Soluciones resumidas del examen de Matemática Discreta 2 - Curso 2006 - IMERL

Miércoles 27 de diciembre de 2006

Ejercicio 1.

(1) Ver teórico.

(2) Como $mcd(a,b) = 13$, sean a' y b' tales que $a = 13a'$ y $b = 13b'$ con $mcd(a',b') = 1$. Entonces $169(a'^2 + b'^2) = 14365$, es decir $a'^2 + b'^2 = 85$ $(*)$, luego:
Si $a' = 1$, no existe b' entero que verifique la igualdad (*); Si $a' = 2$ entonces $b' = 9$;
Si $a' = 3$, no existe b' entero que verifique la igualdad (*); Si $a' = 4$, no existe b' entero que verifique (*);
Si $a' = 5$, no existe b' entero que verifique la igualdad (*); Si $a' = 6$ entonces $b' = 7$.
Las soluciones son: $(26, 117), (78, 91), (117, 26)$ y $(91, 78)$.

Ejercicio 2.

(1) $\big(A[i], +\big)$ es grupo abeliano: $+$ es asociativo: $\big[(a+bi)+(c+di)\big]+(e+fi) = \big(a+c+(b+d)i\big)+(e+fi) = \big(((a+c)+e\big)+\big((b+d)+f\big)i\big) = \big((a+(c+e)\big)+\big(b+(d+f)\big)i\big) = (a+bi)+\big[(c+e)+(d+f)i\big] = (a+bi)+\big[(c+di)+(e+fi)\big]$
Existe neutro aditivo: Si z es el neutro del anillo A entonces $z+zi$ es el neutro aditivo de $A[i]$ pues, $(a+bi)+(z+zi) = (a+z)+(b+z)i = a+bi; (z+zi)+(a+bi) = (z+a)+(z+b)i = a+bi.$
Existencia opuesto: $a+bi$ tiene opuesto que es $-a-bi$: $(a+bi)+(-a-bi) = (a-a)+(b-b)i = z+zi(-a-bi)+(a+bi) = (-a+a)+(-b+b)i = z+zi.$
$+$ es conmutativo: $(a+bi)+(c+di) = (a+c)+(b+d)i = (c+a)+(d+b)i = (c+di)+(a+bi)$
$\star$ es asociativa: $\big[(a+bi)\star(c+di)\big]\star(e+fi) = \big[(ac-bd)+(ad+bc)i\big]\star(e+fi) = \big[(ac-bd)e-(ad+bc)f\big]+\big[(ac-bd)f+(ad+bc)e\big]i = (ace-bde-adf-bcf)+(acf-bdf+ade+bce)i$ $(a+bi)\star\big[(c+di)\star(e+fi)\big] = (a+bi)\star\big[(ce-df)+(cf+de)i\big] = \big[a(ce-df)-b(cf+de)\big]+\big[a(cf+de)+b(ce-df)\big]i = (ace-adf-bcf-bde)+(acf+ade+bce-bdf)i.$
$\star$ es conmutativo : $(a+bi)\star(c+di) = (ac-bd)+(ad+bc)i = (ca-db)+(cb+da) = (c+di)\star(a+bi).$
Distributivas: Alcanza probar una pues ya vimos que $\star$ es conmutativo $\big[(a+bi)+(c+di)\big]\star(e+fi) = \big[(a+c)+(b+d)i\big]\star(e+fi) = \big[(a+c)e-(b+d)f\big]+\big[(a+c)f+(b+d)e\big]i = (ae+ce-bf-df)+(af+cf+be+de)i(a+bi)\star(e+fi)+(c+di)\star(e+fi) = \big[(ae-bf)+(af+be)i\big]+\big[(ce-df)+(cf+de)\big]i = (ae-bf+ce-df)+(af+be+cf+de)i.$
$A[i]$ tiene elemento unidad : Si u es el elemento unidad de A entonces $u+zi$ es elemento unidad de $A[i]$ $(a+bi)\star(u+zi) = (au-bz)+(bu+az)i = au+bui = a+bi$ y $(u+zi)\star(a+bi) = a+bi.$

(2) En $\mathbb{Z}_2[i]$ se tiene que $(1+i)\times(1+i) = (1-1)+(1+1)i = 0+0i$ por lo que $\mathbb{Z}_2[i]$ no es dominio de integridad y por lo tanto no es cuerpo.
En $\mathbb{Z}_3[i]$ hay 9 elementos : $0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i$. Tenemos: $1\times 1 = 1$; $2\times 2 = 1$; $i\times 2i = -2 = 1$; $(1+i)\times(2+i) = (2-1)+(2+1)i = 1+0i = 1(1+2i)\times(2+2i) = (2-4)+(4+2)i = -2+0i = 1$.Por tanto el inverso de 1 es 1, el de 2 es 2, el de i es 2i y recíprocamente, el de $1+i$ es $2+i$ y recíprocamente y el de $1+2i$ es $2+2i$ y recíprocamente. Así, todos los elementos de $\mathbb{Z}_3[i]$ excepto 0 tienen inverso multiplicativo por lo que es cuerpo.

(3) Si $(a+bi)\in M$ y $(c+di)\in M$, entonces $3|a, 3|b, 3|c$ y $3|d$; por lo tanto $3|(a+c)$ y $3|(b+d)$, con lo que $(a+c)+(b+d)i\in M$ y entonces $(a+bi)+(c+di)\in M$. Si $(a+bi)\in M$ entonces $3|a, 3|b$ por lo que $3|(-a)$, $3|(-b)$ y entonces $-a-bi\in M$ Si $(a+bi)\in M$ y $c+di\in\mathbb{Z}[i]$ entonces $3|a, 3|b$ y por tanto $3|(ac-bd)$ y $3|(ad+bc)$ con lo que $(a+bi)\star(c+di)\in M$. Como el producto es conmutativo $(c+di)\star(a+bi)\in M$. Por todo lo anterior se tiene que M es ideal de $\mathbb{Z}[i]$.

