Traccia del 13 novembre 2020

1.

(a) Osserviamo preliminarmente che i cicli associati ad una permutazione, essendo a due a due disgiunti, commutano a due a due. Quindi ogni ciclo commuta tutti i cicli associati alla permutazione, e dunque commuta anche con il loro prodotto, ossia con la permutazione stessa. Se la permutazione σ ha, tra i suoi cicli associati, un ciclo γ_1 di lunghezza 2 ed un ciclo γ_2 di lunghezza 4, entrambi, insieme alle loro potenze, apparterranno dunque a $C(\sigma)$. Ora: γ_1^2 e γ_2 sono entrambi elementi di $C(\sigma)$ aventi periodo 2, e sono evidentemente distinti. Ma ciò è impossibile in un gruppo ciclico. Dunque $C(\sigma)$ non è ciclico.

(b) Una permutazione che appartenga all'intersezione, commutando con entrambe le permutazioni $(1,2,3)$ e $(4,5)$, commuta con il loro prodotto, ossia con σ. Viceversa, se una permutazione commuta con σ, allora commuta con ogni sua potenza, in particolare con $(1,2,3)=\sigma^4$ e con $(4,5)=\sigma^3$.

2.

(a) Un omomorfismo siffatto è definito da $([a]_n,[b]_m)\mapsto[ma]_{nm}$. Si verificano facilmente la buona definizione e la conservazione della somma. La sua immagine è il sottogruppo ciclico di $\mathbb{Z}_{nm}$ generato da $[m]_{nm}$, il cui ordine è n. Essendo $1<n<nm$, ciò prova che l'omomorfismo non è banale, né surgettivo.

(b) Gli elementi invertibili dell'anello $\mathbb{Z}_n\times\mathbb{Z}_m$ sono le coppie del tipo (α,β), ove α è invertibile in $\mathbb{Z}_n$ e β è invertibile in $\mathbb{Z}_m$. Tali elementi sono $\phi(n)\phi(m)$, essendo ϕ la funzione toziente di Eulero. Sono tutti elementi regolari. I restanti elementi sono le coppie in cui uno dei due elementi è zero oppure è non nullo e non invertibile: in tal caso la coppia è l'elemento zero oppure è un divisore dello zero (in quanto in $\mathbb{Z}_n$ e in $\mathbb{Z}_m$ ogni elemento non nullo e non invertibile è divisore dello zero). Ciò prova che gli elementi regolari dell'anello $\mathbb{Z}_n\times\mathbb{Z}_m$ sono tutti e soli gli elementi invertibili. Quindi i divisori dello zero sono quelli non nulli e non invertibili, il cui numero è $nm-\phi(n)\phi(m)-1$.

(c) Se ad $\mathrm{Im}\psi$ appartenesse $[1]_{nm}$, vi apparterrebbe anche ogni suo multiplo, ossia si avrebbe $\mathrm{Im}\psi=\mathbb{Z}_{nm}$. In tal caso ψ sarebbe surgettivo, quindi bigettivo, ma ciò è impossibile, perché i gruppi di partenza ed arrivo non sono isomorfi. Se n ed m non sono coprimi, infatti, il gruppo $\mathbb{Z}_n\times\mathbb{Z}_m$, contrariamente a $\mathbb{Z}_{nm}$, non è ciclico, in quanto il periodo di ogni suo elemento è un divisore di $\mathrm{mcm}(n,m)<nm$.

3.

(a) Basta prendere $f(X)=(X-\alpha)(X-\overline{\alpha})=X^2-2\mathrm{Re}(\alpha)X+||\alpha||$, i cui coefficienti sono numeri razionali, visto che tutti gli α_k, e quindi anche il loro prodotto α, hanno parte reale e parte immaginaria intere. Il polinomio è irriducibile in $\mathbb{Q}[X]$ poiché di grado due e privo di radici reali (o anche perché soddisfa il criterio di Eisenstein con $p=2$).

(b) Basta prendere $g(X)=\prod_{k=0}^{n}(X-\alpha_k)\left(X-\overline{\alpha_k}\right)$.

.