MATERI PEMBEKALAN PESERTA OLIMPIADE NASIONAL MATEMATIKA PERGURUAN TINGGI

BIDANG ALJABAR

Oleh:

AGUS MAMAN ABADI

JURUSAN PENDIDIKAN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI YOGYAKARTA

2011

Disampaikan dalam Pembekalan Peserta Olimpiade Nasional Matematika Perguruan Tinggi

di Universitas Islam Indonesia pada 29 Maret 2011

DAFTAR ISI

ABSTRAK

Kegiatan Olimpiade Nasional Matematika Perguruan Tinggi dilaksanakan setiap tahun. Kegiatan ini diikuti oleh mahasiswa dari perguruan tinggi di Indonesia. Berdasarkan pengalaman penulis, mahasiswa mengalami kesulitan dalam mengerjakan soal-soal olimpiade nasional matematika Perguruan Tinggi, karena mahasiswa yang ikut belum semuanya memperoleh materi yang diujikan. Hal ini karena mahasiswa yang ikut ada yang berasal dari semester awal yang belum mengambil mata kuliah yang diujikan di olimpiade. Tujuan pembekalan ini adalah agar mahasiswa mampu mempersiapkan diri secara maksimal dalam mengikuti olimpiade nasional matematika perguruan tinggi.

Materi olimpiade matematika ini meliputi analisis, aljabar linear, struktur aljabar, analisis kompleks, kombinatorik dan matematika terapan. Soal untuk masing-masing materi terdiri dari dua jenis, bagian pertama berupa jawaban singkat dan bagian kedua untuk jawaban uraian. Pada tulisan ini akan diberikan materi bidang struktur aljabar yang meliputi teori grup dan teori ring. Harapannya setelah mempelajari materi ini, mahasiswa mempunyai kepercayaan diri dan siap untuk mengikuti seleksi olimpiade nasional matematika perguruan tinggi tingkat provinsi.

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kegiatan Olimpiade Nasional Matematika Perguruan Tinggi dilaksanakan setiap tahun. Kegiatan ini diikuti oleh mahasiswa dari perguruan tinggi di Indonesia. Seleksi dilakukan dalam beberapa tahap. Seleksi awal dilakukan oleh masing-masing perguruan tinggi. Mahasiswa yang berhasil dalam seleksi awal tersebut akan dibina oleh perguruan tinggi yang bersangkutan untuk mempersiapkan diri dalam seleksi tingkat provinsi. Mahasiswa yang lolos seleksi tingkat provinsi akan mengikuti seleksi tingkat nasional. Kemudian mahasiswa yang lolos seleksi tingkat nasional akan dibina untuk mengikuti olimpiade matematika tingkat internasional.

Berdasarkan pengalaman penulis, mahasiswa mengalami kesulitan dalam mengerjakan soal-soal olimpiade nasional matematika Perguruan Tinggi, karena mahasiswa yang ikut belum semuanya memperoleh materi yang diujikan. Hal ini karena mahasiswa yang ikut ada yang berasal dari semester awal yang belum mengambil mata kuliah yang diujikan di olimpiade. Oleh karena itu perlu diadakan pembekalan materi olimpiade nasional matematika perguruan tinggi untuk calon peserta olimpiade. Materi olimpiade matematika ini meliputi analisis, aljabar linear, struktur aljabar, analisis kompleks, kombinatorik dan matematika terapan. Soal untuk masing-masing materi terdiri dari dua jenis, bagian pertama berupa jawaban singkat dan bagian kedua untuk jawaban uraian.

1.2 Tujuan

Tujuan pembekalan ini adalah agar mahasiswa mampu mempersiapkan diri secara maksimal dalam mengikuti olimpiade nasional matematika perguruan tinggi. Pada tulisan ini akan diberikan materi bidang struktur aljabar yang meliputi teori grup dan teori ring.

1.3 Manfaat

Harapannya setelah mempelajari materi ini, mahasiswa mempunyai kepercayaan diri dan siap untuk mengikuti seleksi olimpiade nasional matematika perguruan tinggi tingkat provinsi.

BAB II
MATERI ALJABAR (GRUP DAN RING)

2.1 Grup dan sifat-sifatnya

Di dalam subbab ini akan diperkenalkan suatu struktur aljabar yang melibatkan satu operasi biner.

Definisi 2.1.1 Misalkan G adalah himpunan tidak kosong dan * adalah suatu operasi biner pada G. Himpunan G yang dilengkapi dengan operasi biner *, ditulis (G, *), disebut grup jika memenuhi semua aksioma berikut ini:

G1. Untuk semua $a, b, c \in G$ $a*(b*c) = (a*b)*c$ (asosiatif)

G2. Ada elemen $e \in G$ sedemikian sehingga untuk semua $a \in G$, $a*e = e*a = a$

G3. Untuk setiap $a \in G$, ada $b \in G$ sedemikian sehingga $a*b = b*a = e$.

Elemen e yang memenuhi G2 disebut **elemen identitas** dan elemen b yang memenuhi G3 disebut **invers dari a** dan dinotasikan dengan a^{-1}. Jika grup (G,*) memenuhi untuk setiap $a, b \in G$ $a*b = b*a$, maka (G,*) disebut grup komutatif.

Contoh 2.1.1

1. Himpunan bilangan bulat B yang dilengkapi dengan operasi penjumlahan aritmetik adalah grup.
2. Misalkan n adalah bilangan bulat positif > 1 dan $\mathbb{Z}_n$ adalah himpunan semua kelas-kelas bilangan bulat modulo n. Didefinisikan operasi $+_n$ pada $\mathbb{Z}_n$ sebagai $[a] +_n [b] = [a+b]$ untuk setiap $[a],[b] \in \mathbb{Z}_n$, maka $(\mathbb{Z}_n, +_n)$ adalah grup komutatif.

Teorema 2.1.1 Jika (G,*) suatu grup, maka berlaku:

1. $(a^{-1})^{-1} = a$ untuk setiap $a \in G$.
2. $(a*b)^{-1} = b^{-1} * a^{-1}$ untuk setiap $a, b \in G$.
3. Untuk setiap $a, b, c \in G$, jika $a*c = b*c$ atau $c*a = c*b$, maka $a = b$.
4. Untuk setiap $a, b \in G$, persamaan $a*x = b$ dan $y*a = b$ mempunyai solusi tunggal di G untuk x dan y.

Definisi 2.1.2 Misalkan (G, *) suatu grup dan $a \in G$. Order dari a, ditulis $\circ(a)$, adalah bilangan bulat positif terkecil n sedemikian sehingga $a^n = e$. Jika tidak ada bilangan n yang demikian, maka dikatakan order a adalah takhingga.

Teorema 2.1.2 Misalkan (G, *) suatu grup dan $a \in G$ dengan $\circ(a)$ = n.

1. Jika $a^m = e$ untuk suatu bilangan bulat positif m, maka n membagi m.

2. Untuk setiap bilangan bulat positif t, berlaku $\circ(a^t) = \frac{n}{(t,n)}$.

2.1.1 Subgrup dan Sifat-sifatnya

Definisi 2.1.3 Misalkan (G, *) suatu grup dan S suatu himpunan bagian tidak kosong dari G. (S, *) disebut subgrup dari (G,*) jika (S,*) juga grup.

Contoh 2.1.2 Himpunan {[0]}, N = { [0], [3], S = { [0], [2], [4]} dan $\mathbb{Z}_6$ subgrup-subgrup dari $\mathbb{Z}_6$.

Selanjutnya suatu grup (G,*) ditulis G saja dan a*b ditulis ab.

Teorema 2.1.3 Misalkan G suatu grup dan S suatu himpunan bagian tidak kosong dari G. S subgrup dari G jika dan hanya jika untuk setiap $a,b \in S$, $ab^{-1} \in S$.

Akibat 2.1.4 Misalkan G suatu grup dan S suatu himpunan bagian tidak kosong dari G dan berhingga. S subgrup dari G jika dan hanya jika untuk setiap $a,b \in S$, $ab \in S$.

Misalkan G suatu grup dan $Z(G) = \{b \in G \mid ab = ba, \forall a \in G\}$, maka $Z(G)$ disebut center dari G.

Teorema 2.1.5 Misalkan G suatu grup, maka $Z(G)$ merupakan subgrup komutatif dari G.

Definisi 2.1.4 Misalkan G suatu grup dan S suatu himpunan bagian dari G. Didefinisikan $N = \{H \mid H \text{ subgrup dari G dan } S \subset H\}$ dan subgrup yang **dibangun oleh S**, ditulis $< S >$, adalah irisan semua subgrup yang memuat S yaitu $< S > = \bigcap_{H \in N} H$. Jika grup G = $< S >$, maka S disebut himpunan pembangun dari G.

