longrightarrow F$ definida por $S(\alpha) = \alpha - \sigma(\alpha)$ es nilpotente.

   (b) Muestre que existe un elemento $\alpha$ en el nucleo de $S^2 = S \circ S$, pero no en el nucleo de $S$, y que $\beta = \frac{\alpha}{\sigma(\alpha) - \alpha}$ satisface $\sigma(\beta) = \beta + 1$.

   (c) Muestre que $\beta$ de (b) satisface una ecuación del tipo $x^p - x - a = 0$ sobre $K$.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo no necesariamente finito y sea $Z(G)$ su centro. Suponiendo que $G/Z(G)$ es cíclico, muestre que $G$ es abeliano.
2. Sea $G$ un grupo de orden 55.
   (a) Pruebe que $G$ está generado por dos elementos $x, y$ tales que $x^{11} = 1, y^5 = 1, yxy^{-1} = x^r$ donde $r \in \{1, 2, \ldots, 11\}$.
   (b) Demuestre que $r \notin \{2, 6, 7, 8, 10, 11\}$.
3. Sea $R$ un anillo comutativo con 1.
   (a) Suponga que para cada $a \in R$ existe un $n > 1$ tal que $a^n = a$. Muestre que cada ideal primo de $R$ es maximal.
   (b) Suponga que cada ideal de $R$ es primo. Muestre que $R$ es un cuerpo.
4. Sea $R = \mathbb{Z}[i]$. Encuentre el máximo comun divisor entre 25 y $13 + 16i$ en $R$.
5. Sean $E = \mathbb{Q}(i, 2^{1/8})$, $F = \mathbb{Q}(i)$ y $K = \mathbb{Q}(\sqrt{-2})$. Muestre que
   (a) $E$ es de Galois sobre $\mathbb{Q}$.
   (b) $\text{Gal}(E/F)$ es cíclico.
   (b) $\text{Gal}(E/K)$ es no abeliano.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo finito y sea $N \trianglelefteq G$ un subgrupo normal de $G$. Se dice que el subgrupo $H \leq G$ es un *complemento* de $N$ si $G = NH$ y si $N \cap H = \{1\}$.
   (a) Sea $p$ un número primo y sea $H \leq G$ un complemento de $N \trianglelefteq G$ tal que $|H| = p^k$ para algún $k \geq 0$. Sea $S \in \mathrm{Syl}_p(G)$. Muestre que $S$ contiene un complemento de $N$.
   (b) Sea $N \trianglelefteq G$ tal que $Z(N) = \{1\}$. Suponga que los únicos automorfismos de $N$ son conjugaciones por elementos de $N$. Muestre que existe un complemento $K$ de $N$ tal que $K \trianglelefteq G$.
2. Sea $G$ un grupo finito que actúa en un conjunto $A$, via $(g, a) \mapsto g \cdot a$. Para $a \in A$ se define $O(a) = G \cdot a \subseteq A$ y $G_a = \{g \in G \,|\, g \cdot a = a\}$.
   (a) Muestre que $G_a \leq G$ y que $|G : G_a| = |O(a)|$.
   (b) Sea $P$ un grupo de orden $|P| = p^n$ donde $p$ es un primo. Usando (a) con una acción apropiada muestre que $Z(P) \neq 1$.
