Padova, 15 dicembre 2005

Appello di Algebra

Esercizio 1

Nel gruppo simmetrico Σ_n si consideri il ciclo $\gamma = (12 \dots n)$.
a) Si provi che la classe di coniugio di γ in Σ_n ha $(n-1)!$ elementi.
b) Si provi che il centralizzante $C(\gamma)$ in Σ_n è $< \gamma >$.
c) Sia $\sigma = (123)(456) \in \Sigma_6$. È vero che $C(\sigma) =< \sigma >$?

a) I coniugati di γ sono i cicli di lunghezza n che sono appunto $(n-1)!$ (le liste $(a_1, a_2, \dots, a_n)$ di elementi distinti in $\{1, \dots, n\}$ sono $n!$ e le n liste che si ottengono da una di queste permutando circolarmente danno lo stesso ciclo).
b) L'ordine di $C(\gamma)$ per il suo indice in Σ_n dà l'ordine $n!$ di Σ_n. L'indice del centralizzante è l'ordine $(n-1)!$ della classe di coniugio; quindi $|C(\gamma)| = n$. D'altra parte $C(\gamma)$ contiene $\langle\gamma\rangle$ che ha ordine n e si conclude che sono uguali.
c) Si controlla subito che per esempio $(123) \in C(\sigma)$ ma $(123) \notin \langle\sigma\rangle$.

Esercizio 2

Sia $u = \dfrac{1-\sqrt{3}}{\sqrt[4]{3}}$.
a) Si verifichi che $\mathbb{Q}(u^2) = Q(\sqrt{3})$.
b) Si determini il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
c) È vero che $Q(u) = Q(\sqrt[4]{3})$?
d) Si verifichi che $\mathbb{Q}(u)$ non è campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

a),b),c) Poichè $\sqrt{3} = (\sqrt[4]{3})^2$ è intanto $Q(u) \subseteq Q(\sqrt[4]{3})$. Quadrando $\sqrt[4]{3}\cdot u = 1-\sqrt{3}$ si ottiene $\sqrt{3}\cdot u^2 = 4-2\sqrt{3}$, $\quad \sqrt{3}(u^2+2) = 4$ e quindi $\sqrt{3} = \dfrac{4}{u^2+2} \in Q(u^2)$ e anche $u^2 = \dfrac{4-2\sqrt{3}}{\sqrt{3}} \in Q(\sqrt{3})$. Ancora, da $\sqrt{3} \in Q(u^2)$ segue $\sqrt[4]{3} = \dfrac{1-\sqrt{3}}{u} \in Q(u)$. Così il grado $[Q(u) : Q] = [Q(\sqrt[4]{3}) : Q] = 4$. Quadrando ancora si ha $3(u^2+2)^2 = 16$, $\quad 3u^4 + 12u^2 - 4 = 0$. Dal discorso sui gradi si conclude che il polinomio minimo di u su Q è $f(x) = x^4 + 4x^2 - 4/3$.
d) $f(x)$ è biquadratico ed è facile vedere che non tutte le sue radici sono reali, mentre $Q(u) \subseteq R$. Per informazioni più precise sul campo di spezzamento, si può osservare che se si sostituisce $i\sqrt[4]{3}$ a $\sqrt[4]{3}$ e il suo quadrato $-\sqrt{3}$ a $\sqrt{3}$ si ottiene un altro zero $v = \dfrac{1+\sqrt{3}}{i\sqrt[4]{3}}$ di $f(x)$.

Esercizio 3

Sia D un dominio a ideali principali.
a) Provare che ogni ideale primo non nullo di D è massimale.
b) Sia R un dominio di integrità e sia $f\colon D \to R$ un epimorfismo d' anelli. Provare che f è un isomorfismo oppure R è un campo.
c) Provare che se $D[x]$ è un dominio a ideali principali, allora D è un campo.

a) Si veda il testo.
b) $\operatorname{Ker} f$ è primo perchè $D/\operatorname{Ker} f$ è un dominio d'integrità. Se $\operatorname{Ker} f = 0$ f è iniettivo. Se $\operatorname{Ker} f \neq 0$, $\operatorname{Ker} f$ è massimale e $R \cong D/\operatorname{Ker} f$ è un campo.
c) Sia $f\colon D[x] \to D$ la valutazione in 0 (manda ogni polinomio nel suo termine noto). È suriettivo ma non iniettivo. Da b) segue il risultato.

