Bab 5

Matematika II - Polynomial Field

Di ahir bab 3 kita melihat bagaimana aritmatika modulo sebuah bilangan prima mempunyai struktur *finite field*. *Finite field* seperti itu dinamakan *prime field*, dan dari *prime field*, kita dapat membuat *field* yang lebih besar yang dinamakan *polynomial field*. Dalam bab ini kita akan bahas aritmatika *polynomial field*, yang digunakan antara lain dalam enkripsi AES, dimana transformasi *affine* dengan aritmatika *polynomial field* digunakan untuk substitusi. Pembaca yang cukup paham dengan *cyclic redundancy check* (CRC) tentunya mengetahui bahwa CRC juga menggunakan aritmatika *polynomial field*.

Sebelum membahas aritmatika *polynomial field*, kita perlu kembangkan dahulu teori mengenai *ring* dengan membahas beberapa konsep, antara lain konsep *integral domain*, *homomorphism*, *ideal* dalam suatu *ring*, *principal ideal domain*, *polynomial ring* dan *irreducible polynomial*.

Notasi logika matematika akan banyak digunakan di bab ini. Tabel 5.1 menjelaskan notasi logika yang digunakan.

Beberapa pembuktian matematika di bab ini akan menggunakan rantaian $\Longrightarrow$ dan rantaian $\Longleftrightarrow$. Pembuktian dengan bentuk

$$A_1 \Longrightarrow A_2 \Longrightarrow A_3 \Longrightarrow A_4$$

agar dibaca sebagai A_4 merupakan konsekuensi dari A_3, yang merupakan konsekuensi dari A_2, yang merupakan konsekuensi dari A_1. Demikian juga, pembuktian dengan bentuk

$$A_1 \Longleftrightarrow A_2 \Longleftrightarrow A_3 \Longleftrightarrow A_4$$

agar dibaca sebagai A_4 ekuivalen dengan A_3, yang ekuivalen dengan A_2, yang ekuivalen dengan A_1.

Notasi	**Penjelasan**
$A \Longrightarrow B$	A hanya jika B (atau B jika A).
$A \Longleftrightarrow B$	A jika dan hanya jika B.
$A \wedge B$	A dan B.
$A \vee B$	A atau B.
$\neg A$	Tidak A.
$\forall x : P(x)$	Untuk setiap x, $P(x)$ berlaku.
$\forall x \in S : P(x)$	Untuk setiap $x \in S$, $P(x)$ berlaku.
$\exists x : P(x)$	Terdapat x dimana $P(x)$ berlaku.
$\exists x \in S : P(x)$	Terdapat $x \in S$ dimana $P(x)$ berlaku.

Tabel 5.1: Tabel Notasi Logika Matematika

5.1 Integral Domain

Kita akan mulai dengan membahas konsep *integral domain*, tetapi sebelumnya kita definisikan konsep *zero divisor* dan *unit*.

Definisi 9 *Untuk ring R dan elemen $a \in R$,*

- *$a \neq 0$ adalah zero divisor jika ada $0 \neq b \in R$ dengan $ab = 0$,*
- *a adalah unit jika a mempunyai inverse.*

Suatu *zero divisor* tidak mungkin juga merupakan *unit* karena jika $a \in R$ adalah *zero divisor*, maka terdapat $0 \neq b \in R$ dengan $ab = 0$, sedangkan jika a juga merupakan *unit*, maka terdapat $0 \neq c \in R$ dengan $ac = 1$, jadi $0 = c \cdot 0 = c(ab) = (ac)b = 1 \cdot b = b$, suatu kontradiksi.

Suatu *ring* yang tidak mempunyai *zero divisor* dinamakan *integral domain*. $\mathbf{Z}$ merupakan *integral domain* karena dalam aritmatika bilangan bulat tidak ada *zero divisor*.

Teorema 12 *Jika R merupakan suatu integral domain, $a, b, c \in R \setminus \{0\}$, dan $ab = ac$, maka $b = c$. Menggunakan notasi logika:*

$$\forall a, b, c \in R \setminus \{0\} : (ab = ac) \Longrightarrow (b = c).$$

Kita buktikan teorema 12 secara kontra-positif. Jika $b \neq c$ maka konsekuensi $ab = ac$ adalah

$$a(b - c) = 0,$$

sesuatu yang tidak mungkin karena a dan $b - c$ keduanya bukan *zero divisor*. Jadi jika $ab = ac$ maka $b = c$.

Teorema 13 *Suatu finite integral domain R merupakan suatu field (tentu saja finite field).*

Untuk membuktikan teorema 13, kita tunjukkan bahwa setiap elemen dari R yang bukan 0 merupakan *unit*. Jika $a \in R \setminus \{0\}$ maka fungsi

$$f_a(x) = ax$$

untuk $x \in R \setminus \{0\}$ merupakan suatu *bijection* dari $R \setminus \{0\}$ ke $R \setminus \{0\}$. Jadi terdapat $b \in R \setminus \{0\}$ dimana $ab = 1$, dengan kata lain a merupakan *unit* karena mempunyai *inverse* yaitu $a^{-1} = b$. Jadi setiap elemen dari R yang bukan 0 merupakan *unit*, jadi R merupakan *field*.

5.2 Homomorphism dan Ideal

Suatu *homomorphism* antara dua himpunan adalah suatu fungsi yang mempertahankan struktur aljabar.

Definisi 10 (Homomorphism) *Untuk ring, suatu homomorphism* $\varphi : R \longrightarrow S$ *dari ring* R *ke ring* S *mempertahankan struktur ring sebagai berikut:*

- $\forall a, b \in R : \varphi(a + b) = \varphi(a) + \varphi(b)$,
- $\forall a, b \in R : \varphi(ab) = \varphi(a) \cdot \varphi(b)$, *dan*
- $\varphi(1_R) = 1_S$,

dimana 1_R *adalah 1 untuk* R *dan* 1_S *adalah 1 untuk* S.

Kerap 1 dan 0 tanpa subskrip digunakan jika jelas apa yang dimaksud. Jika *homomorphism* bersifat *injective* ($\varphi(a) = \varphi(b)$ hanya jika $a = b$), maka *homomorphism* disebut *embedding*. Jika *homomorphism* bersifat *bijective* (*injective* dan *surjective*), maka *homomorphism* disebut *isomorphism*. *Homomorphism* φ dari R ke S bersifat *surjective* jika untuk setiap $b \in S$, terdapat $a \in R$ dimana $b = \varphi(a)$, jadi φ "mengisi penuh" S. Jika φ adalah *isomorphism* dari R ke S, maka φ^{-1} adalah *isomorphism* dari S ke R, dan S disebut *isomorphic* dengan R dan diberi notasi $R \simeq S$.

Contoh dari *homomorphism* adalah *canonical homomorphism* dari $\mathbf{Z}$ ke $\mathbf{Z}/7\mathbf{Z}$ sebagai berikut:

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/7\mathbf{Z} \\ a & \mapsto & [a]. \end{array}$$

Kita periksa apakah ini benar merupakan homomorphism:

$$\varphi(a + b) = [a + b] = [a] + [b] = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = [a \cdot b] = [a] \cdot [b] = \varphi(a) \cdot \varphi(b)$$

$$\varphi(1) = [1] = 1_{\mathbf{Z}/7\mathbf{Z}}$$

Jadi ada *homomorphism* dari aritmatika bilangan bulat ke aritmatika modulo 7. (Pembaca dapat meninjau kembali bagian 3.5 mengenai aritmatika modular.)

Konsep berikutnya yang perlu dibahas adalah konsep *ideal* dalam suatu *ring*. Mari kita tinjau kembali aritmatika modulo sebuah bilangan, sebut saja n. Dalam aritmatika modulo n, setiap bilangan jika dikalikan dengan bilangan yang berada dalam *congruence class* $[0]$ (yang berisi semua kelipatan n, jadi $[0] = n\mathbf{Z}$) akan menghasilkan bilangan dalam *congruence class* $[0]$. Konsep ini sangat penting dalam teori *ring*, kita katakan $n\mathbf{Z}$ adalah *ideal* dalam *ring* $\mathbf{Z}$. Jadi sebetulnya aritmatika modulo 7 adalah aritmatika bilangan bulat modulo *ideal* $7\mathbf{Z}$.