(4) La aplicación $f : \mathbb{Z}[i]\to\mathbb{Z}_3[i]$ definida por $f(a+bi) = [a]_3+[b]_3 i$, donde $[\ ]_3$ denota la clase módulo 3 de un entero, es un homomorfismo de anillos que es sobreyectivo con $Ker(f) = M$.
$f\big((a+bi)+(c+di)\big) = f\big((a+c)+(b+d)i\big) = [a+c]_3+[b+d]_3 i = [a]_3+[c]_3+[b]_3 i+[d]_3 i = \big([a]_3+[b]_3 i\big)+\big([c]_3+[d]_3 i\big) = f(a+bi)+f(c+di).$
$f\big((a+bi)x(c+di)\big) = f\big((ac-bd)+(ad+bc)i\big) = [ac-bd]_3+[ad+bc]_3 i = \big([a]_3[c]_3-[b]_3[d]_3\big)+\big([a]_3[d]_3+[b]_3[c]_3\big)i = \big([a]_3+[b]_3 i\big)\times\big([c]_3+[d]_3 i\big) = f(a+bi)\times f(c+di)$. Por el Primer Teorema del Homomorfismo para anillos se tiene que $\mathbb{Z}[i]/M$ es isomorfo a $\mathbb{Z}_3[i]$, que es un cuerpo. Como $\mathbb{Z}[i]$ es anillo conmutativo con unidad se tiene entonces que M es ideal maximal de $\mathbb{Z}[i]$.

Ejercicio 3.
(1) Como $|G| = pq$, por el primer teorema de Sylow, existe un subgrupo $S_p = H$ con $|H| = p$. La cantidad de tales subgrupos es $n_p = 1 + kp$, $k \in \mathbb{N}$ y tiene que dividir a q. Como $p > q$ entonces si $k > 0$, se tiene que $1 + kp > q$, luego $k = 0$, $n_p = 1$ y H es normal en G.

(2) (a) Sea G un grupo con $91 = 7 \times 13$ elementos. Entonces existen subgrupos de Sylow S_7 y S_{13} con 7 y 13 elementos respectivamente. Por la parte (1), existe un único subgrupo S_{13} con 13 elementos y se prueba también de la misma manera que existe un único subgrupo S_7 ya que $1 + k7$ debe dividir a 13 y como 13 es primo, necesariamente $k = 0$ y $n_7 = 1$. Además $S_7 \cap S_{13} = \{e_G\}$ (justificarlo) y si H es otro subgrupo de G entonces el orden de H debe dividir al orden de G. Por lo tanto los únicos subgrupos de G son $\{e_G\}, S_7, S_{13}$ y G.
(b) Los subgrupos S_7 y S_{13} son ambos normales. Consideremos $T = S_{13}S_7$. Al ser normales S_{13} y S_7, T es un subgrupo de G. Además $T \simeq S_{13} \times S_7$ porque además de ser normales, S_{13} y S_7 tienen intersección trivial, es decir, $S_{13} \cap S_7 = \{e_G\}$.
Por otro lado $|T| = |S_{13}S_7| = \frac{|S_{13}||S_7|}{|S_{13} \cap S_7|} = 13 \times 7 = 91$ pues $S_{13} \cap S_7 = \{e_G\}$. Luego $G \equiv S_{13} \times S_7$ es el producto directo de dos grupos abelianos, es decir G es abeliano.

Ejercicio 4.
(1) Si $P = \sum\limits_{i=0}^{m} a_i x^i \in \mathbb{Z}[x]$ tiene una raíz α en $\mathbb{Z}$, entonces $P(\alpha) = \sum\limits_{i=0}^{m} a_i \alpha^i = 0$, luego tomando clase módulo n, se tiene que $\big[P(\alpha)\big] = \left[\sum\limits_{i=0}^{m} a_i \alpha^i\right] = [0]$, es decir

$$\big[P(\alpha)\big] = \left[\sum_{i=0}^{m} a_i \alpha^i\right] = \sum_{i=0}^{m} \big[a_i \alpha^i\big] = \sum_{i=0}^{m} \big[a_i\big] \big[\alpha\big]^i = \big[P\big]\big([\alpha]\big) = [0].$$

Entonces si $P \in \mathbb{Z}[x]$ tiene una raíz $\alpha \in \mathbb{Z}$, el polinomio $[P](x) = \sum\limits_{i=0}^{m} [a_i] x^i \in \mathbb{Z}_n[x]$ tiene una raíz $[\alpha]$ en $\mathbb{Z}_n$ para todo n.

Si $P(0)$ y $P(1)$ son impares entonces $\big[P\big]\big([0]\big) = [1]$ y $\big[P\big]\big([1]\big) = [1]$ en $\mathbb{Z}_2$, entonces $[P]$ no tiene raíz en $\mathbb{Z}_2$, luego P no tiene raíz en $\mathbb{Z}$.

(2) Si n no divide a ninguno de $P(0), P(1), \ldots, P(n-1)$ entonces $[P]\big([0]\big) \neq [0], [P]\big([1]\big) \neq [0], \ldots, [P]\big([n-1]\big) \neq [0]$ en $\mathbb{Z}_n$ y $[P]$ no tiene raíz en $\mathbb{Z}_n$, luego P no tiene raíz en $\mathbb{Z}$.