Esercizio 4

Sia K un sottogruppo del gruppo G. K si dice caratteristico in G se risulta $f(K) = K$ per ogni automorfismo f di G.
Si verifichi che:
a) se K è caratteristico in G, allora K è normale in G,
b) per ogni gruppo G il centro $Z(G)$ è caratteristico in G.
c) Si provi con un esempio che non ogni sottogruppo normale è caratteristico.

a) Per ogni $g \in G$ la mappa $i_g : G \to G, \quad x \mapsto gxg^{-1}$ è un automorfismo di G e per ogni sottogruppo H di G è $i_g(H) = gHg^{-1}$. Se K è caratteristico in G è allora $gKg^{-1} = i_g(K) = K$, cioè $K \trianglelefteq G$.
b) $x \in Z(G)$ se e solo se $xg = gx$ per ogni $g \in G$. Se $x \in Z(G)$ e f è un automorfismo di G allora $f(x)f(g) = f(g)f(x)$ per ogni $f(g)$, ma f è suriettiva, quindi $f(x)y = yf(x)$ per ogni $y \in G$ e $f(x) \in Z(G)$. Questo dice $f(Z(G)) \subseteq Z(G)$. L'altra inclusione si ottiene usando l'automorfismo f^{-1}.
c) Un esempio facile: nel gruppo additivo Q dei razionali tutti i sottogruppi sono normali perchè è commutativo e le moltiplicazioni per numeri razionali non nulli sono automorfismi. Allora $Z \trianglelefteq Q$ ma $(1/2)Z \neq Z$ e quindi Z non è un sottogruppo caratteristico di Q.

Esercizio 5

Sia $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.
Sia ϕ: $\mathbb{Z}[\sqrt{5}] \to \mathbb{Z}/11\mathbb{Z}$ definito da $\phi(a + b\sqrt{5}) = \overline{a + 4b}$.
a) Verificare che ϕ è omomorfismo d'anelli e che $(11, 4 - \sqrt{5}) \subseteq \operatorname{Ker}\phi$.
b) Osservando che $11 = (4 - \sqrt{5})(4 + \sqrt{5})$, provare che $\operatorname{Ker}\phi = (4 - \sqrt{5})$.
c) Verificare che 11 è elemento riducibile in $\mathbb{Z}[\sqrt{5}]$. 11 è primo in $\mathbb{Z}[\sqrt{5}]$?

a) I controlli che ϕ rispetti la somma e che $\phi(1)$ sia l'unità del codominio sono immediati. Per il prodotto

$$\phi((a + b\sqrt{5})(c + d\sqrt{5})) = \phi(ac + 5bd + (ad + bc)\sqrt{5}) = \overline{ac + 5bd + 4(ad + bc)}$$

$$\phi(a+b\sqrt{5})\phi(c+d\sqrt{5}) = \overline{a + 4bc + 4d} = \overline{ac + 16bd + 4ad + 4bc} = \overline{ac + 5bd + 4(ad + bc)}.$$

E poi $\phi(11) = \overline{11} = 0$ e $\phi(4 - \sqrt{5}) = \overline{4 - 4} = 0$.
b) Certo $\operatorname{Ker}\phi \supseteq (4 - \sqrt{5})$. E se $a + b\sqrt{5} \in \operatorname{Ker}\phi$ allora $\overline{a + 4b} = \overline{0}$ cioè $a + 4b = 11k$ con $k \in Z$, $a + b\sqrt{5} = -4b + 11k + b\sqrt{5} = -b(4 - \sqrt{5}) + k(4 - \sqrt{5})(4 + \sqrt{5}) \in (4 - \sqrt{5})$.
c) 11 è divisibile per $4 - \sqrt{5}$ che non è invertibile perchè genera un ideale proprio e non è un suo associato (11 non lo divide). Non essendo irriducibile non è nemmeno primo.

Esercizio 6

Sia D un dominio a fattorizzazione unica.
a) Si completi la definizione: $f(x) \in D[x]$ è primitivo se . . . .
b) Si dimostri che se $f, g \in D[x]$ sono primitivi, allora fg è primitivo.

Si veda il testo.