Dalam struktur *ring*, sesuatu yang berada dalam *ring* jika dikalikan dengan sesuatu yang berada dalam suatu *ideal* dalam *ring* akan menghasilkan sesuatu dalam *ideal* (*ideal* mempunyai sifat *inside-outside multiplication*), dan sesuatu yang berada dalam *ideal* jika ditambahkan dengan sesuatu yang juga berada dalam *ideal* menghasilkan sesuatu dalam *ideal*. Jadi $n\mathbf{Z}$ adalah suatu *ideal* dalam $\mathbf{Z}$ (*ring* bilangan bulat) karena kelipatan n dikalikan apa saja menghasilkan kelipatan n, dan kelipatan n ditambahkan dengan kelipatan n menghasilkan kelipatan n.

Secara formal definisi untuk *ideal* adalah sebagai berikut (dengan menggunakan $\Longrightarrow$ untuk "berarti"):

Definisi 11 (ideal) *$I \subseteq R$ adalah ideal dari ring R jika:*

- $\forall a, b \in I : (a + b) \in I$ *dan*
- $\forall a \in R, n \in I : (a \cdot n) \in I$.

Untuk setiap *ring* R, jelas bahwa $\{0\}$ merupakan *ideal* dari R (dinamakan *trivial ideal*), karena $0 + 0 = 0$ dan $a \cdot 0 = 0$. Juga jelas bahwa R merupakan *ideal* dalam R karena sifat *closure* untuk *ring*. *Ideal* I dalam *ring* R adalah *proper ideal* dalam R jika $I \neq R$. Jika I adalah suatu *ideal*, maka

$$0 \in I$$

karena apapun dikalikan dengan 0 akan menghasilkan 0.

Satu dari sekian cara untuk mendapatkan *ideal* dalam suatu *ring* adalah dengan menggunakan *generator* tunggal berupa elemen dalam *ring*. Menggunakan *generator* tunggal $n \in R$, suatu *ideal* dalam *ring* R didapat dengan mengumpulkan semua kelipatan n. *Ideal* yang didapat dengan cara ini dinamakan *principal ideal* dengan *generator* tunggal n, dan diberi notasi nR. Jadi *ideal* $7\mathbf{Z}$ adalah *principal ideal* dengan *generator* tunggal 7. Notasi $7\mathbf{Z}$ digunakan untuk *ideal*, bukan $[0]$, agar jelas apa yang dimaksud (notasi $[0]$ hanya menjelaskan himpunan sebagai *congruence class* yang mempunyai elemen 0, tidak menjelaskan *ideal* yang dimaksud yaitu berisi semua bilangan kelipatan 7).

Secara umum, *generator* untuk *ideal* berupa himpunan A yang merupakan *subset* dari R ($A \subseteq R$). *Ideal* yang didapat adalah himpunan semua kombinasi linear dari elemen-elemen A:

$$\left\{ \sum_{i=1}^{n} a_i r_i \middle| 0 < n \in \mathbf{N}, r_i \in R \text{ dan } a_i \in A \text{ untuk } 1 \leq i \leq n \right\}.$$

Jika *generator* A merupakan *finite subset* dari R, maka *ideal* disebut *finitely generated*. Jelas bahwa suatu *principal ideal* adalah *finitely generated*.

Dalam memperkenalkan konsep *homomorphism*, *canonical homomorphism* dari $\mathbf{Z}$ ke $\mathbf{Z}/7\mathbf{Z}$ dijadikan contoh, dengan pemetaan elemen a: $a \mapsto [a]$. Pemetaan ini khusus untuk $\mathbf{Z}/n\mathbf{Z}$. Secara umum, untuk *ideal* I dalam *ring* R, elemen a dari R dapat dipetakan sebagai berikut:

$$\begin{array}{ccc} R & \longrightarrow & R/I \\ a & \mapsto & a + I \end{array}$$

menghasilkan *canonical homomorphism* dari R ke R/I (*ring* R modulo *ideal* I) dimana $a + I$ didefinisikan sebagai berikut:

$$a + I = \{a + e | e \in I\}.$$

Jadi $a + I$ adalah himpunan yang didapat dengan menambahkan a terhadap setiap elemen dari I. Sebagai contoh, kembali ke $\mathbf{Z}/7\mathbf{Z}$ dimana $I = [0]$, $3 + I = 3 + [0] = [3]$.

Kita definisikan pertambahan, perkalian dan *inverse* pertambahan untuk $a + I$ sebagai berikut:

$$\begin{array}{rcl} (a + I) + (b + I) & = & ((a + b) + I) \\ (a + I) \cdot (b + I) & = & ((a \cdot b) + I) \\ -(a + I) & = & (-a + I) \end{array}$$

Mari kita tunjukkan bahwa R/I adalah *ring* (semua aksioma *ring* berlaku) untuk sembarang *ring* R dan *proper ideal* I, dengan

$$\begin{array}{rcl} 0_{R/I} & = & 0_R + I = I \\ 1_{R/I} & = & 1_R + I \end{array}$$

Associativity untuk $+$:

$$\begin{array}{rcl} (a + I) + ((b + I) + (c + I)) & = & (a + I) + ((b + c) + I) \\ & = & ((a + (b + c)) + I) \end{array}$$

$$\begin{aligned} &= (((a+b)+c)+I) \\ &= ((a+b)+I)+(c+I) \\ &= ((a+I)+(b+I))+(c+I). \end{aligned}$$

Identity untuk $+$:

$$(a+I)+(0_R+I) = ((a+0_R)+I) = (a+I).$$

Commutativity untuk $+$:

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

Inverse untuk $+$:

$$(a+I)+(-(a+I)) = (a+I)+(-a+I) = ((a+(-a))+I) = (0_R+I) = I.$$

Associativity untuk $\cdot$:

$$\begin{aligned} (a+I)\cdot((b+I)\cdot(c+I)) &= (a+I)\cdot((b\cdot c)+I) \\ &= ((a\cdot(b\cdot c))+I) \\ &= (((a\cdot b)\cdot c)+I) \\ &= ((a\cdot b)+I)\cdot(c+I) \\ &= ((a+I)\cdot(b+I))\cdot(c+I). \end{aligned}$$

Identity untuk $\cdot$:

$$(a+I)\cdot(1_R+I) = ((a\cdot 1_R)+I) = (a+I).$$

Commutativity untuk $\cdot$:

$$(a+I)\cdot(b+I) = ((a\cdot b)+I) = ((b\cdot a)+I) = (b+I)\cdot(a+I).$$

Distributivity:

$$\begin{aligned} (a+I)\cdot((b+I)+(c+I)) &= (a+I)\cdot((b+c)+I) \\ &= ((a\cdot(b+c))+I) \\ &= (((a\cdot b)+(a\cdot c))+I) \\ &= ((a\cdot b)+I)+((a\cdot c)+I) \\ &= ((a+I)\cdot(b+I))+((a+I)\cdot(c+I)). \end{aligned}$$

Ring R/I dinamakan *quotient ring*.

Sekarang kita bahas bagaimana *ideal* dipetakan oleh suatu *homomorphism*. Jika $\varphi : R \longrightarrow S$ merupakan *homomorphism* dari *ring* R ke *ring* S, maka *kernel* dari *homomorphism* dengan notasi $\ker(\varphi)$ adalah subset dari R sebagai berikut:

$$\ker(\varphi) = \{a \in R | \varphi(a) = 0_S\}$$

jadi *kernel* dari *homomorphism* adalah subset dari *ring* asal R, dan terdiri dari semua elemen R yang dipetakan ke 0 dalam *ring* tujuan S. Tidak terlalu sulit untuk membuktikan bahwa $\ker(\varphi)$ adalah suatu *proper ideal* dalam R. Kita tahu bahwa $0_R \in \ker(\varphi)$ karena $\varphi(0_R) = 0_S$, jadi $\ker(\varphi) \neq \emptyset$. Kita buktikan bahwa $\ker(\varphi)$ adalah suatu *ideal* dalam R:

- Jika $a, b \in \ker(\varphi)$, maka $\varphi(a) = \varphi(b) = 0_S$, dan $\varphi(a+b) = \varphi(a) + \varphi(b) = 0_S + 0_S = 0_S$, jadi $a + b \in \ker(\varphi)$.

