Soluzioni esame scritto di ALGEBRA II
25 giugno 2013

Esercizio 1. Sia G un gruppo.

1. Siano M, N sottogruppi normali di G; si provi che se G/N e G/M sono abeliani allora $G/(N \cap M)$ è abeliano.

2. Siano $H \leq G$ e $N \trianglelefteq G$; si provi che se G/N è abeliano allora $H/(H \cap N)$ è abeliano.

soluzione 1. È noto che, poiché N ed M sono sottogruppi normali di G anche $N \cap M$ è un sottogruppo normale di G. Siano $x, y \in G$. Poiché, per ipotesi, G/N è abeliano si ha,

$$(xy)N = xN \cdot yN = yN \cdot xN = (yx)N$$

e dunque

$$(xy)^{-1}(yx) \in N.$$

Analogamente, da G/M abeliano segue $(xy)^{-1}(yx) \in M$. Quindi

$$(xy)^{-1}(yx) \in N \cap M.$$

Pertanto, risvolgendo il prodotto,

$$x(N \cap M) \cdot y(N \cap M) = xy(N \cap M) = yx(N \cap M) = y(N \cap M) \cdot x(N \cap M),$$

il che prova che il quoziente $G/(N \cap M)$ è abeliano.

2. Poiché $N \trianglelefteq G$, $N \leq HN \leq G$. Dal secondo Teorema di omomorfismo segue poi

$$\frac{H}{H \cap N} \simeq \frac{HN}{N} \leq \frac{G}{N}.$$

Essendo isomorfo ad un sottogruppo di un gruppo abeliano, $H/(H \cap N)$ è quindi abeliano.

Esercizio 2. Sia G un gruppo di ordine 231.

1. si provi che esiste un omomorfismo non banale $G \to C_3$ (dove C_3 è un gruppo ciclico di ordine 3);

2. si provi che G contiene un elemento di ordine 77;

3. si provi che se G contiene un sottogruppo ciclico e normale di ordine 21 allora G è ciclico.

soluzione Preliminarmente, si osserva che $|G| = 231 = 11 \cdot 7 \cdot 3$; quindi, posto, per ciascun primo p, n_p il numero di p-sottogruppi di Sylow di G, dal teorema di Sylow segue

$$n_{11} \equiv 1 \pmod{11} \quad \text{e} \quad n_{11} | 21$$

da cui $n_{11} = 1$. Similmente si ricava

$$n_7 = 1, \qquad n_3 \in \{1, 7\}.$$

1. Siano P l'unico 11-sottogruppo di Sylow di G e T l'unico 7-sottogruppo di Sylow di G. Allora $P \trianglelefteq G$ e $T \trianglelefteq G$; quindi $N = PT \trianglelefteq G$. Inoltre $|N| = |P||T| = 77$ e, per il teorema di Lagrange, $[G : N] = 3$. Dunque, G/N è un gruppo ciclico di ordine 3 (cioè $G/N \simeq C_3$) e la proiezione canonica $G \to G/N$ è l'omomorfismo cercato.

2. Con le notazione del punto precedente si ha $N = P \times T$. Poiché P e T sono ciclici (in quanto gruppi di ordine primo) ed hanno ordine coprimo, N è ciclico per un fatto noto. Un generatore di N è l'elemento cercato.

3. Supponiamo che G contenga un sottogruppo normale K, con K ciclico di ordine 21. Allora (con le notazioni dei punti precedenti), $K \cap P = 1$ e $KP = G$. Quindi $G = K \times P$ è un podotto diretto (interno) di gruppi cic;lici di ordine coprimo e dunque è esso stesso un gruppo ciclico.

Esercizio 3. Posto $u = \sqrt[3]{2} \in \mathbb{R}$:

1. si determini il polinomio minimo f di u su $\mathbb{Q}$;
2. si dica se $\mathbb{Q}[u] = \mathbb{Q}[\sqrt[3]{2}]$;
3. posto E il campo di spezzamento di f su $\mathbb{Q}$, si determini $Gal(E|\mathbb{Q})$;
4. posto $L = E \cap \mathbb{R}$, si determini $[L : \mathbb{Q}]$.

soluzione 1. Calcolando:

$$u^3 = 4 + 3\sqrt[3]{4^2}\sqrt[3]{2} + 3\sqrt[3]{4}\sqrt[3]{2^2} + 2 = 6 + 6\sqrt[3]{4} + 6\sqrt[3]{2} = 6 + 6u.$$

Quindi, u è radice del polinomio

$$f = x^3 - 6x - 6,$$

che è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein (oppure verificando direttamente che non ha radici intere). Pertanto f è il polinomio minimo di u su $\mathbb{Q}$. In particolare, $[\mathbb{Q}[u] : \mathbb{Q}] = 3$.

