Ariketak

3.1. Izan bedi $\varphi : A \longrightarrow B$ eraztun-isomorfismoa.

(i) Frogatu $a \in A$ elementua irreduziblea dela baldin eta soilik baldin $\varphi(a)$ irreduziblea bada. Egia da emaitza hori φ homomorfismoa besterik ez bada?

(ii) Ondorioztatu A faktorizazio bakarreko domeinua dela baldin eta soilik baldin B faktorizazio bakarreko domeinua bada.

(iii) Frogatu A ideal nagusietako domeinua dela baldin eta soilik baldin B ideal nagusietako domeinua bada, eta A domeinu euklidearra dela baldin eta soilik baldin B domeinu euklidearra bada.

3.2. Problema honetan $\mathbb{Z}/n\mathbb{Z}$ eraztunaren elementu irreduzibleak aurkitzen ditugu, $n \geq 2$ denean. Baldin eta n lehena bada, orduan $\mathbb{Z}/n\mathbb{Z}$ gorputza da, eta ez du elementu irreduziblerik. Beraz, n konposatua hartuko dugu hemendik aurrera.

(i) Dakigunez, irreduzibilitatea ez da aldatzen unitateez biderkatzean. Ondorioztatu nahikoa dela $\overline{a}$ elementu baten irreduzibilitatea aztertzea $a \mid n$ den kasuan. Egoera horretan, a ez bada lehena, orduan $\overline{a}$ ez da irreduziblea. Beraz, ondorengo ataletan $\overline{p}$ elementu baten irreduzibilitatea aztertuko dugu, $p \mid n$ izanik.

(ii) Baldin eta $p^2 \nmid n$ bada, frogatu $\overline{p}$ ez dela irreduziblea $\mathbb{Z}/n\mathbb{Z}$-n. (Laguntza: Idatzi $n = pm$, $\text{zkh}(p, m) = 1$ izanik. Orduan, existitzen da $a \in \mathbb{Z}$ non $am \equiv -1 \pmod{p}$ baita. Ikusi $\overline{p} = \overline{p} \cdot \overline{am+1}$ dela, eta faktorizazio horrek frogatzen duela $\overline{p}$ ez dela irreduziblea.)

(iii) Baldin eta $p^2 \mid n$ bada, frogatu $\overline{p}$ irreduziblea dela $\mathbb{Z}/n\mathbb{Z}$-n. (Laguntza: Demagun $\overline{p} = \overline{a} \cdot \overline{b}$ dela eta ikus dezagun faktoreetako bat unitatea dela $\mathbb{Z}/n\mathbb{Z}$-n. Izan ere, $n \mid ab - p$ dugu eta, hortik, $p \mid ab$ dugu. Orokortasuna galdu gabe, $p \mid a$ den kasuan jar gaitezke. Orduan, $n \mid ab - p$ erlaziotik $p \nmid b$ dela ondorioztatzen dugu. Antzera, $q \neq p$ n-ren beste zatitzaile lehen bat bada, orduan $q \nmid b$ dugu. Beraz, $\text{zkh}(b, n) = 1$ eta $\overline{b}$ $\mathbb{Z}/n\mathbb{Z}$-ren unitatea da.)

(iv) Laburbilduz, $\mathbb{Z}/n\mathbb{Z}$-ren elementu irreduzible elkartuen baliokidetasun-klase bakoitzeko ordezkari bat hartuta, multzo hau lortzen dugu:

$$\{\overline{p} \mid p \text{ zenbaki lehena } \mathbb{Z}\text{-n eta } p^2 \mid n\}.$$

Bereziki, n zenbaki karratugabea bada, orduan $\mathbb{Z}/n\mathbb{Z}$-n ez dago elementu irreduziblerik.

3.3. Aurreko probleman aipatu dugun azken emaitza, $\mathbb{Z}/n\mathbb{Z}$-n ez dagoela elementu irreduziblerik n karratugabea bada, ikuspegi aljebraikoago batetik frogatu daiteke, ariketa honetan ikusten dugun bezala.