- Jika $a \in \ker(\varphi)$ dan $r \in R$, maka $\varphi(a) = 0_S$, dan $\varphi(ar) = \varphi(a) \cdot \varphi(r) = 0_S \cdot \varphi(r) = 0_S$, jadi $ar \in \ker(\varphi)$.

Jadi $\ker(\varphi)$ adalah suatu *ideal* dalam R. Karena $\varphi(1_R) = 1_S \neq 0_S$, $1_R \notin \ker(\varphi)$, $\ker(\varphi)$ adalah *proper ideal*.

Masih menyangkut *homomorphism* φ dari R ke S, setiap *ideal* J dalam S "berasal" dari *ideal* yang mencakup $\ker(\varphi)$ dalam R:

$$I = \{c | c \in R, \varphi(c) \in J\} \text{ adalah } \textit{ideal} \text{ dalam } R \text{ dan } \ker(\varphi) \subseteq I. \tag{5.1}$$

Dengan notasi himpunan, konsep "J berasal dari I" diformalkan, dan I disebut *inverse image* dari J menurut φ. Mari kita buktikan 5.1. Jika $a, b \in I$, maka $\varphi(a), \varphi(b) \in J$, jadi karena J merupakan *ideal*,

$$\varphi(a + b) = \varphi(a) + \varphi(b) \in J$$

jadi $a + b \in I$. Jika $a \in I$ dan $r \in R$ maka $\varphi(a) \in J$ dan $\varphi(r) \in S$, jadi

$$\varphi(ra) = \varphi(r) \cdot \varphi(a) \in J$$

jadi $ar \in I$, dan I merupakan *ideal* dalam R. Karena $0_S \in J$ maka $\ker(\varphi) = \{c | c \in R, \varphi(c) = 0_S\} \subseteq I$.

Sebaliknya apakah setiap *ideal* I dalam R dipetakan oleh φ menjadi suatu *ideal* dalam S? Ternyata ini hanya bisa dipastikan bila φ *surjective* sehingga "mengisi penuh" S, karena jika tidak, ada pertanyaan dengan elemen S yang diluar target φ apabila dikalikan dengan elemen dari $J = \{\varphi(c) | c \in I\}$.

$$\text{Jika } \varphi \textit{ surjective} \text{ maka } J = \{\varphi(c) | c \in I\} \text{ adalah } \textit{ideal} \text{ dalam } S. \tag{5.2}$$

Mari kita buktikan 5.2. Kita tahu bahwa J tidak kosong (karena I tidak kosong), jadi jika $b_1, b_2 \in J$, maka terdapat $a_1, a_2 \in I$ dimana $b_1 = \varphi(a_1)$ dan $b_2 = \varphi(a_2)$, jadi

$$b_1 + b_2 = \varphi(a_1) + \varphi(a_2) = \varphi(a_1 + a_2) \in J$$

karena I adalah suatu *ideal* ($a_1 + a_2 \in I$). Jika $b \in J$ dan $s \in S$ maka terdapat $a \in I$ dan $r \in R$ dimana $b = \varphi(a)$ dan $s = \varphi(r)$, jadi

$$sb = \varphi(r) \cdot \varphi(a) = \varphi(ra) \in J.$$

Jadi J merupakan *ideal* dalam S.

Kita sudah buktikan bahwa jika *homomorphism* φ dari *ring* R ke *ring* S *surjective*, maka setiap *ideal* I dalam R dipetakan oleh φ menjadi suatu *ideal* dalam S. Apakah hubungan antara *ideal* dalam R dengan *ideal* dalam S jika φ *surjective*? Ternyata jika φ *surjective*, ada korespondensi satu dengan satu antara himpunan semua *ideal* yang mencakup $\ker(\varphi)$ dalam R dengan himpunan semua *ideal* dalam S. Mari kita buat

$$\begin{aligned} I_\varphi &= \{I | I \textit{ ideal} \text{ dalam } R, \ker(\varphi) \subseteq I\}, \\ I_S &= \{J | J \textit{ ideal} \text{ dalam } S\}. \end{aligned}$$

Dengan pemetaan $\chi : I_\varphi \longrightarrow I_S$ sebagai berikut

$$\begin{aligned} \chi : I_\varphi &\longrightarrow I_S \\ I &\mapsto \{\varphi(a) | a \in I\} \end{aligned}$$

jika φ *surjective* maka

$$\chi \textit{ bijective} \text{ dengan } \chi^{-1}(J) = \{a | a \in R, \varphi(a) \in J\}. \qquad (5.3)$$

Definisi χ diatas mengatakan bahwa untuk $I \in I_\varphi$, $\chi(I)$ adalah *image* dari I menurut φ dan notasi $\varphi(I)$ kerap digunakan walaupun notasi ini agak membingungkan. Untuk χ^{-1} definisi diatas mengatakan bahwa untuk $J \in I_S$, $\chi^{-1}(J)$ adalah *inverse image* dari J menurut φ dan notasi $\varphi^{-1}(J)$ kerap digunakan.

Pembuktian 5.3 mempunyai dua bagian:

- membuktikan bahwa $\chi^{-1}(\chi(I)) = I$ untuk setiap $I \in I_\varphi$, dan
- membuktikan bahwa $\chi(\chi^{-1}(J)) = J$ untuk setiap $J \in S$.

Walaupun teori mengenai pemetaan dengan konsep *image* dan *inverse image* dapat mempersingkat pembuktian, teori tersebut tidak akan digunakan, jadi kita akan membuktikan secara langsung.

- Kita tunjukkan bahwa $I \subseteq \chi^{-1}(\chi(I))$ untuk setiap $I \in I_\varphi$:

$$\begin{aligned} b \in I &\implies \varphi(b) \in \{\varphi(a)|a \in I\} \\ &\implies b \in \{a_1|a_1 \in R, \varphi(a_1) \in \{\varphi(a)|a \in I\}\} \\ &\implies b \in \{a_1|a_1 \in R, \varphi(a_1) \in \chi(I)\} \\ &\implies b \in \chi^{-1}(\chi(I)). \end{aligned}$$

  Jadi $I \subseteq \chi^{-1}(\chi(I))$ untuk setiap $I \in I_\varphi$. Berikutnya, kita tunjukkan bahwa $\chi^{-1}(\chi(I)) \subseteq I$ untuk setiap $I \in I_\varphi$:

$$\begin{aligned} b \in \chi^{-1}(\chi(I)) &\implies b \in \{a_1|a_1 \in R, \varphi(a_1) \in \chi(I)\} \\ &\implies b \in \{a_1|a_1 \in R, \varphi(a_1) \in \{\varphi(a)|a \in I\}\} \\ &\implies \varphi(b) \in \{\varphi(a)|a \in I\}\} \\ &\implies \text{terdapat } a \in I \text{ dimana } \varphi(b) = \varphi(a) \\ &\implies (b-a) \in \ker(\varphi) \subseteq I \\ &\implies b = (a + (b-a)) \in I. \end{aligned}$$

  Jadi $\chi^{-1}(\chi(I)) \subseteq I$ untuk setiap $I \in I_\varphi$. Menggabungkan kedua cakupan, kita dapatkan $\chi^{-1}(\chi(I)) = I$ untuk setiap $I \in I_\varphi$.