Teorema 2.1.6 Misalkan S himpunan bagian tidak kosong dari grup G, maka $< S > = \{s_1^{e_1} s_2^{e_2} \ldots s_n^{e_n} \mid s_i \in S, e_i = \pm 1, i = 1,2,\ldots,n, n = 1,2,3,\ldots\}$.

Akibat 2.1.7 Misalkan G suatu grup dan $a \in G$, maka $< a > = \{a^n \mid n \in Z\}$.

Definisi 2.1.5 Misalkan H dan K himpunan bagian tidak kosong dari grup G, pergandaan H dan K didefinisikan sebagai $HK = \{hk \mid h \in H, k \in K\}$.

Teorema 2.1.8 Jika H dan K subgrup-subgrup dari grup G, maka HK subgrup dari G jika dan hanya jika $HK = KH$.

Akibat 2.1.9 Jika H dan K subgrup-subgrup dari grup komutatif G, maka HK subgrup dari G.

Teorema 2.1.10 Jika H dan K subgrup-subgrup dari grup G, maka HK subgrup dari G jika dan hanya jika $HK = < H \cup K >$.

2.1.2 Grup Siklik dan sifat-sifatnya

Definisi 2.1.6 Suatu grup G disebut grup siklik jika ada $a \in G$ sedemikian sehingga $G = < a >$ dengan $< a > = \{a^n \mid n \in \mathbb{Z}\}$.

Contoh 2.1.3

(i). $(\mathbb{Z}, +)$ adalah grup siklik dengan generatornya 1.

(ii). $(\mathbb{Z}_n, +_n)$ adalah grup siklik dengan generatornya [1].

Teorema 2.1.11 Jika $< a >$ grup siklik order n, maka $< a > = \{e, a, a^2, ..., a^{n-1}\}$.

Akibat 2.1.12 JIka $< a >$ grup siklik hingga, maka $\circ(a) = |< a >|$.

Akibat 2.1.13 Suatu grup G adalah grup siklik jika dan hanya jika ada elemen $a \in G$ sedemikian sehingga $\circ(a) = |G|$.

Teorema 2.1.14 Setiap subgrup dari grup siklik adalah siklik.

Akibat 1.15 Misalkan $G = < a >$ suatu grup siklik order m, m >1, dan H subgrup sejati dari G, maka $H = \langle a^k \rangle$ untuk suatu bilangan bulat k dengan k membagi m dan k > 1.

Teorema 2.1.16 Misalkan G suatu grup siklik order m, maka untuk setiap pembagi positif d dari m, ada dengan tunggal subgrup G berorder d.

Berdasarkan Teorema 1.16, misalkan G suatu grup siklik order m, maka jika d pembagi positif dari m, ada dengan tunggal subgrup G berorder d yaitu $H = < a^{m/d} >$.

Latihan 2.1.1

1. Tunjukkan bahwa grup $(Q, +)$ tidak siklik.
2. JIka G grup dengan $|G| = mn, n > 1, m > 1$, tunjukkan bahwa G mempunyai subgrup nontrivial.
3. Jika G grup siklik takhingga, tunjukkan bahwa G mempunyai tepat dua generator.
4. JIka $G = < a >$ grup siklik order n, tunjukkan bahwa a^k generator untuk G jika dan hanya jika gcd(k,n) = 1 dengan k adalah bilangan bulat positif.
5. Tentukan semua subgrup dari grup siklik $G = < a >$ order 30.

6. Jika G grup siklik order n, tunjukkan bahwa banyaknya generator dari G adalah $\phi(n)$ dengan ϕ adalah fungsi Euler.

2.1.3 Teorema Lagrange

Definisi 2.1.7 Misalkan H adalah subgrup dari grup G dan $a \in G$. Himpunan $aH = \{ah \mid h \in H\}$ dan $Ha = \{ha \mid h \in H\}$ berturut-turut disebut koset kiri dan kanan dari H dalam G.

JIka G grup komutatif, maka $aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha$, tetapi jika G tidak komutatif, maka aH belum tentu sama dengan Ha.

Contoh 2.1.4

Diberikan grup simetris S_3 dan subgrup dari S_3, $H = \{e, (123), (132)\}$ dan $H_1 = \{e, (23)\}$, maka dapat ditunjukkan bahwa untuk setiap $a \in S_3$ berlaku $aH = Ha$. Tetapi ada $(132) \in S_3$ sedemikian sehingga $(132)H_1 \neq H_1(132)$.

Teorema 2.1.17 Misalkan H adalah subgrup dari grup G dan $a, b \in G$, maka

(i). $aH = bH$ jika dan hanya jika $b^{-1}a \in H$

(ii). $Ha = Hb$ jika dan hanya jika $ab^{-1} \in H$.

Teorema 2.1.18 Jika H subgrup dari grup G , maka untuk setiap $a, b \in G$ $aH = bH$ atau $aH \cap bH = \phi$.

Akibat 2.1.19 Jika H subgrup dari grup G, maka $\{aH \mid a \in G\}$ membentuk partisi pada G.

Teorema 2.1.20 Jika H subgrup dari grup G, maka ada korespondensi 1-1 antara elemen-elemen H dengan elemen-elemen dari aH maupun Ha.

Akibat 2.1.21 Jika H subgrup dari grup G, maka untuk semua $a \in G$, $|H| = |aH| = |Ha|$.

Definisi 2.1.8 Misalkan H adalah subgrup dari grup G. Indek dari H dalam G didefinisikan sebgai banyaknya koset kiri (kanan) yang berbeda dari H dalam G dan ditulis [G:H].

Teorema 1.22 (Teorema Lagrange) Misalkan H adalah subgrup dari grup hingga G, maka order dari H membagi order G dan $|G| = [G:H]|H|$.

Akibat 2.1.23 JIka G grup hingga order n, maka order setiap elemen $a \in G$ membagi n dan $a^n = e$.

Teorema 2.1.24 (Teorem Fermat) Misalkan p adalah bilangan prima dan a adalah bilangan bulat sedemikian sehingga p tidak membagi a, maka p membagi $a^{p-1} - 1$.

Teorema 2.1.25 Jika H dan K adalah subgrup-subgrup hingga dari grup G, maka $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

Akibat 2.1.26 Jika H dan K adalah subgrup-subgrup hingga dari grup G dengan Jika H dan K adalah subgrup-subgrup hingga dari grup G, maka $H \cap K = \{e\}$, maka $|HK| = |H||K|$.

Latihan 2.1.2

1. Jika H subgrup dari grup G, tunjukkan bahwa untuk semua $a \in G$, $aH = H$ jika dan hanya jika $a \in H$
2. Jika G grup order p^2, p prima, maka tunjukkan bahwa order elemen G selain e adalah p.
3. Jika G grup dengan $|G| > 1$, tunjukkan bahwa G hanya mempunyai subgrup trivial jika dan hanya jika order G prima.
4. Tunjukkan bahwa jika G grup order p^n, p prima, maka G memuat elemen berorder p.
5. Jika G grup hingga komutatif yang memuat dua elemen yang berbeda berorder dua, tunjukkan bahwa order G kelipatan empat.
6. Buktikan bahwa jika G grup order pq dengan p dan q prima, maka setiap subgrup sejati dari G adalah siklik.
7. Jika H dan K subgrup dari grup hingga G dengan $|H| > \sqrt{|G|}$ dan $|K| > \sqrt{|G|}$, buktikan bahwa $|H \cap K| > 1$.
8. Buktikan bahwa Jika G grup order pq, p dan q prima, p > q, maka G mempunyai paling banyak satu subgrup order p.
9. Jika G grup order kurang dari 200 dan G mempunyai subgrup order 25 dan 35, tentukan order G.
10. Jika G grup order 35 dan H dan K subgrup dari G beruturt-turut order 5 dan 7, maka buktikan bahwa G = HK.

2.1.4 Subgrup Normal dan grup faktor

Definisi 2.1.9 Misalkan G suatu grup. Subgrup H dari G disebut subgrup normal dari G jika $aH = Ha$ untuk setiap $a \in G$.

Contoh 2.1.5

Diberikan grup simetris S_3 dan subgrup dari S_3, $H = \{e, (123), (132)\}$ dan $H_1 = \{e, (23)\}$, maka dapat ditunjukkan bahwa untuk setiap $a \in S_3$ berlaku $aH = Ha$. Tetapi ada $(132) \in S_3$

sedemikian sehingga $(132)H_1 \neq H_1(132)$. Jadi H adalah subgrup normal dari S_3 tetapi H_1 bukan subgrup normal dari S_3.

Teorema 2.1.27 Misalkan H subgrup dari grup G. H subgrup normal dari G jika dan hanya jika untuk semua $a \in G$, $aHa^{-1} \subseteq H$.

Teorema 2.1.28 Jika H dan K subgrup normal dari grup G, maka

(i). $H \cap K$ subgrup normal dari G.

(ii). $HK = KH$ subgrup normal dari G.