3. Sea $p$ un numero primo. Sea $F$ un cuerpo tal que $|F| = p^n$ para algún $n$.
   (a) Muestre que la aplicación $\varphi$ de $F$ dada por $\alpha \mapsto \alpha^p$ es un automorfismo de $F$.
   (b) Muestre que $\varphi$ tiene orden $n$.
4. Sea $A$ un anillo conmutativo con 1. Suponga que para cada $a \in A$ existe un $n \geq 1$ tal que $a^n = a$. Pruebe que todo ideal primo de $A$ es maximal.
5. Sea $\eta$ una séptima raíz primitiva de unidad y sea $K = \mathbb{Q}(\eta)$.
   (a) Encuentre explicitamente el grupo de Galois $Gal(K/\mathbb{Q})$.
   (b) Muestre que hay un único cuerpo intermedio $\mathbb{Q} \subset F \subset K$ tal que $[F : \mathbb{Q}] = 2$. Describa $F$ explicitamente.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo finito, y sea $S_n$ el grupo simétrico sobre $\{1, 2, \ldots, n\}$ para $n$ un número natural fijo. Muestre que las siguientes afirmaciones son equivalentes:
   (a) Existe homomorfismo $\varphi : G \to S_n$ y un elemento $g \in G$ tal que $g \notin \ker\varphi$.
   (b) Existe subgrupo $H$ de $G$ tal que $1 < |G : H| \leq n$.
2. Sea $G$ un grupo finito con subgrupo $H$, y sea $\mathcal{A} = \{P \in \mathrm{Syl}_p(G) \mid H \leq P\}$ para un primo $p$. Sea $Q \in \mathcal{A}$.
   (a) Muestre que $Q \cap N_G(H)$ actúa en $\mathcal{A}$ por conjugación.
   (b) Muestre que $|\mathcal{A}| = 1 \mod p$.
3. Sea $R$ un anillo con 1 tal que 0 y $R$ son los únicos ideales de $R$. Muestre que el centro de $R$ es un cuerpo.
4. Sea $p$ un primo. Sea $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ donde $n \geq 1$. Muestre las siguientes afirmaciones.
   (a) $f(x)$ es separable.
   (b) Si $g(x)$ es un factor irreducible de $f(x)$ entonces $\deg g(x)$ divide a $n$.
5. Sea $f(x) = x^4 - 4x^2 + 2$.
   (a) Sea $E$ el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$. Determine $E$ y el grado $[E : \mathbb{Q}]$.
   (b) Encuentre $G = \mathrm{Gal}(E/\mathbb{Q})$ y describa la acción de $G$ sobre las raíces de $f(x)$.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $V$ un $\mathbb{C}$-espacio vectorial de dimensión finita y sea $(\cdot,\cdot) : V \times V \to \mathbb{C}$ una función tal que:
   - $(v_1, v_2) = \overline{(v_2, v_1)}$, donde $\overline{a}$ es el conjugado de $a \in \mathbb{C}$;
   - $(v, av_1 + bv_2) = a(v, v_1) + b(v, v_2)$ para todo $v, v_1, v_2 \in V$ y $a, b \in \mathbb{C}$;
   - $(v, v) \in \mathbb{R}_{>0}$ para todo $v \in V \setminus \{0\}$.