- Kita tunjukkan bahwa $\chi(\chi^{-1}(J)) \subseteq J$ untuk setiap $J \in S$:

$$\begin{aligned} b \in \chi(\chi^{-1}(J)) &\implies b \in \{\varphi(a)|a \in \chi^{-1}(J) \\ &\implies b \in \{\varphi(a)|a \in \{a_1|a_1 \in R, \varphi(a_1) \in J\} \\ &\implies \text{terdapat } a \in R, \varphi(a) \in J \text{ dimana } b = \varphi(a) \\ &\implies b \in J. \end{aligned}$$

  Jadi $\chi(\chi^{-1}(J)) \subseteq J$ untuk setiap $J \in S$. Berikutnya, kita tunjukkan bahwa $J \subseteq \chi(\chi^{-1}(J))$ untuk setiap $J \in S$ dan φ *surjective*:

$$\begin{aligned} b \in J \text{ dan } \varphi \text{ surjective} &\implies \text{terdapat } I \in I_\varphi, a \in I \text{ dimana } b = \varphi(a) \\ &\implies a \in I, b = \varphi(a) \text{ dan} \\ &\qquad a \in \{a_1|a_1 \in R, \varphi(a_1) \in J\} \\ &\implies a \in I, b = \varphi(a) \text{ dan } a \in \chi^{-1}(J) \\ &\implies b \in \chi(\chi^{-1}(J)) \end{aligned}$$

  Jadi $J \subseteq \chi(\chi^{-1}(J))$ untuk setiap $J \in S$. Menggabungkan kedua cakupan, kita dapatkan $\chi(\chi^{-1}(J)) = J$ untuk setiap $J \in I_S$.

Jadi kita selesai dengan pembuktian 5.3, dan selesai sudah pembahasan mengenai bagaimana *ideal* dipetakan oleh *homomorphism* secara umum.

Sekarang kita sudah dapat menjelaskan lebih lanjut, menggunakan hasil 5.3, *canonical homomorphism* φ dari *ring* R ke ring R/I, dimana I adalah suatu *ideal* dalam R. R/I disebut *quotient ring* modulo suatu *ideal*, dan setiap elemen dalam R/I adalah suatu *congruence class* $a + I$ untuk suatu a (kerap juga disebut *coset*). Untuk *ring* R, *proper ideal* I dalam R, dan *canonical homomorphism* φ dari R ke R/I, kita dapatkan:

$$I = \ker(\varphi). \tag{5.4}$$

Pembuktian 5.4 adalah sebagai berikut:

$$\begin{aligned} a \in \ker(\varphi) &\iff \varphi(a) = 0 \\ &\iff a + I = 0 + I \\ &\iff a \in I. \end{aligned}$$

Akibatnya, berdasarkan prinsip *extensionality* dari teori himpunan, $I = \ker(\varphi)$.

Teorema 14 *Untuk ring R, proper ideal I dalam R, dan φ canonical homomorphism dari R ke R/I dengan*

$$\begin{aligned} I_\varphi &= \{I_1 | I_1 \textit{ ideal dalam } R, I \subseteq I_1\}, \\ I_S &= \{J | J \textit{ ideal dalam } S\}. \end{aligned}$$

dan pemetaan $\chi : I_\varphi \longrightarrow I_S$ sebagai berikut

$$\begin{aligned} \chi : I_\varphi &\longrightarrow I_S \\ I_1 &\mapsto \{\varphi(a) | a \in I_1\} \end{aligned}$$

kita dapatkan

$$\chi \textit{ bijective, dengan } \chi^{-1}(J) = \{a | a \in R, \varphi(a) \in J\}.$$

Teorema 14 adalah aplikasi dari 5.3 dengan $S = R/I$ dan menggunakan 5.4. Teorema mengatakan ada korespondensi satu dengan satu antara himpunan *ideal* dalam R yang mencakup $\ker(\varphi)$ dengan himpunan *ideal* dalam R/I. Lebih terperinci lagi, setiap *ideal* dalam R yang mencakup I, dipasangkan secara unik oleh fungsi χ dengan satu *ideal* dalam R/I, dan tidak ada *ideal* dalam R/I yang tidak dipasangkan. Teorema ini akan digunakan dalam pembahasan *polynomial field* yaitu *polynomial ring* modulo *ideal* dengan *generator irreducible polynomial*.

Yang terahir dibagian ini adalah teorema mengenai *ideal* dalam *field*.

Teorema 15 *Suatu ring R adalah field jika dan hanya jika ($\iff$) tidak ada ideal untuk R selain $\{0\}$ dan R.*

Pembuktian teorema 15 mempunyai dua bagian. Di bagian pertama kita tunjukkan bahwa untuk *field* R hanya ada dua *ideal* yaitu $\{0\}$ dan R. Di bagian kedua kita tunjukkan bahwa jika *ring* R hanya mempunyai dua *ideal* $\{0\}$ dan R, maka R adalah suatu *field*.

- Mari kita umpamakan bahwa R adalah suatu *field* dan kita cari *ideal* untuk R selain $\{0\}$ dan R, sebut saja I. Ini berarti I harus berupa *proper ideal* dan *non-trivial*. Untuk *proper ideal*, kita tahu bahwa $1 \notin I$ karena jika $1 \in I$, seluruh ring R akan masuk dalam *ideal* berdasarkan *inside-outside multiplication*. Akibatnya, untuk setiap *unit* u dari R, $u \notin I$ sebab $u \in I$ berarti $u \cdot u^{-1} = 1 \in I$. Akan tetapi untuk *field* setiap elemen kecuali 0 merupakan *unit*, jadi hanya ada satu *proper ideal* untuk R yaitu $\{0\}$ yang merupakan *trivial ideal*. Berarti untuk *field* R hanya ada dua *ideal*: $\{0\}$ dan R.

- Untuk kebalikannya, kita umpamakan hanya $\{0\}$ dan R merupakan *ideal* dalam R. Jika ada *non-unit* $a \neq 0$, maka a dapat digunakan sebagai *generator* untuk membuat *ideal* aR yang tidak mengandung *unit* (kelipatan *non-unit* a tidak bisa berupa *unit*). Jadi aR harus berupa *non-trivial proper ideal* dalam R, suatu kontradiksi jika hanya $\{0\}$ dan R merupakan *ideal* dalam R. Jadi setiap elemen kecuali 0 berupa *unit*, yang berarti R harus berupa *field*.

Selesai sudah pembuktian teorema 15.

5.3 Principal Ideal Domain

Jika setiap *ideal* dalam suatu *ring* R merupakan *principal ideal* maka R dinamakan *principal ideal ring*. Jika R juga merupakan *integral domain* maka R merupakan *principal ideal domain* (PID).

$\mathbf{Z}$ merupakan *integral domain* karena dalam aritmatika bilangan bulat tidak ada *zero divisor*. Mari kita coba buktikan bahwa $\mathbf{Z}$ merupakan PID, jadi kita harus buktikan bahwa setiap *ideal* I dalam $\mathbf{Z}$ adalah *principal ideal*. Jika $I = \{0\}$ maka I adalah *principal ideal* dengan *generator* 0. Jika $I \neq \{0\}$, mari kita fokus pada himpunan

$$I^+ = \{m \in I | m > 0\}.$$

I^+ merupakan himpunan non-kosong karena $I \neq \{0\}$ dan $k \in I$ berarti $-k \in I$ untuk setiap $k \in \mathbf{Z}$. Berdasarkan prinsip *well-ordering*, I^+, yang merupakan subset dari $\mathbf{N}$, mempunyai elemen terkecil, sebut saja n. Karena $n \in I$ maka $n\mathbf{Z} \subseteq I$. Untuk kebalikannya, mari kita analisa apa konsekuensi dari $m \in I$. Kita gunakan algoritma pembagian untuk membagi m dengan n menghasilkan

$$m = nq + r$$

dengan $0 \leq r < n$. Tetapi $r = m - nq \in I$, jadi $r = 0$ karena n adalah minimal dalam I^+. Jadi $m = nq$ yang berarti $m \in n\mathbf{Z}$ yang juga berarti $I \subseteq n\mathbf{Z}$. Jadi $I = n\mathbf{Z}$ yang berarti I adalah *principal ideal* dengan *generator* n. Jadi $\mathbf{Z}$ adalah suatu PID.