(iii). $\langle H \cup K \rangle = HK$.

Misalkan H subgrup normal dari grup G dan $G/H = \{aH \mid a \in G\}$. Didefinisikan operasi * pada G/H dengan $aH * bH = abH$ untuk setiap $aH, bH \in G/H$, maka operasi * well-defined.

Teorema 2.1.29 Misalkan H subgrup normal dari grup G dan $G/H = \{aH \mid a \in G\}$, maka $\left(G/H, *\right)$ suatu grup.

Definisi 2.1.10 Misalkan G grup dan H subgrup normal dari G, maka grup G/H disebut grup faktor dari G oleh H.

Contoh 2.1.6

Diberikan grup simetris S_3. Berdasarkan Contoh 1.5, $H = \{e, (123), (132)\}$ adalah subgrup normal dari S_3. Selanjutnya $|S_3| = 6, |H| = 3$, sehingga menurut Teorema Lagrange, $[S_3 : H] = \frac{|S_3|}{|H|} = \frac{6}{3} = 2$. Jadi $S_3/H = \{H, (23)H\}$.

Definisi 2.1.11 Misalkan G suatu grup. Grup G dikatakan simple jika $G \neq \{e\}$ dan subgrup normal dari G hanyalah G dan {e}.

Contoh 2.1.7 Misalkan G grup order p, p prima, maka subgrup dari G hanyalah G dan {e} sehingga G simple. Jadi setiap grup order prima adalah simple.

Teorema 2.1.30 Jika H subgrup normal dari maka $A_n, n \geq 5$ dan H memuat sikel panjang 3, maka $H = A_n$.

Teorema 2.1.31 Jika H subgrup normal dari maka $A_n, n \geq 5$ dan H memuat suatu pergandaan dari dua transposisi-transposisi yang saling asing, maka $H = A_n$.

Teorema 2.1.32 Jika $n \geq 5$, maka grup A_n adalah simple.

Latihan 2.1.3

1. Misalkan H subgrup dari grup G. Jika $x^2 \in H$ untuk setiap $x \in G$, buktikan bahwa H subgrup normal dari G dan G/H komutatif.

2. Misalkan H subgrup dari grup G. Jika $[G:H]$= 2, buktikan bahwa H subgrup normal dari G.

3. Misalkan G suatu grup sedemikian sehingga setiap subgrup siklik dari G adalah subgrup normal dari G, buktikan bahwa setiap subgrup dari G adalah subgrup normal dari G.

4. Misalkan H subgrup sejati dari grup G sedemikian sehingga untuk setiap $x, y \in G \setminus H$, $xy \in H$, buktikan bahwa H subgrup normal dari G.

5. Misalkan H subgrup dari grup G dan jika untuk setiap $a, b \in G$, $ab \in H$ berakibat $ba \in H$, buktikan bahwa H subgrup normal dari G.

6. Buktikan bahwa jika H dan K sugrup normal dari grup G dan $H \cap K = \{e\}$, maka $hk = kh$ untuk setiap $h \in H, k \in K$.

7. Misalkan H subgrup dari grup G. Didefinisikan relasi ρ_H pada G dengan $\rho_H = \{(a,b) \in G \times G \mid a^{-1}b \in H\}$. Buktikan bahwa jika ρ_H relasi kongruensi, maka H subgrup normal dari G.

8. Misalkan G grup dan H subgrup dari G dengan $H \subseteq Z(G)$. Tunjukkan bahwa jika G/H siklik, maka $G = Z(G)$ yaitu G komutatif.

9. Apakah setiap subgrup komutatif dari grup G merupakan subgrup normal dari G?

10. Apakah setiap grup G order 2p, p prima, adalah komutatif atau memuat subgrup normal?

2.1.5 Homomorpisma grup dan sifat-sifatnya

Definisi 2.1.12 Misalkan $(G,*)$ dan $(G_1,*_1)$ adalah grup-grup dan f adalah fungsi dari G ke G_1. Fungsi f disebut homomorpisma grup dari G ke G_1 jika untuk setiap $a,b \in G$ berlaku

$$f(a*b) = f(a) *_1 f(b)$$

Jika f homomorpisma grup dari G ke G_1 dan injektif, maka f disebut monomorpisma. Jika f homomorpisma grup dari G ke G_1 dan surjektif, maka f disebut epimorpisma dan jika f homomorpisma grup dari G ke G_1 dan bijektif, maka f disebut isomorpisma. Jika f isomorpisma grup dari G ke G_1, maka G dikatakan isomorpis dengan G_1 dan ditulis $G \cong G_1$.

Contoh 2.1.8 1. Misalkan $(G,*)$ dan $(G_1,*_1)$ adalah grup-grup dan f adalah fungsi dari G ke G_1 dengan $f(a) = e_1$ untuk setiap $a \in G$ dengan e_1 elemen identitas dari G_1, maka f suatu homomorpisma grup dan disebut homomorpisma trivial.

2. Jika $(G,*)$ suatu grup dan f adalah fungsi dari G ke G dengan $f(a) = a$ untuk setiap $a \in G$, maka f suatu homomorpisma grup.

Teorema 2.1.33 Jika f adalah homomorpisma dari grup G ke grup G_1, maka berlaku

(i). $f(e) = e_1$ dengan e dan e_1 berturut-turut elemen identitas dari G dan G_1.

(ii). $f(a^{-1}) = f(a)^{-1}$ untuk setiap $a \in G$.

(iii). Jika H subgrup dari G, maka $f(H) = \{f(h) \mid h \in H\}$ adalah subgrup dari G_1.

(iv). Jika H_1 subgrup dari G_1, maka $f^{-1}(H_1) = \{g \in G \mid f(g) \in H_1\}$ adalah subgrup dari G.

(v). Jika H_1 subgrup normal dari G_1, maka $f^{-1}(H_1) = \{g \in G \mid f(g) \in H_1\}$ adalah subgrup normal dari G.

(vi). Jika G komutatif, maka $f(G)$ juga komutatif.

(vii). Jika $a \in G$ dengan $\circ(a) = n$, maka $\circ(f(a))$ membagi n.

Definisi 2.1.13 Misalkan f adalah homomorpisma dari grup G ke grup G_1 dan e_1 elemen identitas dari G_1, kernel dari f, ditulis $\mathrm{Ker}(f)$, didefinisikan sebagai

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_1\}$$

Teorema 2.1.34 Misalkan f adalah homomorpisma dari grup G ke grup G_1. Homomorpisma f injektif jika dan hanya jika $\mathrm{Ker}(f) = \{e\}$.

Teorema 2.1.35 Jika f adalah homomorpisma dari grup G ke grup G_1, $\mathrm{Ker}(f)$ subgrup normal dari G.

Teorema 2.1.36 Misalkan f adalah isomorpisma dari grup G ke grup G_1, maka berlaku

(i). $f^{-1} : G_1 \to G$ adalah isomorpisma grup.

(ii). G komutatif jika dan hanya jika G_1 komutatif.

(iii). Untuk setiap $a \in G$, $\circ(a) = \circ(f(a))$.

(iv). G siklik jika dan hanya jika G_1 siklik.

Teorema 2.1.37 Setiap grup siklik hingga order n isomorpis dengan $(\mathbb{Z}_n, +_n)$ dan setiap grup siklik takhingga isomorpis dengan $(\mathbb{Z}, +)$.

Latihan 2.1.4

1. Misalkan f adalah epimorpisma dari grup G ke grup G_1. Buktikan bahwa jika H subgrup normal dari G, maka $f(H)$ subgrup normal dari G_1.
2. Misalkan G dan H grup hingga dengan $\gcd(|G|, |H|) = 1$, tunjukkan bahwa satu-satunya homomorpisma dari G ke H adalah homomorpisma trivial.
3. Tunjukkan bahwa $(Q, +)$ tidak isomorpis dengan $(Q/Z, +)$.
4. Tunjukkan bahwa $(Q, +)$ tidak isomorpis dengan $(\mathbb{R}, +)$.
5. Tentukan semua homomorpisma grup dari $\mathbb{Z}_6$ ke $\mathbb{Z}_4$.
6. Tentukan semua homomorpisma grup dari $\mathbb{Z}_8$ ke $\mathbb{Z}_{12}$.
7. Tentukan semua homomorpisma grup dari $\mathbb{Z}_{20}$ ke $\mathbb{Z}_{10}$.
8. Buktikan bahwa jika G grup siklik dan f adalah epimorpisma dari grup G ke grup G_1, maka G_1 siklik.
9. Jika f, g adalah epimorpisma dari grup G ke grup G_1 dengan $\mathrm{Ker}(f) = \mathrm{Ker}(g)$, apakah $f = g$?
10. Jika f adalah epimorpisma dari suatu grup siklik order 8 ke suatu grup siklik order 4, tentukan $\mathrm{Ker}(f)$.