(i) Izan bitez $K_1, \ldots, K_r$ gorputzak. Frogatu $K_1 \times \cdots \times K_r$ biderkadura cartesiarrak ez duela elementu irreduziblerik.

(ii) Izan bedi $n \in \mathbb{N}$, $n \geq 2$, zenbaki karratugabea. Erabili aurreko atala eta hondarraren teorema txinatarra frogatzeko $\mathbb{Z}/n\mathbb{Z}$-n ez dagoela elementu irreduziblerik.

3.4. Problema honen helburua da erabakitzea noiz den X indeterminatua irreduziblea $\mathbb{Z}/n\mathbb{Z}[X]$ eraztunean, $n \in \mathbb{N}$ izanik.

(i) Lehenengo eta behin, demagun $n = p^m$ dugula, p zenbaki lehena izanik. Frogatu X irreduziblea dela $\mathbb{Z}/n\mathbb{Z}[X]$-n. (Laguntza: Demagun $X = f(X)g(X)$ dela, $f, g \in \mathbb{Z}/n\mathbb{Z}[X]$ izanik, eta frogatu dezagun f edo g unitateak direla. Idatzi $f(X) = \sum_{i\geq 0} \overline{a_i}X^i$ eta $g(X) = \sum_{i\geq 0} \overline{b_i}X^i$. Baldin eta $\overline{a_0} = \overline{0}$ bada, erabili 1.6 ariketa g unitatea dela ondorioztatzeko. Beraz, simetriagatik, $\overline{a_0} \neq \overline{0}$ eta $\overline{b}_0 \neq \overline{0}$ den kasura pasa gaitezke. Orain, $X = f(X)g(X)$ baldintzatik

$$\overline{a_0} \cdot \overline{b_0} = \overline{0} \qquad \text{eta} \qquad \overline{a_0} \cdot \overline{b_1} + \overline{a_1} \cdot \overline{b_0} = \overline{1} \tag{3.6}$$

dela lortzen dugu. Ondorioztatu kontraesan bat, $n = p^m$ dela kontuan hartuz.)

(ii) Demagun orain n ez dela zenbaki lehen baten berretura. Frogatu X ez dela irreduziblea. (Laguntza: Ari garen baldintzapean $n = n_1n_2$ jar dezakegu, $1 < n_1, n_2 < n$ eta zkh$(n_1, n_2) = 1$ izanik. Idatzi Bézouten identitatea n_1^2-rekin eta n_2^2-rekin, eta erabili hori X indeterminatua lehenengo mailako bi polinomioren biderkadura gisa adierazteko. Ikusi bi faktore horiek ez direla $\mathbb{Z}/n\mathbb{Z}[X]$-ren unitateak.)

3.5. Izan bitez K gorputza eta

$$A = \left\{\textstyle\sum_{i\geq 0} c_iX^i \in K[X] \mid c_1 = 0\right\}.$$

Orduan, 1.5 ariketan ikusi genuen bezala, A eraztuna da.

(i) Zein dira A-ren unitateak? Horretan oinarrituz, ikusi elementu elkartuen baliokidetasun-klaseen ordezkari gisa A-ko polinomio monikoak har daitezkeela.

(ii) Frogatu X^2 eta X^3 irreduzibleak direla A-n.

(iii) Eman X^6 polinomioaren bi deskonposizio A-ko elementu irreduzibleen biderkadura gisa, faktore-kopuru desberdinak dituztenak. Ondorioztatu A ez dela faktorizazio bakarreko domeinua.

(iv) Kalkulatu X^5 eta X^6 polinomioen zatitzaile moniko guztiak A-n. Ondorioztatu X^5-en eta X^6-ren zatitzaile komunetako handiena ez dela existitzen eraztun horretan. Existitzen da X^5-en eta X^6-ren multiplo komunetako txikiena?