Sekarang kita bahas konsep gcd abstrak dalam *integral domain* dengan definisi gcd sebagai berikut:

Definisi 12 (GCD untuk ring) *Untuk $a, b \in R$ dimana R adalah ring, d adalah* gcd *dari a dan b jika*

1. *$d|a$ dan $d|b$ (a dan b merupakan kelipatan d), dan*
2. *$d'|a$ dan $d'|b$ berarti $d'|d$.*

Menggunakan notasi logika:

$$\forall a, b, d \in R : d|a \wedge d|b \wedge (\forall d' \in R : (d'|a \wedge d'|b) \Longrightarrow d'|d) \Longrightarrow d \equiv \gcd(a, b).$$

Kita gunakan $d \equiv \gcd(a, b)$ untuk mengatakan "d adalah gcd dari a dan b" karena bisa terdapat banyak gcd tetapi semua ekuivalen karena berasosiasi. Untuk $a, b \in R$ dimana R adalah suatu *ring*, u suatu *unit* dari R, dan $a = ub$, a disebut *associated* dengan b (a dan b berasosiasi). Jika d adalah gcd dari a dan b dan d' juga merupakan gcd dari a dan b, maka d dan d' berasosiasi. Untuk membuktikan ini, definisi gcd mengatakan $d|a$, $d|b$, $d'|a$ dan $d'|b$, jadi karena syarat 2 dari definisi, $d|d'$ dan $d'|d$. Akibatnya, terdapat $a, b \in R$ dimana $d' = ad$ dan $d = bd'$. Jadi

$$\begin{aligned} d|d' \text{ dan } d'|d &\Longrightarrow d' = ad = abd' \\ &\Longrightarrow ab = 1 \end{aligned}$$

yang berarti $b = a^{-1}$, jadi a dan a^{-1} adalah *unit* dalam R. Jadi d dan d' berasosiasi.

Jika R adalah *integral domain* dan $a, b, d \in R$, maka kedua proposisi sebagai berikut ekuivalen:

1. d adalah gcd dari a dan b dan terdapat $s, t \in R$ dengan $d = sa + tb$.
2. $aR + bR = dR$.

Pembuktian bahwa proposisi 1 ekuivalen proposisi 2 mempunyai dua bagian:

- Kita tunjukkan bahwa proposisi 1 $\Longrightarrow$ proposisi 2. Karena d adalah gcd dari a dan b, maka $d|a$ dan $d|b$.

$$\begin{aligned} d|a \text{ dan } d|b &\Longrightarrow aR \subseteq dR \text{ dan } bR \subseteq dR \\ &\Longrightarrow aR + bR \subseteq dR. \end{aligned}$$

Karena terdapat $s, t \in R$ dengan $d = sa + tb$

$$\begin{aligned} d = sa + tb &\implies d \in aR + bR \\ &\implies dR \subseteq aR + bR. \end{aligned}$$

Jadi $aR + bR = dR$.

- Kita tunjukkan bahwa proposisi 2 $\implies$ proposisi 1.

$$\begin{aligned} aR + bR = dR &\implies aR + bR \subseteq dR \\ &\implies aR \subseteq dR \text{ dan } bR \subseteq dR \\ &\implies d|a \text{ dan } d|b. \end{aligned}$$

Juga

$$\begin{aligned} aR + bR = dR &\implies dR \subseteq aR + bR \\ &\implies d \in dR \subseteq aR + bR \\ &\implies \text{terdapat } s, t \in R \text{ dengan } d = sa + tb. \end{aligned}$$

Jika ada $d' \in R$ dengan $d'|a$ dan $d'|b$, karena $d = sa + tb$ maka $d'|d$. Jadi d adalah gcd dari a dan b.

Selesai sudah pembuktian bahwa proposisi 1 ekuivalen dengan proposisi 2. Karena PID merupakan *integral domain*, ini menghasilkan teorema berikut.

Teorema 16 *Jika R adalah PID dan $a, b \in R$ maka a dan b mempunyai* gcd *$d \in R$ dengan $aR + bR = dR$ jadi ada $s, t \in R$ dengan $d = sa + tb$. Menggunakan notasi logika:*

$$\forall a, b \in R : \exists d, s, t \in R : d \equiv \gcd(a, b) \wedge aR + bR = dR \wedge d = sa + tb.$$

5.4 Prime Ideal dan Maximal Ideal

Definisi 13 (Prime Ideal) *Suatu proper ideal I dalam ring R disebut prima (prime ideal) jika $ab \in I$ berarti $a \in I$ atau $b \in I$ untuk setiap $a, b \in R$.*

Untuk $2 \le p \in \mathbf{Z}$, p adalah bilangan prima jika dan hanya jika ($\iff$) *ideal* $p\mathbf{Z}$ dalam $\mathbf{Z}$ adalah prima. Untuk $2 \le p \in \mathbf{Z}$:

$$\begin{aligned} p \text{ prima} &\iff p|mn \text{ berarti } p|m \text{ atau } p|n \text{ untuk setiap } m, n \in \mathbf{Z} \\ &\iff mn \in p\mathbf{Z} \text{ berarti } m \in p\mathbf{Z} \text{ atau } n \in p\mathbf{Z} \text{ untuk setiap } m, n \in \mathbf{Z} \\ &\iff p\mathbf{Z} \text{ adalah } \textit{ideal} \text{ prima dalam } \mathbf{Z}. \end{aligned}$$

Jadi ada korespondensi satu dengan satu antara bilangan prima dalam $\mathbf{Z}$ dengan *non-trivial ideal* prima dalam $\mathbf{Z}$.

Definisi 14 (Maximal Ideal) *Suatu ideal I dalam ring R disebut maksimal (maximal ideal) jika $I \neq R$ dan untuk setiap ideal J dalam R yang mencakup I ($I \subseteq J$), $I = J$ atau $J = R$ (I merupakan proper ideal dalam R yang tidak tercakup oleh proper ideal dalam R lainnya).*

Teorema 17 *Jika I adalah proper ideal dalam R, maka:*

- *I prima $\Longleftrightarrow R/I$ adalah suatu integral domain.*
- *I maksimal $\Longleftrightarrow R/I$ adalah suatu field.*

Mari kita buktikan teorema 17. Jika I adalah *proper ideal* dalam R, maka

$$\begin{aligned} ab \in I &\Longleftrightarrow ab + I = 0 \\ &\Longleftrightarrow (a+I)(b+I) = 0. \end{aligned}$$

Untuk bagian pertama, pembuktian cukup mudah:

$$\begin{aligned} I \text{ prima} &\Longleftrightarrow \forall a, b \in R : ab \in I \Longrightarrow a \in I \text{ atau } b \in I \\ &\Longleftrightarrow \forall a, b \in R : (a+I)(b+I) = 0 \Longrightarrow a + I = 0 \text{ atau } b + I = 0 \\ &\Longleftrightarrow R/I \text{ adalah } \textit{integral domain}. \end{aligned}$$

Untuk bagian kedua, menggunakan teorema 14:

$$\begin{aligned} I \text{ maksimal} &\Longleftrightarrow \text{tidak ada } \textit{ideal} \supseteq I \text{ dalam } R \text{ kecuali } R \text{ dan } I \\ &\Longleftrightarrow \text{tidak ada } \textit{ideal} \text{ dalam } R/I \text{ kecuali } R/I \text{ dan } \{I\} \\ &\Longleftrightarrow \text{tidak ada } \textit{ideal} \text{ dalam } R/I \text{ kecuali } R/I \text{ dan } \{0_{R/I}\} \\ &\Longleftrightarrow R/I \text{ adalah } \textit{field}. \end{aligned}$$

Apa kaitan *ideal* prima dengan *ideal* maksimal? Untuk setiap *ring* R dan *ideal* I dalam R

$$I \text{ maksimal} \Longrightarrow I \text{ prima}. \tag{5.5}$$

Dengan kata lain, *ideal* yang maksimal juga merupakan suatu *ideal* prima. Untuk membuktikan ini, menggunakan teorema 17, I maksimal berarti R/I adalah suatu *field* yang juga berarti R/I adalah suatu *integral domain* yang berarti I prima.