2.1.6 Teorema utama isomorpisma grup

Teorema 2.1.38 Misalkan f adalah epimorpisma dari grup G ke grup G_1 dan H subgrup normal dari G dengan $H \subseteq \mathrm{Ker}(f)$ dan g homomorpisma natural dari G ke G/H, maka ada dengan tunggal epimorpisma h dari G/H ke G_1 sedemikian sehingga $f = h \circ g$. Kemudian h injektif jika dan hanya jika $h = \mathrm{Ker}(f)$.

Teorema 2.1.39 (Teorema Isomorpisma Pertama) Misalkan f adalah homomorpisma dari grup G ke grup G_1, maka $f(G)$ subgrup dari G_1 dan $G/\mathrm{Ker}(f) \cong f(G)$.

Teorema 2.1.40 Misalkan f adalah epimorpisma dari grup G ke grup G_1, maka berlaku (i). Jika G siklik, maka G_1 siklik.

(ii). Jika G komutatif, maka G_1 komutatif.

(iii). Jika G_1 memuat elemen order n dan $|G|$ berhingga, maka G memuat elemen order n.

Teorema 2.1.41 (Teorema Isomorpisma Kedua) Misalkan H dan K subgrup dari grup G dan K normal, maka $H/(H \cap K) \cong (HK)/K$.

Teorema 2.1.42 (Teorema Isomorpisma Ketiga) Misalkan M dan N subgrup normal dari grup G dan $N \subseteq M$, maka $(G/N)/(M/N) \cong G/M$.

Teorema 2.1.43 (Teorema Cauchy) Jika p prima dan p membagi order grup G, maka G memuat elemen berorder p.

Teorema 2.1.44 Misalkan G suatu grup berorder pq dengan p dan q prima dan p > q. Jika q tidak membagi p – 1, maka G siklik.

Latihan 2.1.5

1. Buktikan bahwa suatu grup order 35 adalah siklik.
2. Buktikan bahwa suatu grup order 42 mempunyai subgrup normal order 21.
3. Buktikan bahwa suatu grup order 99 mempunyai subgrup normal taktrivial.

Untuk nomor 4-7. Misalkan G suatu grup dan H suatu subgrup dari G dan N subgrup normal dari G. Misalkan $HN = \{hn \mid h \in H, n \in N\}$. Buktikan bahwa:

4. $H \cap N$ subgrup normal dari H.
5. HN subgrup dari G.
6. $N \subseteq HN$ dan N subgrup normal dari HN.
7. $HN/N \cong H/(H \cap N)$.
8. Jika G suatu grup dan N subgrup normal dari G dan $a \in G$ dengan $\circ(a) = n < \infty$, buktikan bahwa order $Na \in G/N$ membagi order a.
9. Jika f adalah epimorpisma dari grup G ke grup G_1 dan N subgrup normal dari G, tunjukkan bahwa $f(N)$ subgrup normal dari G_1.

2.2 Ring dan sifat-sifatnya

Pada bagian 1, kita sudah mengenal tentang grup dan sifat-sifatnya. Pada grup didefinisikan satu operasi biner. Selanjutnya dalam bagian ini akan diberikan konsep dasar suatu struktur aljabar yang melibatnya dua operasi biner yaitu ring.

Definisi 2.2.1 Misalkan R adalah himpunan tidak kosong. Pada R didefinisikan dua operasi biner + (penjumlahan) dan .(perkalian). Selanjutnya (R, +,.) disebut ring jika memenuhi I, II dan III berikut ini.

I. (R, +) ada grup komutatif .

II. (R, .) adalah semigrup.

III. Berlaku hukum distributif kiri dan kanan yaitu untuk setiap $a, b, c \in R$

(i). $a(b+c) = ab + ac$ (distributif kiri)

(ii). $(a+b)c = ac + bc$ (distributif kanan)

Contoh 2.2.1

1. Misalkan B adalah himpunan semua bilangan bulat dan operasi + dan . berturut-turut adalah operasi penjumlahan dan perkalian aritmetik, maka (B, +,.) adalah ring.

2. Misalkan $B_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ adalah himpunan kelas-kelas bilangan bulat modulo 3 dan $+_3$ dan x_3 adalah operasi penjumlahan dan perkalian modulo 3, maka (B_3, $+_3$, x_3) adalah ring.

Definisi 2.2.2 1. Jika (R, +, .) adalah ring, maka elemen identitas terhadap operasi + disebut elemen nol dan dinotasikan dengan z.

2. Jika ada elemen u sedemikian sehingga $u \neq z$ dan u adalah elemen identitas terhadap operasi ., maka u disebut elemen kesatuan.

3. Jika ring R mempunyai elemen kesatuan, maka ring R disebut ring dengan elemen kesatuan.

4. Jika u, $a \in R$ dan ada $a^{-1} \in R$ sedemikian sehingga $a\,a^{-1} = a^{-1}a = u$, maka *a* disebut unit.

5. Jika ring R komutatif terhadap operasi perkalian, maka R disebut ring komutatif.

Definisi 2.2.3 1. Misalkan a dan b elemen-elemen taknol dari ring R sedemikian sehingga ab = z, maka a disebut pembagi nol kiri dan b disebut pembagi nol kanan. Jika a pembagi nol kiri dan pembagi nol kanan, maka a disebut pembagi nol.

2. Suatu ring komutatif dengan elemen kesatuan dan tidak memuat pembagi nol disebut **daerah integral** (integral domain).

3. Suatu ring komutatif dengan elemen kesatuan dan setiap elemen yang tidak nol mempunyai invers terhadap perkalian disebut **lapangan** (field).

Contoh 2.2.2

1. Himpunan bilangan bulat $\mathbb{Z}$ terhadap operasi penjumlahan (+) dan perkalian (.) aritmetik adalah daerah integral.

2. Misalkan himpunan $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ berturut-turut adalah himpunan bilangan real, rasional dan kompleks dan didefinisikan operations penjumlahan (+) dan perkalian (.) aritmetik, maka $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ adalah lapangan ?

3. Himpunan $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ terhadap operasi ($+_4$) dan perkalian ($\times_4$) modulo 4 adalah ring yang bukan daerah integral.

4. Himpunan $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ terhadap operasi ($+_5$) dan operasi ($\times_5$) modulo 5 adalah lapangan.

5. Himpunan $Z_p = \{\overline{0}, \overline{1}, \tilde{2}, ..., \overline{p-1}\}$ terhadap operasi ($+_n$)dan operasi ($\times_n$) modulo *p* adalah lapangan jika dan hanya jika p bilangan prima.

6. Himpunan $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a,b,c,d \in \mathbb{R} \right\}$ terhadap operasi (+) dan perkalian (x) matriks adalah ring.

Teorema 2.2.1. Jika R adalah ring, maka untuk setiap $a,b,c \in R$ pernyataan berikut dipenuhi:

1. $az = za = z$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $-(a+b) = (-a)+(-b)$
5. $a(b-c) = ab - ac$
6. $(a-b)c = ac - bc$
7. $(-u)a = -a$ where *u* is unity

Teorema 2.2.2. Misalkan R adalah ring. Ring R tidak mempunyai pembagi nol jika dan hanya jika hukum kanselasi berlaku di R.

Teorema 2.2.3. Daerah integral yang berhingga adalah lapangan.

Definisi 2.2.4 Diberikan ring R dan $a \in R$, m adalah bilangan bulat positif. Didefinisikan:

1. ma = $\underbrace{a + a + a + ... + a}_{m}$

2. $-ma = \underbrace{(-a)+(-a)+. \quad +.(-a)}_{m} = -(ma)$

3. $0a = z$

Teorema 2.2.4. Jika R adalah ring dan m, n adalah bilangan-bilangan bulat, maka:

1. $(m+n)a = ma + na$
2. $m(a+b) = ma + mb$
3. $m(na) = (mn)a = n(ma)$

Definisi 2.2.5 1. Diberikan ring R dan $a \in R$, m adalah bilangan bulat positif, didefinisikan:

$a^m = \underbrace{a.a.a...a}_{m}$

2. Jika $a \in R$ dan $a^2 = a$, maka a disebut elemen **idempotent** dari R.

3. Jika $a \in R$ dan ada bilangan bulat positif *n* sehingga $a^n = z$, maka a disebut elemen **nilpotent** dari R.

Definisi 2.2.6. Diberikan ring R. JIka ada bilangan bulat positif terkecil *n* sehingga $na = z$ untuk setiap $a \in R$, maka n disebut **karakteristik** (characteristic) dari ring R . Jika tidak ada bilangan yang demikian, maka karakteristik dari ring R dikatan 0 atau takhingga.

Contoh 2.2.3

1. Karakteristik dari ring $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ adalah 0.
2. Karakteristik dari ring $n\mathbb{Z}$ adalah 0.
3. Karakteristik dari ring $\mathbb{Z}_n$ adalah n.