   Suponga que $f : V \to V$ es $\mathbb{C}$-lineal y $(f(v), v) = 0$ para todo $v \in V$, pruebe que $f = 0$.

   **Indicación:** Primero pruebe que la matriz asociada a $f$ es nilpotente.

2. Sea $p$ un número primo, $G$ un grupo finito y $H \leq G$ un subgrupo de $G$. Además, sea $m(H)$ el número de $p$-subgrupos de Sylow de $G$ que contienen a $H$.

   Demuestre que $m(H) = 0$ o $m(H) = 1$ módulo $p$.

3. Considere el anillo $R := \mathbb{Q}[x]/I$, donde $I$ es el ideal generado por $x - x^2$. Pruebe que $R \cong \mathbb{Q} \times \mathbb{Q}$.

4. Sea $k$ un cuerpo y $R$ el subanillo de $k[x]$ que consiste en todos los polinomios sin termino de grado 1, es decir $R := \{p(x) \in k[x] : \ p(x) = a_0 + a_2x^2 + \cdots\}$. Pruebe que $x^5$ y $x^6$ no tienen máximo común divisor en $R$.

5. Sea $F$ un cuerpo de característica 0 y $E$ una extensión Galois finita simple de $F$, es decir, existe $\alpha \in E \setminus \{0\}$ tal que $E = F[\alpha]$.
   (a) Pruebe que $F[\alpha^2] \neq E$ si y solo si existe $g \in \mathrm{Gal}(E/F)$ tal que $g(\alpha) = -\alpha$.
   (b) Pruebe que existe $\beta \in E \setminus F$ tal que $E = F[\beta^2]$.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 3 horas

1. (a) Sea $G$ un grupo y $H$ un subgrupo de $G$ de indice finito. Demuestre que $G$ posee un subgrupo **normal** de indice finito que está contenido en $H$.
   (b) Sean $H_1$ y $H_2$ dos subgrupos de $G$ de indice finito. Demuestre que $H_1 \cap H_2$ es un subgrupo de $G$ de indice finito.
2. Sea $p$ un entero primo, $G$ un grupo finito y $H$ un subgrupo **normal** de orden $p$.
   (a) Demuestre que $H$ esta contenido en todo $p$-subrupo de Sylow de $G$.
   (b) Suponga que $P$ es un $p$-subgrupo de $G$ que contiene a $H$. Demuestre que $H$ está contenido en el centro del grupo $P$.
3. Se considera el anillo $R = \mathbb{Z}[x]/(2, x^3 + 1)$. Encuentre dos cuerpos $K_1$ y $K_2$ tales que $R$ sea isomorfo a $K_1 \times K_2$.
4. Considere el anillo $\mathbb{Z}[\sqrt{-5}]$. Verifique que $1 + \sqrt{-5}$ es elemento irreducible que no es primo. Concluya que $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única.
5. Sea $p(x) \in \mathbb{Q}[X]$ un polinomio de grado $n > 2$, $K$ el cuerpo de descomposición de $p(x)$ sobre $\mathbb{Q}$ y suponga que $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{S}_n$. Demuestre que $|\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 1$, donde $\alpha$ es una raíz de $p(x)$.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo de orden $|G| = 3 \times 5^2 \times 7$ y sea $H \leq G$ un subgrupo de orden $|H| = 5^2 \times 7$. Sea $\varphi : G \to \mathrm{Sym}(G/H)$ el homomorfismo asociado a la acción de $G$ en $G/H$ por multiplicación por la izquierda. Muestre que $H = \operatorname{Ker}\varphi$.

2. (a) Sean $k$, $m$ y $p$ tres enteros estrictamente positivos, tal que $p$ es un primo que no divide a $m$, y sea $G$ un grupo simple de orden $mp^k$. Pruebe que $p^k$ divide a $(m-1)!$.
   (b) Sea $G$ un grupo de orden $2^k 5$. Pruebe que para todo $k \geq 1$ el grupo $G$ no es simple.

3. (a) Considere el anillo $\mathbb{Z}[i]$ y el ideal $I$ generado por 6 y $9 - 3i$.
      i. Explique, sin realizar cálculos, por qué existe $a \in \mathbb{Z}[i]$ tal que $I = (a)$.
      ii. Encuentre explicitamente $a \in \mathbb{Z}[i]$ tal que $I = (a)$.
   (b) Sea $R$ un dominio de factorización única y sea $K$ su cuerpo de fracciones. Considere un polinomio mónico $f(x) \in R[x]$ y suponga que $\alpha \in K$ es una raíz de $f$. Pruebe que $\alpha$ pertenece a $R$.

4. Sea $R = \mathbb{Z}/6\mathbb{Z}$. Encuentre todos los polinomios $f(x), g(x) \in R[x]$ tal que $x = f(x)g(x)$ en $R[x]$.

5. Sea $K$ un cuerpo de característica $p > 0$ y $L$ una extensión finita de $K$. Pruebe que si $[L : K]$ es relativo con $p$, entonces $L|K$ es una extensión separable.

6. Sean $p, q$ dos primos distintos, $n > 0$ un entero positivo y $K/F$ una extensión de Galois tal que

$$|\operatorname{Gal}(K/F)| = pq^n$$

   (a) Suponga que $p < q$. Demuestre que existe una extensión de Galois de $F$ de grado $p$ contenida en $K$.

   (b) Suponga que $p > q$. De un contraejemplo a la parte $(a)$.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo finito y sea $H \leq G$ subgrupo tal que $|G| \nmid |G : H|!$. Muestre que $H$ tiene un subgrupo $1 \neq N \leq H$ tal que $N \trianglelefteq G$.