Kebalikannya tidak selalu benar. Tidak semua *ideal* yang prima juga merupakan *ideal* maksimal. Tetapi untuk *principal ideal domain*, kita dapatkan hasil yang cukup memuaskan. Untuk setiap PID R dan *non-trivial ideal* I dalam R

$$I \text{ prima} \Longrightarrow I \text{ maksimal}. \tag{5.6}$$

Setiap *non-trivial ideal* prima dalam PID juga merupakan *ideal* maksimal. Untuk membuktikan ini, karena R merupakan PID, kita cukup membuktikan bahwa setiap *ideal* prima aR dengan $a \neq 0$ adalah *ideal* maksimal. Jadi jika bR adalah *ideal* dalam R dan $aR \subseteq bR$, maka kita harus tunjukkan bahwa $bR = aR$ atau $bR = R$.

$$\begin{aligned} aR \subseteq bR &\implies a \in bR \\ &\implies a = bc \text{ untuk suatu } c \in R \\ &\implies b \in aR \text{ atau } c \in aR \text{ (karena } aR \text{ prima).} \end{aligned}$$

Untuk $b \in aR$

$$\begin{aligned} b \in aR &\implies bR \subseteq aR \\ &\implies bR = aR. \end{aligned}$$

Untuk $c \in aR$

$$\begin{aligned} c \in aR &\implies c = ad \text{ untuk suatu } d \in R \\ &\implies a = bc = bad = abd \\ &\implies bd = 1 \\ &\implies 1 \in bR \\ &\implies bR = R. \end{aligned}$$

Jadi $bR = aR$ atau $bR = R$.

Jadi, dengan menggabungkan 5.5 dengan 5.6 kita dapatkan

Teorema 18 *Untuk setiap R yang berupa PID dan I suatu non-trivial ideal dalam R*

$$I \text{ prima} \iff I \text{ maksimal.}$$

Jadi untuk PID, konsep *ideal* prima dan konsep *ideal* maksimal menjadi satu.

Selanjutnya, kita definisikan konsep elemen prima dan elemen *irreducible* dalam *integral domain* yang akan kita kaitkan dengan konsep *ideal* prima dan *ideal* maksimal.

Definisi 15 *Untuk suatu integral domain R dan $0 \neq a$ suatu non-unit dalam R:*

- *a irreducible jika $a = bc$ berarti b adalah unit atau c adalah unit untuk setiap $b, c \in R$.*
- *a prima jika $a|bc$ berarti $a|b$ atau $a|c$ untuk setiap $b, c \in R$.*

Jika $a \in R$ dan u adalah suatu *unit* dalam R, maka a dapat diuraikan secara *trivial* menjadi $a = u(u^{-1}a)$. Jadi elemen *irreducible* adalah elemen yang tidak dapat diuraikan kecuali secara *trivial*. Jika a *irreducible* dan u unit, maka ua

juga *irreducible* karena ua tetap tidak dapat diuraikan kecuali secara *trivial*. Kebalikannya juga berlaku, jika ua *irreducible* maka a juga *irreducible*, sebab jika a *reducible* berarti terdapat *non-unit* $b, c \in R$ dengan $a = bc$ jadi terdapat *non-unit* ub dan c dengan $ua = (ub)c$ yang berarti ua juga *reducible*. Jadi untuk R suatu *integral domain*, $a \in R$ dan *unit* $u \in R$:

$$ua \textit{ irreducible} \Longleftrightarrow a \textit{ irreducible} \tag{5.7}$$

Untuk R suatu *integral domain*,

$$a \text{ prima} \Longrightarrow a \textit{ irreducible}. \tag{5.8}$$

Untuk membuktikan 5.8, dengan a prima, mari kita lihat apakah mungkin a merupakan elemen yang *reducible*.

$$\begin{aligned} a \textit{ reducible} &\Longrightarrow \text{terdapat } \textit{non-unit } b, c : a = bc \\ &\Longrightarrow a|b \text{ atau } a|c \end{aligned}$$

karena a prima dan $a|a$. Jika $a|b$, maka

$$\begin{aligned} a|b &\Longrightarrow \exists d \in R : b = ad \\ &\Longrightarrow \exists d \in R : a = bc = adc \\ &\Longrightarrow \exists d \in R : dc = 1, \end{aligned}$$

sesuatu yang tidak mungkin karena c *non-unit*. Untuk menunjukkan bahwa $a|c$ juga sesuatu yang tidak mungkin, karena simetris, cara pembuktian sama tetapi dengan b dan c dipertukarkan, jadi tidak perlu diulang (cara pembuktian dimana kita cukup membuktikan satu dari beberapa pilihan karena cara pembuktian untuk pilihan lainnya serupa sering dijuluki *without loss of generality*). Jadi selesai sudah pembuktian 5.8.

Jika R suatu *integral domain* dan $a \in R$ *irreducible*

$$\forall b \in R : a \not| b \Longrightarrow 1 \text{ adalah gcd dari } a \text{ dan } b \tag{5.9}$$

Untuk membuktikan bahwa 1 adalah gcd dari a dan b, jelas $1|a$ dan $1|b$ berlaku. Kita tinggal membuktikan bahwa jika $d|a$ dan $d|b$ maka $d|1$ untuk setiap $d \in R$. Jika $d|a$ maka terdapat $c \in R$ dengan $a = cd$. Karena a *irreducible*, maka ada dua kemungkinan untuk d:

- d adalah *unit* atau
- d *irreducible* sebab jika d *reducible* maka a juga *reducible*.

Jika d *irreducible*, maka c harus berupa *unit*, sebab jika tidak, maka a menjadi *reducible*. Jadi $d = c^{-1}a$. Karena $d|b$ maka terdapat $r \in R$ dengan $b = rd = rc^{-1}a$, jadi $a|b$, suatu kontradiksi. Jadi d harus berupa *unit* yang berarti $d|1$.

Teorema 19 *Untuk R suatu PID dan $a \in R$:*

$$a \text{ irreducible} \Longrightarrow a \text{ prima}. \tag{5.10}$$

Kita harus buktikan

$$a \text{ irreducible} \Longrightarrow \forall b, c \in R : a|bc \Longrightarrow a|b \text{ atau } a|c.$$

Jadi kita harus tunjukkan

$$a \text{ irreducible}, a|bc, a \not| b \Longrightarrow a|c.$$

Menggunakan 5.9 kita dapatkan

$$\begin{aligned} a \text{ irreducible}, a|bc, a \not| b &\Longrightarrow 1 \text{ adalah gcd dari } a \text{ dan } b \\ &\Longrightarrow \text{terdapat } s, t \in R : 1 = sa + tb \\ &\Longrightarrow c = sac + tbc \end{aligned}$$

Karena $a|bc$, maka $a|tbc$, jadi $a|c = sac + tbc$. Kita selesai dengan pembuktian teorema 19. Menggabungkan teorema 19 dengan 5.8 kita dapatkan:

Teorema 20 *Untuk R suatu PID dan $a \in R$:*

$$a \text{ irreducible} \Longleftrightarrow a \text{ prima}. \tag{5.11}$$

Untuk R suatu *integral domain*, $a \in R$

$$a \text{ prima} \Longleftrightarrow aR \text{ ideal prima}. \tag{5.12}$$

Pembuktian 5.12 adalah sebagai berikut:

$$\begin{aligned} a \text{ prima} &\Longleftrightarrow a|bc \Longrightarrow a|b \text{ atau } a|c \text{ untuk setiap } b, c \in R \\ &\Longleftrightarrow bc \in aR \Longrightarrow b \in aR \text{ atau } c \in aR \text{ untuk setiap } b, c \in R \\ &\Longleftrightarrow aR \text{ ideal prima}. \end{aligned}$$

Teorema terahir sebelum kita bahas *polynomial ring* adalah sebagai berikut.