Teorema 2.2.5 Jika R adalah daerah integral, maka karakteristik dari R adalah 0 atau bilangan prima.

Teorema 2.2.6 Jika R adalah daerah integral berhingga, maka karakteristik dari R adalah bilangan prima.

Latihan 2.2.1

Tentukan karakteristik dari ring berikut ini.

1. $2\mathbb{Z}$
2. $\mathbb{Z} \times \mathbb{Z}$

3. $\mathbb{Z}_3 \times 3\mathbb{Z}$

4. $\mathbb{Z}_3 \times \mathbb{Z}_3$

5. $\mathbb{Z}_3 \times \mathbb{Z}_4$

6. $\mathbb{Z}_6 \times \mathbb{Z}_{15}$

7. Misalkan R adalah ring komutatif dengan elemen kesatuan dan mempunyai karakteristik 3. Sederhanakan bentuk $(a+b)^4$ untuk setiap $a,b \in R$.

8. Misalkan R adalah ring komutatif dengan elemen kesatuan dan mempunyai karakteristik 3. Sederhanakan bentuk $(a+b)^3$ untuk setiap $a,b \in R$.

9. Misalkan R adalah ring komutatif dengan elemen kesatuan dan mempunyai karakteristik p dengan p adalah prima. Sederhanakan bentuk $(a+b)^p$ untuk setiap $a,b \in R$.

10. Jika R adalah daerah integral order m, maka karakteristik R membagi m.

11. Jika F lapangan order 8, tentukan karakteristik dari F.

12. Jika F lapangan order 2^n, tentukan karakteristik dari F.

13. Jika F lapangan order p^n dengan p prima, tentukan karakteristik dari F.

14. Tentukan semua elemen nilpotent dari daerah integral R.

15. Tentukan semua elemen idempotent dari daerah integral R.

16. Tentukan semua elemen nilpotent sekaligus idempotent dari daerah integral R.

17. Diberikan ring R dengan elemen kesatuan u dan $a \in R$. Misalkan $a^n = z$ untuk suatu bilangan bulat positif n, buktikan bahwa $u-a$ mempunyai invers terhadap perkalian di R. (petunjuk: jabarkan $(u-a)(1+a+a^2+...+a^{n-1})$).

2.2.1 Subring dan sifat-sifatnya

Definisi 2.2.7 Diberikan ring $(R,+,\bullet)$ dan $S \neq \phi$, $S \subset R$. Himpunan S disebut subring dari R jika $(S,+,\bullet)$ juga ring.

Contoh 2.2.4 Ring $\mathbb{Z}$ adalah subring dari $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$. Ring $\mathbb{Q}$ subring dari $\mathbb{R}$ dan $\mathbb{C}$. Ring $\mathbb{R}$ subring dari $\mathbb{C}$.

Teorema 2.2.7 Diberikan ring $(R,+,\bullet)$, $S \neq \phi$ dan $S \subset R$. Himpunan S subring dari R jika dan hanya jika untuk setiap $a,b \in S$ berlaku (i). $a-b \in S$, (ii). $ab \in S$

Teorema 2.2.8: Jika S dan T adalah subring dari R, maka $S \cap T$ juga subring dari R.

Latihan 2.2.2

1. Tentukan semua subring dari $\mathbb{Z}_{15}$.

2. Tentukan semua subring dari $\mathbb{Z}_7$.

2.2.2 Ideal dan Sifat-sifatnya

Definisi 2.2.8 MIsalkan R adalah ring. Suatu himpunan tidak kosong $I \subseteq R$ dikatakan ideal kiri (kanan) dari R jika $\forall a,b \in I, \forall r \in R \quad a-b \in I, ra \in I$ ($a-b \in I, ar \in I$). Selanjutnya suatu himpunan tidak kosong $I \subseteq R$ disebut ideal jika I ideal kiri dan ideal kanan dari R.

Contoh 2.2.5

Diberikan ring $M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a,b,c,d \in \mathbb{Z} \right\}$. Himpunan $I_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a,b,c,d \in 2\mathbb{Z} \right\}$ adalah ideal dari $M_2(\mathbb{Z})$ dan $I_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \, a \in \mathbb{Z} \right\}$ bukan ideal dari $M_2(\mathbb{Z})$.

Teorema 2.2.9 Misalkan R suatu ring. Jika A dan B ideal-ideal dari R, maka $A \cap B$ dan $A+B = \{a+b \mid a \in A, b \in B\}$ juga ideal-ideal dari R.

Teorema 2.2.10 Misalkan R suatu ring komutatif dengan elemen kesatuan u. Ring R merupakan lapangan jika dan hanya jika R tidak mempunyai ideal sejati.

Teorema 2.2.11 Misalkan R suatu ring dan $\{I_\alpha \mid \alpha \in \Lambda\}$ adalah koleksi tak kosong ideal kiri (kanan) dari R, maka $\bigcap_{\alpha \in \Lambda} I_\alpha$ ideal kiri (kanan) dari R.

Teorema 2.2.12 Jika R ring dengan elemen kesatuan dan A ideal yang memuat unit, maka A = R.

Definisi 2.2.9 Misalkan R suatu ring. Suatu ideal $I \neq R$, disebut ideal maksimal dari R jika ada ideal lain A dari R sedemikian hingga $I \subseteq A \subseteq R$, maka $I = A$ atau $A = R$. Dengan kata lain, ideal I dari R dikatakan ideal maksimal jika tidak ada ideal sejati dari R yang memuat I.

Definisi 2.2.10 Misalkan R suatu ring komutatif. Suatu ideal I dari R dengan $I \neq R$ dikatakan ideal prima jika untuk setiap $ab \in I$ berakibat $a \in I$ atau $b \in I$.

Contoh 2.2.6 Misalkan p adalah bilangan prima, maka $p\mathbb{Z}$ adalah ideal maksimal dan ideal prima dari $\mathbb{Z}$. Selanjutnya $\{0\}$ ideal prima dari $\mathbb{Z}$ tetapi bukan ideal maksimal dari $\mathbb{Z}$.

2.2.3 Ring Faktor dan sifat-sifatnya

Misalkan R suatu ring dan I suatu ideal dari R, didefinisikan himpunan $R/I = \{I + a \mid a \in R\}$ dan didefinisikan dua operasi (+) dan (.) pada R/I yaitu untuk setiap $(I+a),(I+b) \in R/I$

$(I+a)+(I+b) = I+(a+b)$

$(I+a)(I+b) = I+a$

Dapat ditunjukkan bahwa $(R/I, +, .)$ adalah suatu ring.

Teorema 2.2.13 Misalkan R suatu ring komutatif dengan elemen kesatuan dan I ideal dari R. Ring R/I merupakan lapangan jika dan hanya jika I ideal maksimal.

Teorema 2.2.14 Misalkan R suatu ring komutatif dengan elemen kesatuan dan I ideal dari R. Ring R/I merupakan daerah integral jika dan hanya jika I ideal prima.

Teorema 2.2.15 Jika R suatu ring komutatif dengan elemen kesatuan dan I ideal maksimal dari R, maka I ideal prima dari R.

2.2.4 Homomorpisma ring dan sifat-sifatnya

Diberikan ring R_1, R_2. Misalkan $f : R_1 \to R_2$ adalah suatu fungsi dari R_1 ke R_2. Fungsi f dikatakan **homomorpisma** ring jika untuk setiap $a,b \in R_1$ berlaku

1. $f(a+b) = f(a) + f(b)$
2. $f(a\ b) = f(a)f(b)$

Suatu homomorpisma ring yang injektif disebut **monomorpisma** ring. Suatu homomorpisma ring yang surjektif disebut **epimorpisma** ring dan suatu homomorpisma ring yang injektif dan surjektif disebut **isomorpisma** ring

Teorema 2.2.16 Misalkan $f : R_1 \to R_2$ adalah suatu homomorpisma ring, maka pernyataan-pernyataan berikut berlaku.

1. $f(z_1) = z_2$ dengan z_1, z_2 berturut-turut elemen nol dari R_1 dan R_2.
2. $f(-a) = -f(a), \forall a \in R_1$
3. $f(R_1) = \{f(a) \mid a \in R_1\}$ adalah subring dari R_2.
4. JIka R_1 komutatif, maka $f(R_1) = \{f(a) \mid a \in R_1\}$ juga komutatif.

5. Jika R_1 mempunyai elemen kesatuan u dan $f(R_1) = \{ f(a) \mid a \in R_1 \} = R_2$, maka R_2 mempunyai elemen kesatuan yaitu $f(u)$

6. Jika R_1 mempunyai elemen kesatuan u dan $f(R_1) = \{ f(a) \mid a \in R_1 \} = R_2$ dan a suatu unit, maka $f(a)$ unit di R_2 dan $f(a)^{-1} = f(a^{-1})$.