3.6. Faktorizazio bakarreko domeinua ez den integritate-domeinu baten adibidea eman nahi badugu, kandidatu natural bat $K[X, Y]/(X^2 - Y^3)$ da, bertan $\overline{X}^2 = \overline{Y}^3$ berdintza dugu eta. Hala ere, zatidura eraztun horretan lan eginda ez da erraza $\overline{X}$ eta $\overline{Y}$ elementuak irreduzibleak direla ikustea. (Hasiera batean, gerta liteke elementu horiek ez izatea irreduzibleak: ikusi 3.7 ariketako (ii) atala.) Horretarako, $\varphi : K[X, Y] \longrightarrow K[T]$ ebaluazio-homomorfismoa erabiliko dugu, $X \longmapsto T^3$ eta $Y \longmapsto T^2$ egokitzapenen bidez emanda.

(i) Frogatu $\ker\varphi = (X^2 - Y^3)$ dela. (Iradokizuna $\subseteq$ partekotasunerako: Ohiko metodoa erabiliz, $f(X,Y) \in \ker\varphi$ hartu eta $X^2 - Y^3$-rekin zatitu, X-rekiko. Idatzi hondarra $a(Y)X + b(Y)$ moduan.)

(ii) Ikusi $\operatorname{im}\varphi = K[T^2, T^3]$ dela. (Hemen, $K[T^2, T^3]$ ikurraren bidez, koefizienteak K-n dituzten T^2-ren eta T^3-ren konbinazio polinomiko guztien multzoa adierazten dugu.) Frogatu

$$K[T^2, T^3] = \left\{\textstyle\sum_{i\geq 0} c_i T^i \in K[T] \mid c_1 = 0\right\}$$

dela.

(iii) Aurreko bi atalen arabera,

$$\frac{K[X,Y]}{(X^2 - Y^3)} \cong K[T^2, T^3]$$

isomorfismoa dugu. Erabili 3.1 eta 3.5 ariketak ondorioztatzeko $\overline{X}$ eta $\overline{Y}$ irreduzibleak direla $K[X,Y]/(X^2 - Y^3)$ zatiduran, eta eraztun hori ez dela faktorizazio bakarreko domeinua, integritate-domeinua den arren.

Ohartu azken atalak propietate honen adibide bat ematen digula: A faktorizazio bakarreko domeinua bada eta B A-ren azpieraztuna bada, orduan B-k ez du zertan faktorizazio bakarreko domeinua izan.

3.7. Izan bitez K gorputza eta $A = K[X,Y]/(X + Y^2 - 1)$.

(i) Frogatu $\overline{f(X,Y)}$ elementua A-ren unitatea dela baldin eta soilik baldin $(f(X,Y), X + Y^2 - 1) = K[X,Y]$ bada.

(ii) Aurreko atalean oinarrituz, ikusi $\overline{X}$ elementua ez dela irreduziblea A-n, unitatea edo $\overline{0}$-ren berdina ez bada ere.

3.8. Problema honetan ikusiko dugu $\mathbb{Z}[\sqrt{-5}]$ eraztuna ez dela faktorizazio bakarreko domeinua.

(i) Frogatu $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ dela.

(ii) Definitu $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ elementu baten *norma* modu honetan:

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z}.$$

Ikusi normak propietate biderkakorra betetzen duela, hau da, $N(xy) = N(x)N(y)$ dela $x, y \in \mathbb{Z}[\sqrt{-5}]$ guztietarako.

(iii) Frogatu x unitatea dela $\mathbb{Z}[\sqrt{-5}]$ eraztunean baldin eta soilik baldin $N(x) = 1$ bada. Ondorioztatu $(\mathbb{Z}[\sqrt{-5}])^\times = \{1, -1\}$ dela.

(iv) Baldin eta $N(x)$ zenbaki lehena bada, frogatu x irreduziblea dela $\mathbb{Z}[\sqrt{-5}]$ eraztunean. Adibidez, $3 + 2\sqrt{-5}$ eta $6 + \sqrt{-5}$ irreduzibleak dira.