Teorema 21 *Untuk R suatu PID dan $a \in R$, a irreducible $\Longleftrightarrow aR$ maksimal.*

Pembuktian teorema ini adalah sebagai berikut:

$$\begin{aligned} a \text{ irreducible} &\Longleftrightarrow a \text{ prima (5.11)} \\ &\Longleftrightarrow aR \text{ ideal prima (5.12)} \\ &\Longleftrightarrow aR \text{ ideal maksimal (teorema 18)} \end{aligned}$$

5.5 Polynomial Ring

Jika R adalah suatu *ring*, maka $R[x]$ adalah *polynomial ring* dengan variabel x. Setiap elemen dari $R[x]$ adalah *polynomial* dengan variabel x dan koefisien dari *ring* R. Sebaliknya, setiap *polynomial* dengan variabel x dan koefisien dari *ring* R merupakan elemen dari $R[x]$.

Sebagai contoh, dengan *ring* untuk koefisien berupa *field* $K = \mathbf{Z}/3\mathbf{Z}$,

$$x^5 + 2x^3 + x^2 + 2$$

merupakan *polynomial* elemen $K[x]$ dengan *degree* (pangkat terbesar) 5. Suatu *polynomial* p dapat ditulis sebagai:

$$p = \sum_{i=0}^{n} a_i x^i$$

dimana n adalah *degree* dari p dan a_i adalah koefisien untuk suku dengan pangkat i, jadi setiap a_i adalah elemen dari *ring* R, dan $a_n \neq 0$. Sebetulnya a_i berlaku untuk setiap $i \in \mathbf{Z}$ tetapi $a_i = 0$ untuk $i > n$ dan $i < 0$. Untuk contoh diatas, $a_0 = 2$, $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 0$ dan $a_5 = 1$. Kita akan namakan fungsi *degree* deg, jadi $\deg(p) = n$.

Aritmatika dalam $R[x]$ adalah sebagai berikut:

- Pertambahan dilakukan dengan menjumlahkan semua suku dari kedua *polynomial* (suku dengan pangkat yang sama dijadikan satu dengan menjumlahkan koefisien). Sebagai contoh, dengan $R = \mathbf{Z}/3\mathbf{Z}$, jika $p_1 = x^5+2x^3+x^2+2$ dan $p_2 = x^4+2x^3+x^2$ maka $p_1+p_2 = x^5+x^4+x^3+2x^2+2$. Penjumlahan koefisien dilakukan dengan aritmatika R, dalam contoh menggunakan aritmatika modulo 3.

- Perkalian dilakukan dengan mengalikan setiap suku dari *polynomial* pertama dengan setiap suku dari *polynomial* kedua dan menjumlahkan semua hasil perkalian. Sebagai contoh, dengan $R = \mathbf{Z}/3\mathbf{Z}$, jika $p_1 = x^2 + 2x$ dan $p_2 = 2x + 1$ maka $p_1 \cdot p_2 = 2x^3 + (2 \cdot 2)x^2 + x^2 + 2x = 2x^3 + 2x^2 + 2x$. Lagi, aritmatika koefisien menggunakan aritmatika R.

Menggunakan notasi penjumlahan dengan

$$p_1 = \sum_{i=0}^{m} a_i x^i \text{ dan } p_2 = \sum_{j=0}^{n} b_j x^j$$

rumus pertambahan menjadi:

$$p_1 + p_2 \quad = \quad (\sum_{i=0}^{m} a_i x^i) + (\sum_{j=0}^{n} b_j x^j)$$

$$= \sum_{i=0}^{max(m,n)} (a_i + b_i)x^i.$$

Rumus untuk perkalian menjadi:

$$\begin{aligned}
p_1 \cdot p_2 &= (\sum_{i=0}^{m} a_i x^i) \cdot (\sum_{j=0}^{n} b_j x^j) \\
&= \sum_{i=0}^{m} (a_i x^i \cdot (\sum_{j=0}^{n} b_j x^j)) \\
&= \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j} \\
&= \sum_{i=0}^{m+n} \left(\sum_{j=0}^{min(i,m)} a_j b_{i-j} \right) x^i.
\end{aligned}$$

Tidak terlalu sukar untuk menunjukkan bahwa aritmatika dalam $R[x]$ mempunyai struktur aljabar *ring*. Rumus untuk pertambahan dan perkalian menunjukkan bahwa hasil pertambahan dan perkalian adalah *polynomial* dalam $R[x]$ juga, jadi kita dapatkan *closure*. Dengan

$$p_3 = \sum_{k=0}^{q} c_k x^k$$

Associativity untuk +:

$$\begin{aligned}
p_1 + (p_2 + p_3) &= (\sum_{i=0}^{m} a_i x^i) + ((\sum_{j=0}^{n} b_j x^j) + (\sum_{k=0}^{q} c_k x^k)) \\
&= ((\sum_{i=0}^{m} a_i x^i) + (\sum_{j=0}^{n} b_j x^j)) + (\sum_{k=0}^{q} c_k x^k) \\
&= (p_1 + p_2) + p_3.
\end{aligned}$$

Identity untuk +:

$$p_1 + 0 = (\sum_{i=0}^{m} a_i x^i) + 0 = \sum_{i=0}^{m} a_i x^i = p_1.$$

Commutativity untuk $+$:

$$p_1 + p_2 = (\sum_{i=0}^{m} a_i x^i) + (\sum_{j=0}^{n} b_j x^j) = (\sum_{j=0}^{n} b_j x^j) + (\sum_{i=0}^{m} a_i x^i) = p_2 + p_1.$$

Inverse untuk $+$:

$$\begin{aligned} p_1 + (-p_1) &= (\sum_{i=0}^{m} a_i x^i) + (-(\sum_{i=0}^{m} a_i x^i)) \\ &= (\sum_{i=0}^{m} a_i x^i) + (\sum_{i=0}^{m} -a_i x^i) \\ &= \sum_{i=0}^{m} (a_i x^i - a_i x^i) \\ &= 0. \end{aligned}$$

Associativity untuk $\cdot$:

$$\begin{aligned} p_1 \cdot (p_2 \cdot p_3) &= (\sum_{i=0}^{m} a_i x^i) \cdot (\sum_{j=0}^{n} \sum_{k=0}^{q} b_j c_k x^{j+k}) \\ &= \sum_{i=0}^{m} \sum_{j=0}^{n} \sum_{k=0}^{q} a_i b_j c_k x^{i+j+k} \\ &= (\sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j}) \cdot (\sum_{k=0}^{q} c_k x^k) \\ &= (p_1 \cdot p_2) \cdot p_3. \end{aligned}$$

Identity untuk $\cdot$:

$$p_1 \cdot 1 = (\sum_{i=0}^{m} a_i x^i) \cdot 1 = \sum_{i=0}^{m} a_i x^i = p_1.$$

Commutativity untuk $\cdot$:

$$p_1 \cdot p_2 = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j} = \sum_{i=0}^{n} \sum_{j=0}^{m} b_i a_j x^{i+j} = p_2 \cdot p_1.$$

Distributivity:

$$p_1 \cdot (p_2 + p_3) = (\sum_{i=0}^{m} a_i x^i) \cdot ((\sum_{j=0}^{n} b_j x^j) + (\sum_{k=0}^{q} c_k x^k))$$

$$\begin{aligned} &= (\sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j}) + (\sum_{i=0}^{m}\sum_{k=0}^{q} a_i c_k x^{i+k}) \\ &= (p_1 \cdot p_2) + (p_1 \cdot p_3). \end{aligned}$$

Jadi $R[x]$ mempunyai struktur aljabar *ring*. Jika K adalah suatu *field*, maka $K[x]$ mempunyai struktur *integral domain* karena jika

$$p_1 = \sum_{i=0}^{m} a_i x^i$$

dan

$$p_2 = \sum_{j=0}^{n} b_j x^j$$

dengan $a_m, b_n \neq 0$, maka

$$p_1 p_2 = a_m b_n x^{m+n} + \sum_{i=0}^{m+n-1} (\sum_{j=0}^{min(i,m)} a_j b_{i-j}) x^i \neq 0,$$

jadi tidak ada *zero divisor*. Untuk bab ini, kita akan fokus pada *polynomial ring* $K[x]$ dimana K merupakan suatu *field*.