Definisi 2.2.11 Misalkan $f : R_1 \to R_2$ adalah suatu homomorpisma ring. Didefinisikan kernel dari f, ditulis Ker f, sebagai $Ker\ f = \{a \in R_1 \mid f(a) = z_2\}$.

Teorema 2.2.17 Jika $f : R_1 \to R_2$ adalah suatu homomorpisma ring, maka $Ker\ f$ adalah ideal dari R_1.

Teorema 2.2.18 Misalkan $f : R_1 \to R_2$ adalah suatu homomorpisma ring, maka $Ker\ f = \{z_1\}$ jika dan hanya jika f injektif.

Teorema 2.2.19 (Teorema isomorpisma pertama) Jika $f : R_1 \to R_2$ adalah suatu homomorpisma ring dan $I = Ker\ f$, maka $R_1/I \cong f(R_1)$.

Teorema 2.2.20 (Teorema isomorpisma kedua) Misalkan A subring dari ring R dan B ideal dari R, maka A + B subring dari R dan B ideal dari A + B dan $A+B/B \cong A/A \cap B$.

Teorema 2.2.21 (Teorema isomorpisma ketiga) Jika A dan B ideal-ideal dari R dengan $A \subset B$, maka $R/B \cong \dfrac{R/A}{B/A}$.

2.2.5 Ring Polinomial

Misalkan *R* suatu ring. Didefinisikan $(a_0, a_1, a_2, ...)$ sebagai barisan takhingga dengan $a_i \in R, i = 0,1,2,...$ dan ada bilangan bulat taknegatif *n* (bergantung pada $(a_0, a_1, a_2, ...)$) sedemikian sehingga untuk semua bilangan bulat $k \geq n, a_k = z$. Selanjutnya didefinisikan $R[x] = \left\{ (a_0, a_1, a_2, ...) \mid a_i \in R, i = 0,1,2,... \right\}$. Elemen-elemen dari $R[x]$ disebut polinomial-polinomial atas *R*.

Didefinisikan operasi penjumlahan dan pergandaan pada $R[x]$ sebagai berikut:

Untuk setiap $(a_0, a_1, a_2, ...)$, $(b_0, b_1, b_2, ...)$ pada $R[x]$,

$(a_0, a_1, a_2, ...)$ + $(b_0, b_1, b_2, ...)$ = $(a_0 + b_0, a_1 + b_1, a_2 + b_2, ...)$

$(a_0, a_1, a_2, ...)$. $(b_0, b_1, b_2, ...)$ = $(c_0, c_1, c_2, ...)$ dengan $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ for *i* = 0, 1, 2, …

Cek bahwa ($R[x]$, +, .) adalah ring dengan $(z, z, z, ...)$ adalah elemen nol dari $R[x]$ dan invers terhadap penjumlahan dari $(a_0, a_1, a_2, ...)$ adalah $(-a_0, -a_1, -a_2, ...)$.

Selanjutnya ring $R[x]$ disebut ring polinomial atas *R*.

Definisikan $f : R \to R[x]$ dengan $f(a) = (a, z, z, z, ...)$ untuk setiap $a \in R$.

Dapat ditunjukkan bahwa f suatu monomorpisma dari *R* ke $R[x]$, sehingga R dikatakan tersisipkan (embedded) dalam $R[x]$ dan kita dapat memandang R sebagai subring dari $R[x]$. Jadi selanjutnya kita tidak membedakan antara *a* dan $(a, z, z, z, ...)$.

Misalkan $(a, z, z, z, ...)$ dinyatakan dengan $a = ax^0$

$(z, a, z, z, ...)$ dinyatakan dengan $ax = ax^1$

$(z, z, a, z, ...)$ dinyatakan dengan ax^2

maka

$$(a_0, a_1, a_2, ..., a_n, z, ...) = (a_0, z, z, ...) + (z, a_1, z, ...) + ... + (z, z, ..., a_n, z, ...)$$

= $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ sebagai polinomil atas *R*.

Simbol *x* disebut **indeterminate** atas *R* dan elemen-elemen $a_0, a_1, a_2, ..., a_n$ dari *R* disebut **koefisien-koefisien** dari $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$.

Alasan dua polinomial $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ dan $b_0 + b_1 x + b_2 x^2 + ... + b_m x^m$ sama jika dan hanya jika *n* = *m* dan $a_i = b_i, i = 0, 1, 2, ..., n$ adalah bahwa dua barisan $(a_0, a_1, a_2, ..., a_n, z, ...)$ dan $(b_0, b_1, b_2, ..., b_m, z, ...)$ sama jika dan hanya jika n = m dan $a_i = b_i, i = 0, 1, 2, ...$

Coba dicek bahwa:

1. Jika ring R komutatif, maka $R[x]$ juga komutatif.

2. Jika ring R mempunyai elemen kesatuan *u*, maka $R[x]$ juga mempunyai elemen kesatuan yaitu $(u, z, z, \ldots)$.

3. Jika ring R daerah integral, maka $R[x]$ juga daerah integral.

Definisi 2.2.12 Misalkan R adalah suatu ring. Jika $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, $a_n \neq z$ adalah polinomial di $R[x]$, maka n disebut derajat (*degree*) dari *f*(*x*), ditulis deg *f*(*x*), dan a_n disebut koefisien pemimpin (*leading coefficient*) dari *f*(*x*). Jika R mempunyai elemen kesatuan *u* dan $a_n = u$, maka *f*(*x*) disebut **polinomial monik**.

Catatan: polinomial $z \in R[x]$ tidak mempunyai derajat.

Teorema 2.2.22 Diberikan ring polinomial $R[x]$ dan $f(x), g(x) \in R[x]$.

(i). Jika $f(x).g(x) \neq z$, maka deg $(f(x).g(x)) \leq \deg f(x) + \deg g(x)$.

(ii).Jika $f(x) + g(x) \neq z$, maka deg$(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.

Catatan: Jika R daerah integral, maka deg $(f(x).g(x)) = \deg f(x) + \deg g(x)$.

Pertanyaan:

Jika *F* lapangan, apakah *F*[x] juga lapangan? Gunakan Teorema 7.1 untuk melihat apakah semua elemen derajat satu atau lebih dari F[x] mempunyai invers terhadap perkalian.

Contoh 2.2.7 Diberikan ring polinomial $\mathbb{Z}_6[x]$ dan $f(x) = [1] + [2]x^2$, $g(x) = [1] + [3]x$ serta $h(x) = [5] + [4]x^2$, maka $f(x)g(x) = [1] + [3]x + [2]x^2$ dan $f(x) + h(x) = [6] + [6]x^2 = [0]$. Selanjutnya, $\deg f(x)g(x) = 2 < 3 = \deg f(x) + \deg g(x)$ dan $\deg(f(x) + h(x))$ tak didefinisikan.

Latihan 2.2.3

1. Jika *I* ideal dari ring *R*, tunjukkan bahwa $I[x]$ juga ideal dari *R*[x].

2. Jika *R* daerah integral, buktikan bahwa *R* dan *R*[x] mempunyai karakteristik sama.

3. Jika *F* lapangan, tentukan semua elemen dari *F*[x] yang mempunyai invers terhadap perkalian.

4. Jika F lapangan dengan delapan elemen, berapa banyak elemen dari F[x] yang mempunyai invers terhadap perkalian?

Teorema 2.2.23 Misalkan R ring komutatif dengan elemen kesatuan u dan $f(x), g(x) \in R[x]$ dengan koefisien pemimpin dari $g(x)$ suatu unit di R, maka ada dengan tunggal polinomial $q(x), r(x) \in R[x]$ sedemikian sehingga

$$f(x) = q(x)g(x) + r(x)$$

dengan $r(x) = z$ atau $\deg r(x) < \deg g(x)$.

Polinomial $q(x), r(x)$ dalam Teorema 7.2 berturut-turut disebut hasil bagi dan sisa pembagian f(x) oleh g(x).

Contoh 2.2.8

1. Misalkan $f(x) = 2 + 2x^2 + 3x^3 + x^4$ dan $g(x) = 1 + 2x + x^2 \in \mathbb{Q}[x]$, Carilah polinomial $q(x), r(x) \in \mathbb{Q}[x]$ sedemikian sehingga $f(x) = q(x)g(x) + r(x)$ dengan $r(x) = z$ atau $\deg r(x) < \deg g(x)$.

Definisi 2.2.13 Misalkan R suatu ring komutatif dengan elemen kesatuan u dan

$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \in R[x]$. Didefinisikan untuk semua $r \in R$,

$$f(r) = a_0 + a_1 r + a_2 r^2 + ... + a_n r^n$$

Jika $f(r) = z$, maka r disebut akar dari f(x).