(v) Frogatu ez dagoela 2 edo 3 normako elementurik $\mathbb{Z}[\sqrt{-5}]$-n. Ondorioztatu 2, 3, $1 + \sqrt{-5}$ eta $1 - \sqrt{-5}$ elementuak irreduzibleak direla, nahiz eta horien norma ez izan zenbaki lehena. Horrek erakusten du aurreko ataleko emaitzaren alderantzizkoa ez dela betetzen.

(vi) Eman 6 zenbakiaren bi faktorizazio desberdin irreduzibleetan $\mathbb{Z}[\sqrt{-5}]$ eraztunean, balio dutenak erakusteko $\mathbb{Z}[\sqrt{-5}]$ ez dela faktorizazo bakarreko domeinua.

3.9. Frogatu 6 eta $2+2\sqrt{-5}$ elementuek ez dutela zatitzaile komunetako handienik $\mathbb{Z}[\sqrt{-5}]$ eraztunean. (Iradokizuna: Absurdora eramanez argudiatuz, demagun bi elementu horiek zatitzaile komunetako hadien bat dutela, d. Zatigarritasun propietateetan normak aplikatuz, frogatu $N(d) = 12$ dela eta lortu kontraesana.)

3.10. Izan bitez A eraztuna eta $\mathfrak{a}$ A-ren ideala.

(i) Izan bedi $\mathfrak{b}$ $\mathfrak{a}$-k sortzen duen ideala $A[X_1, \ldots, X_n]$ polinomioen eraztunean. Deskribatu $\mathfrak{b}$-ko elementuak.

(ii) Frogatu isomorfismo hau betetzen dela:

$$\frac{A[X_1, \ldots, X_n]}{\mathfrak{b}} \cong \frac{A}{\mathfrak{a}}[X_1, \ldots, X_n].$$

3.11. Izan bitez $A \subseteq B$ bi eraztun. Orduan, $a_1, \ldots, a_r \in A$ bada, "a_1 irreduziblea da" eta "$(a_1, \ldots, a_r)$ ideal lehena da" bezalako esaldiak anbiguoak izan daitezke, ez dakigulako A-n edo B-n begiratzen ari garen propietate horiek.

(i) Frogatu 2 zenbakia ez dela irreduziblea $\mathbb{Z}[i]$-n, nahiz eta $\mathbb{Z}$-n bai izan. Beraz, (2) ideala lehena da $\mathbb{Z}$-n, baina ez $\mathbb{Z}[i]$-n. (Ohartu $\mathbb{Z}$-n eta $\mathbb{Z}[i]$-n bi multzo desberdin adierazten dituela (2) ikurrak.)

(ii) Izan bedi $f \in K[X_1, \ldots, X_m]$. Frogatu $n \geq m$ guztietarako propietate hau betetzen dela: f irreduziblea da $K[X_1, \ldots, X_n]$-n baldin eta soilik baldin irreduziblea bada $K[X_1, \ldots, X_m]$-n. Hori dela eta, zentzua du esateak polinomio bat irreduziblea den edo ez *K-ren gainean*, indeterminatuak aipatu gabe.

(iii) Izan bedi $\mathfrak{a}$ $K[X_1, \ldots, X_m]$-ren ideala, eta dei diezaiogun $\mathfrak{b}$ $\mathfrak{a}$-k $K[X_1, \ldots, X_n]$ eraztunean sortzen duen idealari, $n \geq m$ izanik. Frogatu $\mathfrak{a}$ ideal lehena dela $K[X_1, \ldots, X_m]$-n baldin eta soilik baldin $\mathfrak{b}$ ideal lehena bada $K[X_1, \ldots, X_n]$-n. (Laguntza: Erabili 3.10 ariketan emandako isomorfismoa.) Ondorioz, $f_1, \ldots, f_r$ polinomioak badira, badu zentzua $(f_1, \ldots, f_r)$ K-ren gainean ideal lehena dela esateak, indeterminatuak aipatu gabe.