2. Sean $G_1$ y $G_2$ grupos finitos y sea $p \geq 2$ un primo. Sean $n_p(G_1), n_p(G_2)$ y $n_p(G_1 \times G_2)$ los números de grupos Sylow-$p$ de $G_1$, $G_2$ y $G_1 \times G_2$ respectivamente. Muestre que $n_p(G_1 \times G_2) = n_p(G_1)n_p(G_2)$.

3. Sea $S_3$ el grupo simétrico sobre $\{1, 2, 3\}$ y sea $\varphi : S_3 \to Aut(S_3)$ el homomorphismo dado por conjugación. Muestre que $\varphi$ es un isomorphismo.

4. Sean los anillos $R$ y $S$ dados por $R = \mathbb{Z}/15\mathbb{Z}$ y $S = \mathbb{Z}/30\mathbb{Z}$. Encuentre todos los homomorfismos de anillo $\varphi : R \to S$.

5. Exprese $14 + 6i$ como producto de primos de $\mathbb{Z}[i]$. (*Indicación: use la norma de* $\mathbb{Z}[i]$).

6. Demuestre que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ y encuentre el polinomo minimal de $\sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$ y su cuerpo de descomposición.

7. Sea $E = \bigcup_{n=1}^{\infty} \mathbb{Q}(2^{\frac{1}{n}}) \subseteq \mathbb{R}$.
   (a) Muestre que $E$ es un cuerpo.
   (b) Muestre que $[E : \mathbb{Q}] = \infty$.
   (c) Muestre que la identidad es el único $\mathbb{Q}$-automorfismo $\sigma : E \to E$.

# Algebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 3 horas

1. Sea $S_n$ el grupo simétrico de grado $n$ y $H$ un subgrupo normal de $S_n$ que contiene una transposición. Pruebe que $H = S_n$.

2. Sea $P$ un $p$-subgrupo de Sylow de $H$ y $H$ un subgrupo de $G$.

   (a) Si $P \lhd H$ y $H \lhd G$. Demuestre que $P \lhd G$.

   (b) Además suponga que $H = N_G(P) := \{g \in G \mid gPg^{-1} = P\}$, es decir $H$ es el normalizador de $P$ en $G$. Pruebe que $N_G(H) = H$.

3. (a) Encuentre dos polinomios $q(x), r(x) \in \mathbb{Q}[x]$ tales que:

$$x^2 q(x) = 1 \text{ mod } 3x^3 + 1 \text{ y } (3x^3 + 1)r(x) = 1 \text{ mod } x^2$$

   (b) Encuentre todos los polinomios $p(x) \in \mathbb{Q}[x]$ tales que:

$$p(x) = x^2 \quad \text{mod } 3x^3 + 1, \quad p(x) = 2x + 1 \quad \text{mod } x^2$$

4. Sea $p(x) \in \mathbb{Z}[x]$ tal que $p(0)$ y $p(1)$ son enteros impares. Pruebe que $p(x)$ no tiene raíces en $\mathbb{Z}$.

5. Sea $f(x) = x^4 - 7 \in \mathbb{Q}[x]$ y $G$ el grupo de Galois del polinomio $f$.

   (a) Calcule el orden de $G$.

   (b) Determine un sistema de generadores de $G$ y muestre de forma explicita la acción de $G$ sobre las raíces de $f$.

   (c) Determine $G$ como grupo abstracto.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.
**Tiempo**: 4 horas

1. Sea $G$ un grupo finito que actúa transitivamente sobre un conjunto $X$. Diremos que $Y \subset X$ es un **bloque** si para cada $g \in G$ se satisface una de las siguientes propiedades: $g(Y) = Y$ o $g(Y) \cap Y = \emptyset$. El grupo $G$ es llamado **primitivo** si el único bloque en $X$ es el trivial (es decir $Y = X$).

   (a) Sea $x \in X$ y $Y$ un bloque que contiene a $x$. Pruebe que $G_Y := \{g \in G \mid g(Y) = Y\}$ es un subgrupo de $G$ que contiene al estabilizador $G_x$.

   (b) Pruebe que el grupo transitivo $G$ es primitivo si y sólo si para cada $x \in X$ el grupo $G_x$ es un subgrupo maximal de $G$.