Definsi 2.2.14 Misalkan R suatu ring komutatif dengan elemen kesatuan u dan $f(x), g(x) \in R[x]$ sedemikian sehingga $g(x) \neq z$. Polinomial g(x) dikatakan membagi f(x) atau g(x) faktor dari f(x), ditulis $g(x) \mid f(x)$, jika ada polinomial $q(x) \in R[x]$ sedemikian sehingga $f(x) = q(x)g(x)$.

Teorema 2.2.24 (Teorema Sisa) Misalkan R suatu ring komutatif dengan elemen kesatuan u. Untuk $f(x) \in R[x]$ dan $a \in R$, ada polinomial $q(x) \in R[x]$ sedemikian sehingga $f(x) = (x - a)q(x) + f(a)$.

Akibat 2.2.25 (Teorema faktorisasi): Misalkan R suatu ring komutatif dengan elemen kesatuan u. Untuk $f(x) \in R[x]$ dan $a \in R$, $x - a$ membagi $f(x)$ jika dan hanya jika *a* akar dari $f(x)$.

Teorema 2.2.26 Misalkan R daerah integral dan $f(x) \in R[x]$ dengan $f(x)$ polinomial taknol derajat *n*, maka $f(x)$ mempunyai paling banyak *n* akar di R.

Contoh 2.2.9

1. Diberikan $f(x) = [3] + [3]x + x^2, g(x) = [2] + [3]x + x^2 \in \mathbb{Z}_4[x]$, maka

$$f([0]) = [3], f([1]) = [3], f([2]) = [1], f([3]) = [1]$$
$$g([0]) = [2], g([1]) = [2], g([2]) = [0], g([3]) = [0]$$

$$f(x) = (x - [0])(x + [3]) + [3], \quad f(x) = (x - [2])(x + [1]) + [1]$$

$$g(x) = (x - [1])x + [2], \quad g(x) = (x - [2])(x + [3]) + [0], \quad g(x) = (x - [3])(x + [2]) + [0]$$

Latihan 2.2.4

1. Di dalam ring $\mathbb{Z}_8[x]$, tunjukkan bahwa $[1] + [2]x$ unit.

2. Apakah $1 + 5x$ suatu unit di Z[x]?

3. Di dalam ring $\mathbb{Z}_8[x]$, buktikan bahwa:

(a). $[4] + [2]x + [4]x^2$ suatu pembagi nol.

(b). $[2]x$ suatu elemen nilpotent.

(c). $[1] + [4]x$ dan $[3] + [4]x$ unit.

4. Misalkan $f(x) = [2] + [2]x^2 + [3]x^3 + x^4$ dan $g(x) = [1] + [2]x + x^2 \in \mathbb{Z}_5[x]$, tentukan polinomial $q(x), r(x) \in \mathbb{Z}_5[x]$ sehingga $f(x) = q(x)g(x) + r(x)$

Dengan $r(x) = z$ atau $\deg r(x) < \deg g(x)$.

Misalkan R suatu ring dan $f(x) \in R[x]$. Suatu polinomial taknol dan bukan unit $f(x)$ disebut ireducibel (**irreducible**) di $R[x]$ jika $f(x) = g(x)h(x)$ berakibat $g(x)$ unit atau $h(x)$ unit di $R[x]$. Suatu polinomial $f(x)$ disebut reducibel (**reducible)** di $R[x]$ jika $f(x)$ tidak ireducibel di $R[x]$.

Polinomial taknol $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ di $R[x]$ disebut polinomial primitif (**primitive polynomial**) jika FPB(a_0, a_1, …, a_n) suatu unit di *R*.

Cntoh 2.2.10

1. Polinomial $f(x) = x^2 + 1$ irreducible di $\mathbb{R}[x]$ tetapi reducible di $\mathbb{C}[x]$.

2. Apakah polinomial $g(x) = x^2 - 2$ irreducible di $\mathbb{Q}[x]$?

3. Apakah polinomial $g(x) = x^2 - 2$ irreducible di $\mathbb{R}[x]$?

4. Jika F lapangan, maka polinomial $g(x) = ax + b \in F[x]$ dengan $a \neq z$ irreducible.

Teorema 2.2.27 (Einsenstein's irreducibility criterion). (Malik, D.S., et.al, 1997) Misalkan D suatu UFD dan Q(D) suatu lapangan kuosen dari D. Misalkan $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ suatu polinomial tak konstan di D[x]. Andaikan D memuat elemen prima *p* sedemikian sehingga

(i). $p \mid a_i$, $i = 0,1,2,...,n-1$

(ii). $p \nmid a_n$

(iii). $p^2 \nmid a_0$

maka f(x) irreducible di Q(D)[x].

Contoh 2.2.11 Verifikasi ireducibilitas dari polinomial-polinomial berikut ini.

1. $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ irreducible atas Q sebab ada bilangan prima $5 \in \mathbb{Z}$ sedemikian sehingga $5 \mid 20, 5 \mid 10, 5 \mid -20, 5 \mid 15, 5 \nmid 3, 25 \nmid 20$, maka berdasarkan kriteria ireducibilitas Einsenstein, $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ irreducible atas Q.

Akibat 2.2.28 (Malik, D.S., et.al, 1997) Misalkan D suatu UFD

dan $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ suatu polinomial primitif tak konstan di D[x]. Misalkan D memuat elemen prima p sedemikian sehingga

(i). $p \mid a_i$, $i = 0,1,2,...,n-1$

(ii). $p \nmid a_n$

(iii). $p^2 \nmid a_0$

maka f(x) irreducible pada D[x].

Contoh 2.2.12

1. $f(x) = x^5 + 15x^3 + 10x + 5$ irreducible di Z[x] sebab Z adalah UFD dan *content* dari $f(x)$ adalah 1, maka $f(x)$ polinomial primitif tak konstan di Z[x], dan $5 \mid 5, 5 \mid 10, 5 \mid 0, 5 \mid 15, 5 \nmid 1, 25 \nmid 5$, sehingga dengan Akibat 7.7, $f(x)$ irreducible di Z[x].

Akibat 2.2.29 (Malik, D.S., et.al, 1997) Misalkan $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ polinomial tak konstan di Z[x]. Jika ada bilangan prima p sedemikian sehingga

(i). $p \mid a_i$, $i = 0,1,2,...,n-1$

(ii). $p \nmid a_n$

(iii). $p^2 \nmid a_0$

maka f(x) irreducible di Q[x].

Teorema 2.2.30 (Malik, D.S., et.al, 1997) Misalkan F suatu lapangan. Jika $f(x)$ di F[x] dan deg ($f(x)$) 2 atau 3, maka $f(x)$ ireducibel atas F jika dan hanya jika $f(x)$ tidak mempunyai akar di F.

Contoh 2.2.13

1. Gunakan Teorema 7.9 untuk mengecek ireducibilitas polinomial dalam Contoh 7.4.

2. Misalkan $f(x)=x^2+x+[1]\in\mathbb{Z}_2[x]$ dengan $f([0])=[1]\neq[0]; f([1])=[1]\neq[0]$, maka dengan Teorema 7.9, $f(x)$ ireducibel atas $\mathbb{Z}_2$.

3. Apakah polinomial $f(x)=x^3+[2]x+[1]\in\mathbb{Z}_3[x]$ ireducibel atas $\mathbb{Z}_3$?

Teorema 2.2.31 (Gallian, et.al, 2010) Diberikan $f(x)\in\mathbb{Z}[x]$. Jika $f(x)$ ireducibel atas Q, maka $f(x)$ ireducibel atas Z.

Teorema 2.2.32 (Gallian, et.al, 2010) Misalkan *p* suatu bilangan prima dan $f(x)\in\mathbb{Z}[x]$ dengan deg ($f(x)$) ≥ 1. Misalkan $\overline{f}(x)\in\mathbb{Z}_p[x]$ ditentukan dari $f(x)$ dengan menuliskan semua koefisien dari $f(x)$ dalam modulo p. Jika $\overline{f}(x)$ ireducibel atas Z_p dan deg $\overline{f}(x)$ = deg $f(x)$, maka $f(x)$ ireducibel atas Q.

Contoh 2.2.14

1. Diberikan polinomial $f(x)=\frac{5}{7}x^3-\frac{1}{2}x+1\in Q[x]$, maka $14f(x)=10x^3-7x+14$ di $\mathbb{Z}[x]$ dan misalkan $f_1(x)=10x^3-7x+14$ di $\mathbb{Z}[x]$. Ambil bilangan prima 3 dan bentuk $\overline{f_1}(x)=x^3+[2]x+[2]$ di $\mathbb{Z}_3[x]$. Selanjutnya $\overline{f_1}([0])=[2], \overline{f_1}([1])=[2], \overline{f_1}([2])=[2]$, maka $\overline{f_1}(x)$ tidak punya akar di $\mathbb{Z}_3$, sehingga $\overline{f_1}(x)$ ireducibel di $\mathbb{Z}_3[x]$. Deg $\overline{f_1}(x)$ = deg $f_1(x)$, dengan Teorema 7.11, $f_1(x)$ = 14 $f(x)$ ireducibel di $\mathbb{Q}[x]$. Karena 14 adalah unit di $\mathbb{Q}[x]$, maka $f(x)$ ireducibel di $\mathbb{Q}[x]$.