3.12. Demagun $A[X]$ polinomioen eraztuna ideal nagusietako domeinua dela. Frogatu A gorputza dela. (Iradokizuna: Hartu $a \in A$, $a \neq 0$. Frogatu $a \in A^\times$ dela (a, X) ideala aztertuz.)

3.13. Izan bitez A ideal nagusietako domeinua eta K A-ren zatikien gorputza, eta demagun B eraztunak $A \subseteq B \subseteq K$ betetzen duela.

(i) Baldin eta $a/b \in B$ badugu, a/b zatiki laburtezina izanik, frogatu $1/b \in B$ dela. (Erabili Bézouten identitatea.)

(ii) Frogatu B ere ideal nagusietako domeinua dela. (Iradokizuna: Izan bedi $\mathfrak{b}$ B-ren ideala eta jarri $\mathfrak{a} = \mathfrak{b} \cap A$. Baldin eta x $\mathfrak{a}$-ren sortzailea bada, frogatu x-k berak $\mathfrak{b}$ sortzen duela.)

3.14. Izan bitez A eraztuna eta $\mathfrak{p}$ A-ren ideal lehena.

(i) Baldin eta A ideal nagusietako domeinua bada, frogatu $A/\mathfrak{p}$ ere ideal nagusietako domeinua dela. (Bestela esanda, ideal nagusietako domeinu baten zatidurak ideal nagusietako domeinuak dira, integritate domeinuak baldin badira.) Ba al da egia alderantzizkoa?

(ii) Ohartu, 3.6 ariketak erakusten duen bezala, aurreko ataleko emaitza ez dela betetzen ideal nagusietako domeinua izateko propietatearen ordez faktorizazio bakarreko domeinua izatekoa jartzen badugu.

3.15. Izan bitez A integritate-domeinua eta $b \in A$, $b \neq 0$. Baldin eta $S = \{b^n \mid n \in \mathbb{N} \cup \{0\}\}$ bada b-k sortzen duen azpimultzo biderkakorra, frogatu $S^{-1}A \cong A[X]/(bX-1)$ isomorfismoa. (Iradokizuna: Erabili $A[X]$-ren propietate unibertsala $X \longmapsto 1/b$ eraztun-homomorfismo bat definitzeko $A[X]$-tik $S^{-1}A$ zatikien eraztunera.)

3.16. Aurreko problema eraztun batzuk ideal nagusietako domeinuak direla frogatzeko erabil daiteke, jarraian erakusten dugun bezala.

(i) Izan bedi K gorputza. Frogatu $K[X,Y]/(XY-1)$ ideal nagusietako domeinua dela.

(ii) Frogatu $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ ideal nagusietako domeinua dela. (Laguntza: Ohartu $X^2+Y^2 = (X+iY)(X-iY)$ dela $\mathbb{C}[X,Y]$-n, eta erabili (i) atala.)

3.17. Frogatu $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ domeinu euklidearra dela

$$\varphi(a+b\sqrt{2}) = |a^2-2b^2| = |(a+b\sqrt{2})(a-b\sqrt{2})|$$

funtzio euklidearrarekin. (Laguntza: Izan bitez $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $c+d\sqrt{2} \neq 0$ izanik. Orduan,

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = e+f\sqrt{2}$$

jar dezakegu, $e,f \in \mathbb{Q}$ izanik, $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ multzoa gorputza baita. Aukeratu $u,v \in \mathbb{Z}$ non $|e-u| \leq 1/2$ eta $|f-v| \leq 1/2$ baita, eta frogatu $\varphi(a+b\sqrt{2}-(u+v\sqrt{2})(c+d\sqrt{2})) \leq 3/4\,\varphi(c+d\sqrt{2})$ dela.)