2. Sea $D_{2n} := \{r, s \mid r^n = s^2 = (rs)^2 = 1\}$ la presentación usual del grupo Diedral de orden $2n$.

   (a) Sea $m$ un entero positivo que divide a $n$. Pruebe que el grupo $\langle r^m \rangle$ es un subgrupo normal de $D_{2n}$ y que $D_{2n}/\langle r^m \rangle \cong D_{2m}$.

   (b) Sea $n = 2^l k$, donde $k$ es impar y $l$ es un entero positivo. Pruebe que el número que 2-subgrupos de Sylow de $D_{2n}$ es $k$.

3. Determine todos los ideales del anillo $\mathbb{Z}[x]/(2, x^3 + 1)$.

4. Sea $K$ un cuerpo y $f(x) := x^7 + y^7 + z^7$ un polinomio en $K[x, y, z]$. Pruebe que $f$ es irreducible si y sólo si la característica de $K$ es diferente a 7.

5. Sea $B$ un anillo conmutativo y $A$ un subanillo con unidad. Un elemento $b \in B$ es llamado **entero** sobre $A$ si existe un polinomio **mónico** $p(x) \in A[x]$ tal que $p(b) = 0$. Diremos que el anillo $B$ es entero sobre $A$, si todo elemento de $B$ es entero sobre $A$.

   Suponga que $B$ es entero sobre $A$ y que $B$ es un dominio de integridad. Demuestre que $A$ es un cuerpo si y sólo si $B$ lo es.

6. Sea $f(x) = x^5 - 2 \in \mathbb{Q}[x]$ y $G$ el grupo de Galois del polinomio $f$.

   (a) Calcule el orden de $G$.

   (b) Pruebe que $G$ tiene un subgrupo normal de orden 5.

   (c) Pruebe que $G$ no es abeliano.

   (d) Pruebe que $G$ es isomorfo a un subgrupo del grupo simétrico $S_5$ que no contiene transposiciones.

# Álgebra

**Instrucciones**: Conteste en forma ordenada y justifique adecuadamente cada respuesta.

**Tiempo**: 4 horas

1. Sea $G$ un grupo finito que actúa transitivamente sobre un conjunto $X$. Considere el siguiente conjunto $Y := \{(x_1, x_2) \in X \times X \mid x_1 \neq x_2\}$.
   (a) Pruebe que la aplicación $G \times Y \to Y : (g, (x_1, x_2)) \mapsto (g(x_1), g(x_2))$ es una acción bien definida del grupo $G$ sobre el conjunto $Y$.
   (b) Diremos que el grupo $G$ es doblemente transitivo sobre $X$ si $G$ es transitivo sobre $Y$. Pruebe que $G$ es doblemente transitivo sobre $X$ si y sólo si para todo $x \in X$ el estabilizador $G_x := \{g \in G \mid g(x) = x\}$ actúa transitivamente sobre el conjunto $X - \{x\}$.
   (c) Sea $D_8$ el grupo diedral de 8 elementos equipado con su acción natural sobre los vértices de un cuadrado. Muestre que $D_8$ no es doblemente transitivo.
2. Sea $G$ un grupo de orden 105. Pruebe que si un 3-subgrupo de Sylow de $G$ es normal, entonces $G$ es abeliano.
3. Determine todos los ideales del anillo $\mathbb{Z}[x]/(2, x^3 + 1)$.
4. Pruebe que el siguiente polinomio es irreducible en $\mathbb{Q}[x]$:
$$f(x) := 2x^7 + 4x^6 + 12x^4 + 6x + 3$$
5. Sea $B$ un anillo conmutativo y $A$ un subanillo con unidad. Un elemento $b \in B$ es llamado **entero** sobre $A$ si existe un polinomio **mónico** $p(x) \in A[x]$ tal que $p(b) = 0$. Diremos que el anillo $B$ es entero sobre $A$, si todo elemento de $B$ es entero sobre $A$.