2. Misalkan $f(x)=21x^3-3x^2+2x+9\in\mathbb{Z}[x]$, maka $\overline{f}(x)=x^3+x^2+1$ di Z_2 dan $\overline{f}([0])=[1], \overline{f}([1])=[1]$, maka $\overline{f}(x)$ ireducibel atas Z_2, dengan Teorema 7.11, $f(x)$ ireducibel atas Q.

Teorema 2.2.33 (Malik, D.S., et.al, 1997) Polinomial cyclotomic

$f(x)=1+x+x^2+...+x^p=\dfrac{x^p-1}{x-1}$ ireducibel di Z[x] dengan p prima.

Latihan 2.2.5 Selidiki ireducibilitas dari polinomial-polinomial berikut ini.

1. $f(x) = x^3 + [1] \in \mathbb{Z}_2[x]$.

2. $f(x) = x^2 + [2]x + [6] \in \mathbb{Z}_2[x]$

3. $f(x) = x^2 + 2x + 6 \in \mathbb{Z}[x]$

4. $f(x) = 2x^4 + 6x^3 - 9x^2 + 1 \in \mathbb{Z}[x]$

5. $f(x) = 2x^3 - x^2 + 4x - 2 \in \mathbb{Z}[x]$

Diberikan ring komutatif R dan $p(x) \in R[x]$. Didefinisikan $I = \{ p(x)f(x) \mid f(x) \in R[x] \}$. Mudah dicek bahwa I adalah ideal dari $R[x]$ dan ideal I disebut **ideal yang dibangun oleh $p(x)$,** dinotasikan dengan $I = \langle p(x) \rangle$.

Contoh 2.2.15

Jika R suatu ring komutatif dengan elemen kesatuan u, maka ideal dair R[x] yang dibangun oleh u adalah $I = \langle u \rangle = \{ u\, f(x) \mid f(x) \in R[x] \} = \{ f(x) \mid f(x) \in R[x] \} = R[x]$.

Teorema 2.2.34 (Gallian, et.al, 2010) Misalkan *F* suatu lapangan dan $p(x) \in F[x]$. $\langle p(x) \rangle$ adalah ideal maximal di $F[x]$ jika dan hanya jika $p(x)$ ireducibel atas *F*.

Teorema 2.2.35 (Gallian, et.al, 2010) Jika *F* suatu lapangan dan $p(x)$ suatu polinomial ireducibel atas *F*, maka $F[x] / \langle p(x) \rangle$ suatu lapangan.

Jika p adalah bilangan prima, suatu lapangan hingga dengan p elemen adalah $\mathbb{Z}_p$.

Langkah-langah konstruksi lapangan hingga dengan p^n elemen dengan p bilangan prima dan n > 1:

1. Ambil lapangan hingga $\mathbb{Z}_p$.

2. Cari polinomial ireducibel $p(x)$ di $\mathbb{Z}_p[x]$ dengan $\deg p(x) = n$.

3. Bentuk lapangan hingga $\mathbb{Z}_p[x] / \langle p(x) \rangle = \{ f(x) + \langle p(x) \rangle \mid f(x) \in \mathbb{Z}_p[x] \}$.

Lapangan hingga $\mathbb{Z}_p[x] \big/ \langle p(x) \rangle$ mempunyai p^n elemen.

Contoh 2.2.16

1. Bentuk lapangan hingga dengan delapan elemen.

Jawab: $8 = 2^3$, p = 2, n = 3.

1. Ambil lapangan hingga $\mathbb{Z}_2 = \{[0],[1]\}$.

2. Cari polinomial ireducibel $p(x)$ di $\mathbb{Z}_2[x]$ dengan $\deg p(x) = 3$. Kita ambil $p(x) = x^3 + x + [1]$, dan $p(x)$ tidak mempunyai akar di $\mathbb{Z}_2$ sehingga $p(x)$ ireducibel di $\mathbb{Z}_2[x]$.

3. Bentuk lapangan hingga $\mathbb{Z}_2[x] \big/ \langle x^3 + x + [1] \rangle = \left\{ f(x) + \langle x^3 + x + [1] \rangle \mid f(x) \in \mathbb{Z}_2[x] \right\}$.

Maka $\mathbb{Z}_2[x] \big/ \langle x^3 + x + [1] \rangle = \left\{ (a_2x^2 + a_1x + a_0) + \langle x^3 + x + [1] \rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_2 \right\}$

$$\mathbb{Z}_2[x] \big/ \langle x^3 + x + [1] \rangle = \{[0] + \langle x^3 + x + [1] \rangle, [1] + \langle x^3 + x + [1] \rangle, x + \langle x^3 + x + [1] \rangle, x + [1] + \langle x^3 + x + [1] \rangle,$$

$$x^2 + \langle x^3 + x + [1] \rangle, x^2 + [1] + \langle x^3 + x + [1] \rangle, x^2 + x + \langle x^3 + x + [1] \rangle, x^2 + x + [1] + \langle x^3 + x + [1] \rangle\}$$

Untuk menyederhanakan notasi, $a_2x^2 + a_1x + a_0 + \langle x^3 + x + 1 \rangle$ ditulis dengan $a_2x^2 + a_1x + a_0$.

Jadi $\mathbb{Z}_2[x] \big/ \langle x^3 + x + [1] \rangle = \{[0], [1], x, x + [1],\ x^2, x^2 + [1], x^2 + x, x^2 + x + [1]\}$

2. Bentuk lapangan hingga dengan sembilan elemen.

jawab: $9 = 3^2$, p = 3, n = 2.

1. Ambil lapangan hingga $\mathbb{Z}_3 = \{[0],[1],[2]\}$.

2. Cari polinomial ireducibel $p(x)$ di $\mathbb{Z}_3[x]$ dengan $\deg p(x) = 2$. Kita ambil $p(x) = x^2 + [1]$, dan $p(x)$ tidak mempunyai akar di $\mathbb{Z}_3$ sehingga $p(x)$ ireducibel di $\mathbb{Z}_3[x]$.

3. Bentuk lapangan hingga $\mathbb{Z}_3[x] \big/ \langle x^2 + [1] \rangle = \left\{ f(x) + \langle x^2 + [1] \rangle \mid f(x) \in \mathbb{Z}_3[x] \right\}$.

Maka $\mathbb{Z}_3[x] \big/ \langle x^2+[1] \rangle = \left\{ (a_1x+a_0)+\langle x^2+[1] \rangle \mid a_0, a_1 \in \mathbb{Z}_3 \right\}$

$$\mathbb{Z}_3[x] \big/ \langle x^2+[1] \rangle = \left\{ [0],[1],[2],x,x+[1],x+[2],[2]x,[2]x+[1],[2]x+[2] \right\}$$

Latihan 2.2.6

1. Lengkapi tabel penjumlahan dan perkalian dari lapangan hingga Contoh 7.10 bagian 1.
2. Bentuk lapangan hingga dengan 4 elemen.
3. Bentuk lapangan hingga dengan 16 elemen.
4. Bentuk lapangan hingga dengan 25 elemen.
5. Bentuk lapangan hingga dengan 27 elemen.
6. Bentuk lapangan hingga dengan 32 elemen.
7. Bentuk lapangan hingga dengan 64 elemen.

Daftar Pustaka

Adkins, W.A. and Weintraub, S.H.. 1992. *Algebra: An Approach via Module Theory*. Paris: Springer-Verlag.

Fraleigh, J.B.. 1989. *A First Course in Abstract Algebra. Fourth Edition*. Canada: Addison-Wesley Publishing Company.

Gallian, J.A.. 1990. *Contemporary Abstract Algebra. Second Edition*. Toronto: D.C. Heath and Company.

Herstein, I.N.. 1975. *Topics in Algebra. Second Edition*. Singapore: John Wiley & Sons.

Herstein, I.N..1996. *Abstract Algebra. Third Edition*. Upper Saddle River: Prentice-Hall Int. Inc.

Lang, S.. 1993. *Algebra. Third Edition*. New York: Addison-Wesley Publishing Company.

Malik, D.S. , Mordeson, J.M., Sen, M.K.. 1997. *Fundamentals of Abstract Algebra*. New York: McGraw-Hill Companies, Inc.

Raisnghania, M.D. and Aggarwal, R.S.. 1980. *Modern Algebra*. Ram Nagar: S. Chand & Company Ltd.

Sukirman. 2006. *Aljabar Abstrak Lanjut: Teori Gelanggang*. Yogyakarta: Hanggar Kreator.