2. Poiché $u = \sqrt[3]{2} + (\sqrt[3]{2})^2 \in \mathbb{Q}[\sqrt[3]{2}]$, si ha $\mathbb{Q}[u] \subseteq \mathbb{Q}[\sqrt[3]{2}]$. Siccome poi

$$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3 = [\mathbb{Q}[u] : \mathbb{Q}]$$

dalla formula dei gradi segue $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}[u]] = 1$, ovvero $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[u]$.

3. Lo studio della sua derivata mostra che la funzione reale associata ad f ha un solo massimo locale nel punto di ascissa $-\sqrt{2}$, nel quale la funzione vale $f(\sqrt{2}) = 4\sqrt{2} - 6 < 0$. L'esame del grafico mostra quindi che la funzione incrocia l'asse delle ascisse in un solo punto, ovvero che il polinomio f ha una sola radice reale, che è u. In particolare, poiché $\mathbb{Q}[u] \subseteq \mathbb{R}$, si ha $E \neq \mathbb{Q}[u]$, ovvero

$$[E : \mathbb{Q}] > [\mathbb{Q}[u] : \mathbb{Q}] = \deg f = 3.$$

Poiché sappiamo, dalla teoria, che $[E : \mathbb{Q}]$ divide $(\deg f)! = 6$, si conclude che $[E : \mathbb{Q}] = 6$. Siccome E
Q è un'estensione di Galois, posto $G = Gal(E|\mathbb{Q})$, si conclude che $|G| = 6$. Inoltre G opera fedelmente sull'insieme delle 3 radici di f, e dunque è isomorfo ad un sottogruppo di S_3; pertanto $G \simeq S_3$.

4. $L := E \cap \mathbb{R}$ è un sottocampo di E che contiene $\mathbb{Q}[u]$. Poiché, per la formula dei gradi, $[E : \mathbb{Q}[u]] = 2$, si ha $L = E$ oppure $L = \mathbb{Q}[u]$. Siccome E non è contenuto in $\mathbb{R}$ (dato che E contiene le radici non reali di f) si deve avere $L = \mathbb{Q}[u]$.

Esercizio 4.

1. Siano E un campo di ordine 32 e F il suo sottocampo fondamentale; si dica quanti sono i campi intermedi tra F ed E.

2. Sia f un fattore irriducibile del polinomio $x^{32} - x$ in $\mathbb{Z}/2\mathbb{Z}[x]$; si provi che $f = x$, $f = x - 1$ oppure $\deg(f) = 5$.

soluzione. 1. Poichè $|E| = 32 = 2^5$, la caratteristica di E è 2 e quindi $F = \mathbb{Z}/2\mathbb{Z}$. Allora

$$[E : F] = 5 \tag{1}$$

(infatti, se $d = [E : \mathbb{Z}/2\mathbb{Z}]$ allora E, come $Z/2\mathbb{Z}$-spazio vettoriale, è isomorfo allo spazio delle d-uple $(Z/2\mathbb{Z})^d$, e dunque ha ordine 2^d; dal confronto degli

ordini si ricava la (1). Dalla formula dei gradi segue quindi che i soli campi intermedi tra F ed E sono F ed E stessi.

2. Sia f un fattore irriducibile di $g = x^{32} - x \in \mathbb{Z}/2\mathbb{Z}[x]$. Ora, come sappiamo dalla teoria, l'insieme delle radici di g costituisce un campo E di ordine $2^5 = 32$. Se $b \in E$ è una radice di f (c'è perché le radici di f sono radici di g), allora $f[b]$ è un campo intermedio tra $\mathbb{Z}/2\mathbb{Z}$ ed E. Dal punto 1. si conclude che

$$\deg f = [F[b] : \mathbb{Z}/2\mathbb{Z}] \in \{1, 5\}.$$