   Suponga que $B$ es entero sobre $A$ y que $B$ es un dominio de integridad. Demuestre que $A$ es un cuerpo si y sólo si $B$ lo es.
6. Sea $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ y $G$ el grupo de Galois del polinomio $f$.
   (a) Calcule el orden de $G$.
   (b) Muestre de forma explicita la acción de $G$ sobre las raíces de $f$, determine un sistema de generadores de $G$ y pruebe que $G$ es isomorfo a $D_8$.
   (c) Calcule los subgrupos de $G$ de orden 4 y sus cuerpos fijos.

1. Sea $G$ un grupo finito que actúa transitivamente sobre un conjunto $X$ con $\#(X) \geq 2$. Pruebe que existe un elemento $g$ en el grupo $G$ tal que $g(x) \neq x$ para todo $x$ perteneciente a $X$.

2. Sea $G$ un grupo finito, $P$ un $p$-subgrupo de Sylow de $G$ y $H$ un subgrupo normal de $G$

   *a*) Pruebe que $P \cap H$ es un $p$-subgrupo de Sylow de $H$.

   *b*) Pruebe que $PH/H$ es un $p$-subgrupo de Sylow de $G/H$.

   *c*) Suponga que $H < G$ **no** es un subgrupo normal de $G$. Construya un contraejemplo de *a*).

3. Sea $A$ un dominio de integridad. Pruebe que $A$ es un dominio de factorización única si y sólo si todo elemento irreducible es un elemento primo y toda familia no vacía de ideales principales (ordenada por contención) satisface la *condición de la cadena ascendente*.

   **Observación:** La *condición de la cadena ascendente* establece, en este caso, que ninguna cadena ascendente de ideales principales puede prolongarse indefinidamente.

4. Pruebe que el polinomio $x^8 + yx^2 - x^2 + y^2 - 1$ es irreducible en el anillo de polinomios $\mathbb{Q}[x, y]$.

5. Sea $K/\mathbb{Q}$ una extensión finita de cuerpos. Pruebe que a lo más hay un número finito de raíces de la unidad en $K$.

6. Sea $F/\mathbb{Q}$ una extensión de cuerpos de grado 4 que **no** es una extensión de Galois y $K$ la clausura de Galois de $F$ sobre $\mathbb{Q}$.

   *a*) Pruebe que el grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$ es isomorfo a uno de los siguientes grupos:

      1) el grupo Simétrico $S_4$
      2) el grupo Alternante $A_4$
      3) el grupo Diédrico de 8 elementos $D_8$.

   *b*) Demuestre que $\mathrm{Gal}(K/\mathbb{Q})$ es isomorfo a $D_8$ si y sólo si la extensión $F/\mathbb{Q}$ contiene una extensión cuadrática de $\mathbb{Q}$.

# Responder dos problemas de cada sección.

**Sección I**

1. Muestre que si $f(x)$ es un polinomio irreducible sobre un cuerpo $k$, entonces todas sus raices tienen la misma multiplicidad.

2. Sea $a$ un elemento del cuerpo $k$ y $p \in \mathbb{Z}$ un primo. Supongamos que el polinomio $f(x) = x^p - a$ es reducible sobre $k$. Pruebe que $f(x)$ tiene una raiz en $k$.

3. Sea $K$ el cuerpo de descomposición de $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$. Determine el grupo de Galois de $K/\mathbb{Q}$ y describa su acción sobre las raices.

**Sección II**

1. Sea $(g, a) \mapsto ga$ una acción del grupo finito $G$ en el conjunto finito $A$ de orden $n > 1$. Sea $G_a$ el estabilizador de $a \in A$ en $G$ y sea $D := \{(a, b) \mid a \neq b\} \subset A \times A$.

   *a*) Muestre que $(g, a) \mapsto ga$ define una acción de $G_a$ en $A \setminus \{a\}$ y que $(g, (a, a_1)) \mapsto (ga, ga_1)$ define acciones de $G$ en $A \times A$ y en $D$.

   *b*) Supongamos que el orden de $A$ es al menos 3. Muestre que la acción de $G$ en $D$ es transitiva si y solo si la acción de $G_a$ en $A \setminus \{a\}$ es transitiva para todo $a \in A$. Muestre que en este caso $n(n-1)$ divide $|G|$.

2. Sea $G$ subgrupo del grupo simétrico $S_n$. Suponga que existe $g \in G$ tal que $sign(g) = -1$. Muestre que $G \cap A_n$ tiene índice dos en $G$ donde $A_n$ es el grupo alternante.

3. Demuestre que todo grupo $G$ de orden 325 es abeliano.

**Sección III**

1. Encuentre todos los anillos $R$ conmutativos con 1 que tienen un solo ideal maximal y cuyo grupo de unidades: $R^\times$ es trivial.

2. Sea $k$ un cuerpo y sea $R$ el subconjunto de $k[x]$ que consiste de los polinomios en el que el coeficiente de $x$ es 0. Pruebe que $R$ es un subanillo de $k[x]$. Pruebe que $R$ no es un dominio de factorización única.

3. Sea $k$ un cuerpo $x$ una indeterminada, $f, g, h$ polinomios cuadraticos en $k[x]$. Supongamos que $f$ tiene dos raices distintas en $k, g$ tiene exactamente una raiz en $k$ y finalmente supongamos que $h$ es irreducible en $k$. Pruebe que:

   *a*) Los anillos $k[x]/(f)$ y $k \oplus k$ son isomorfos.

   *b*) Los anillos $k[x]/(g)$ y $k[x]/(x^2)$ son isomorfos.

   *c*) los anillos $k[x]/(f), k[x]/(g)$ y $k[x]/(h)$ son todos no isomorfos.

Universidad de Talca
Instituto de Matemática y Física

# Examen de calificación: álgebra

Enero 2011
6 ejercicios
Tiempo: 3 horas

1. *a*) Sea $G := S_5$ el grupo simétrico sobre $\{1, 2, 3, 4, 5\}$ y sea $H$ un subgrupo de $G$ de Sylow-2. Demuestre que $H$ es isomorfo a $D_8$, el grupo dihedral de 8 elementos.

   *b*) Encuentre todos los grupos (modulo isomorfismo) de orden $2p$, donde $p \geq 2$ es un número primo.

2. Sea $A$ un anillo unital comutativo y sea $\mathfrak{P}$ un ideal primo de $A$. Sea $\mathfrak{P}A[X]$ el ideal en $A[X]$ generado por $\mathfrak{P}$. Demuestre que

   *a*) $\mathfrak{P}A[X] = \{\sum_i^n a_i X^i | n \in \mathbb{N}, a_i \in \mathfrak{P}\}$

   *b*) $\mathfrak{P}A[X]$ es un ideal primo de $A[X]$.

   *c*) Muestre que $\mathfrak{P}A[X]$ no es un ideal maximal de $A[X]$.

3. Sea $A$ un anillo unital comutativo y sean $\mathfrak{P}_i, i = 1, \ldots, k$ ideales primos de $A$ tal que también $\mathfrak{P}_1 \cap \ldots \cap \mathfrak{P}_k$ sea ideal primo de $A$. Demuestre que existe $j$ tal que $\mathfrak{P}_j \subset \mathfrak{P}_i$ para todo $i$.

4. Sea $\mathfrak{P}$ un ideal primo no cero del anillo de los enteros de Gauss $\mathbb{Z}[i]$. Muestre que el anillo cuociente $\mathbb{Z}[i]/\mathfrak{P}$ es un cuerpo finito. Mas aún muestre que los únicos cuerpos que se pueden obtener tienen $p$ ó $p^2$ elementos, donde $p \in \mathbb{Z}$ es un primo.

5. Encuentre todos los grupos abelianos de orden 8 (modulo isomorfismo). Para cada uno de los siguientes identifique el grupo correspondiente.

   *a*) $(\mathbb{Z}_{15})^\times$,
   *b*) $(\mathbb{Z}_{17})^\times/\{\pm 1\}$,
   *c*) Las raices de $x^8 - 1$ en $\mathbb{C}$,
   *d*) $\mathbb{F}_8^+$,
   *e*) $(\mathbb{Z}_{16})^\times$.

   Aquí $\mathbb{F}_8$ denota el cuerpo con 8 elementos y $\mathbb{F}_8^+$ su grupo aditivo subyacente; $\mathbb{Z}_n$ denota el anillo cuociente $\mathbb{Z}/n\mathbb{Z}$ y $R^\times$ el grupo de elementos invertibles del anillo $R$.

6. Sea $D \in \mathbb{Z}$, $D \neq 1$, un entero libre de cuadrados (i.e. no hay $m \in \mathbb{Z}, m \neq \pm 1$ tal que $m^2 | D$) y $a \in \mathbb{Q}$ un racional distinto de 0. Suponga que $\mathbb{Q}(\sqrt{a\sqrt{D}})/\mathbb{Q}$ es una extensión de Galois. Pruebe que $D = -1$ y que $\mathrm{Gal}(\mathbb{Q}(\sqrt{a\sqrt{D}})/\mathbb{Q}) \cong K_4$ o $C_2$ (el grupo Klein 4 o el grupo cíclico con 2 elementos respectivamente.) ¿Para que valores de $a$ el grupo de Galois es $K_4$ y para cuales $C_2$?

# Responder dos problemas de cada sección.

**Sección I**

1. Sea $K$ una extension cuadratica de $\mathbb{Q}$, es decir $[K : \mathbb{Q}] = 2$. Supongamos que $f(x) \in \mathbb{Q}[x]$ es un polinomio irreducible. Pruebe que solo una de las siguientes posibilidades sucede:

   *a*) $f(x)$ es irreducible sobre $K[x]$

   *b*) $f(x)$ es un producto de dos factores irreducibles en $K[x]$ del mismo grado.

2. Consideremos $\zeta_5 = \mathrm{e}^{2\pi i/5} \in \mathbb{C}$.

   *a*) Describa el grupo de Galois, $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ y su acción en $\mathbb{Q}(\zeta_5)$.

   *b*) Determinando el polinomio minimal de $\cos(2\pi/5)$ encuentre una expresión algebraica para $\cos(2\pi/5)$.

3. Sea $\alpha = \sqrt{5 + 2\sqrt{5}}$. Muestre que $\mathbb{Q}(\alpha)$ es una extensión de Galois de grado 4 sobre $\mathbb{Q}$ con grupo de Galois ciclico.

**Sección II**

1. Sea $p$ un número primo y $G$ un grupo no abeliano de orden $p^3$

   *a*) Pruebe que el centro de $G$, $Z(G)$ y el conmutador de $G$ coinciden y son de orden $p$

   *b*) Pruebe que $G/Z(G) \cong C_p \times C_p$ donde $C_p$ denota el grupo ciclico con $p$ elementos.

2. Sea $G$ un grupo finito y $H$ un subgrupo normal. Muestre que si $P$ es un $p$-subgrupo de Sylow de $H$ entonces $G = HN_G(P)$

3. Sea $G$ un grupo finito, $H \trianglelefteq G$ y $N \trianglelefteq H$.

   *a*) De un contraejemplo para mostrar que no necesariamente se tiene $N \trianglelefteq G$.

   *b*) Supongamos que $|N|$ (el orden de $N$) y el indice de $N$ en $H$ son relativamente primos. Pruebe que $N$ es el único subgrupo de $H$ de orden $|N|$. Concluya que $N \trianglelefteq G$.

**Sección III**

1. Sea $R$ un anillo conmutativo unital, $P \subset R$ un ideal primo y suponga que $R/P$ es finito. demuestre que $P$ es un ideal maximal.

2. Considere el ideal principal $I$ generado por el polinomio $x^3 + x + 1$ en el anillo $\mathbb{Z}[x]$. Muestre que $I$ **no** es un ideal maximal. Encuentre un ideal maximal $J \subset \mathbb{Z}[x]$ que contenga $I$.

3. Sea $I \subset R$ un ideal en un anillo unital y $\pi : R \longrightarrow R/I$ el homomorfismo canonico. Suponga que para todo $x \in I$ hay un entero positivo $n$ (que depende de $x$) tal que $x^n = 0$. Demuestre que $r \in R$ es invertible si y solo si $\pi(r) \in R/I$ es invertible.