Untuk bilangan bulat, efek dari algoritma pembagian dirumuskan oleh teorema 4. Teorema serupa diperlukan untuk pembagian *polynomial* dalam $K[x]$.

Teorema 22 (Pembagian Polynomial) *Untuk setiap pasangan polynomial $f, g \in K[x]$ dengan $g \neq 0$, ada sepasang polynomial $q, r \in K[x]$ dimana $f = qg + r$, dan $deg(r) < deg(g)$ atau $r = 0$.*

Jika $\deg(f) < \deg(g)$, kita dapatkan $q = 0$ dan $r = f$ sesuai dengan teorema. Jika $\deg(f) \geq \deg(g)$, kita perlu lakukan algoritma *long division* sebagai berikut, menggunakan notasi penjumlahan untuk f dan g:

$$f = \sum_{i=0}^{m} a_i x^i \text{ dan } g = \sum_{i=0}^{n} b_i x^i$$

dengan $a_m, b_n \neq 0$ dan $m \geq n$. Berikut algoritma untuk *long division*:

1. $r \leftarrow f$; $q \leftarrow 0$.

2. $c \leftarrow \frac{a_m}{b_n}$ dimana $r = \sum_{i=0}^{m} a_i x^i$ sebelum langkah ini dilakukan.

3. $r \leftarrow r - cx^{n-m} g$.

4. $q \leftarrow q + cx^{n-m}$.
5. Jika $r = 0$ atau $\deg(r) < \deg(g)$, kita selesai dengan q, r yang diinginkan. Jika tidak, ulangi dari langkah 2.

Algoritma *long division* mempunyai proposisi invarian (*invariant*):

$$f = qg + r$$

yang berlaku setelah langkah 1 dan dipertahankan oleh langkah-langkah selanjutnya. Setelah algoritma selesai,

$$r = 0 \text{ atau } \deg(r) < \deg(g)$$

juga berlaku, jadi algoritma *long division* menghasilkan q, r yang sesuai dengan teorema 22. Kita tunjukkan bahwa pasangan ini unik, jadi andaikan pasangan q, r dan pasangan q', r' keduanya sesuai dengan teorema 22, kita harus tunjukkan bahwa $q = q'$ dan $r = r'$.

$$f = qg + r = q'g + r' \Longrightarrow (q - q')g = r' - r.$$

Karena $g \neq 0$ dan $K[x]$ merupakan *integral domain*, maka $q - q' \neq 0 \Longleftrightarrow r' - r \neq 0$ (jadi $q - q' = 0 \Longleftrightarrow r' - r = 0$). Jika $q - q' \neq 0$ dan $r' - r \neq 0$

$$\deg(r') < \deg(g) \text{ dan } \deg(r) < \deg(g) \Longrightarrow \deg(r' - r) < \deg(g),$$

sedangkan

$$(q - q')g = r' - r \Longrightarrow \deg(r' - r) = \deg(q - q') + \deg(g) \geq \deg(g),$$

suatu kontradiksi. Jadi $q - q' = 0$ dan $r' - r = 0$, yang berarti $q = q'$ dan $r = r'$.

5.6 Euclidean Domain

Kita ingin tunjukkan bahwa $K[x]$ merupakan suatu *principal ideal domain*. Untuk itu kita gunakan konsep *Euclidean domain*.

Definisi 16 (Euclidean Domain) *Suatu ring R disebut Euclidean domain jika R adalah suatu integral domain dan terdapat fungsi $\delta : R \setminus \{0\} \longrightarrow \mathbf{N}$ dengan ketentuan sebagai berikut:*

1. *$\delta(fg) \geq \delta(f)$ untuk setiap $f, g \in R$ dengan $f, g \neq 0$.*
2. *Untuk setiap $f, g \in R$ dengan $f, g \neq 0$ dan $\delta(f) \geq \delta(g)$, terdapat $s, t \in R$ dimana $f - sg = t$, dan $\delta(t) < \delta(g)$ atau $t = 0$.*

Fungsi δ dinamakan *abstract degree function*, dan untuk *polynomial ring* merupakan fungsi *degree* deg. Dari definisi dan namanya, kita bisa menyimpulkan bahwa algoritma Euclid dapat digunakan untuk mencari gcd dalam *Euclidean domain*.

Teorema 23 *Jika K adalah suatu field, maka polynomial ring $K[x]$ adalah suatu Euclidean domain.*

Syarat 1 dari *Euclidean domain* dengan mudah dipenuhi oleh $K[x]$ karena mengalikan suatu *polynomial* yang bukan 0, dengan *polynomial* yang juga bukan 0, tidak akan mengurangi *degree* dari *polynomial* pertama. Syarat 2 dipenuhi oleh teorema 22.

Teorema 24 *Setiap Euclidean domain merupakan principal ideal domain.*

Untuk membuktikan teorema ini, pertama kita beri nama R untuk *Euclidean domain*. Mari kita analisa pembuatan *ideal* I untuk R. Jika $I = \{0\}$, maka $I = 0 \cdot R$ merupakan *principal ideal* dengan *generator* 0. Jika $I \neq \{0\}$, maka himpunan

$$\{\delta(r)|0 \neq r \in I\} \subseteq \mathbf{N}$$

tidak kosong dan mempunyai elemen terkecil, sebut saja m. Jadi ada elemen $a \in I$ dengan $\delta(a) = m$. Kita akan buktikan bahwa $I = aR$. Untuk $aR \subseteq I$, pembuktiannya jelas dari definisi *ideal* yaitu jika elemen *ideal* (dalam hal ini a) dikalikan dengan elemen *ring*, hasilnya tetap dalam *ideal*. Untuk kebalikannya, kita umpamakan $b \in I$. Definisi *Euclidean domain* mengatakan terdapat $s, t \in R$ dengan $b - sa = t$ dan $\delta(t) < \delta(a)$ atau $t = 0$. Karena $t = (b - sa) \in I$ dan m minimal, tidak mungkin $\delta(t) < \delta(a)$, jadi $t = 0$ dan $b = sa$ ($b \in aR$). Jadi $I \subseteq aR$ dan kita selesai membuktikan $I = aR$ yang berarti I adalah *principal ideal* dengan *generator* a, membuktikan teorema 24.

Konsep terahir yang kita bahas sebelum membahas *polynomial field* adalah konsep *unique factorization*. Sebelum menjelaskan teorema mengenai *unique factorization*, ada beberapa fakta mengenai *Euclidean domain* yang akan digunakan untuk membuktikan teorema. Untuk R suatu *Euclidean domain* dengan *abstract degree function* δ dan $0 \neq a \in R$:

1. Jika $a = bc$ adalah uraian non-trivial (b dan c adalah non-unit dalam R), maka $\delta(b) < \delta(a)$ dan $\delta(c) < \delta(a)$.

2. Jika $\delta(a) = 0$ maka a adalah unit dalam R.

3. Jika $\delta(a) = 1$ dan a adalah non-unit, maka a *irreducible*.

Untuk membuktikan fakta 1, karena simetris, kita cukup membuktikan $\delta(b) < \delta(a)$. Karena R merupakan *Euclidean domain*, kita mengetahui bahwa $\delta(b) \leq$

$\delta(a)$. Jika $\delta(b) = \delta(a)$, karena R merupakan *Euclidean domain*, terdapat $q, r \in R$ dengan

$$b = qa + r, \delta(r) < \delta(a) = \delta(b) \text{ atau } r = 0.$$

Jadi

$$\begin{aligned} r = b - qa = b - qbc = (1 - qc)b &\implies \delta(r) \geq \delta(b) \text{ atau } r = 0 \\ &\implies r = 0 \\ &\implies qc = 1 \\ &\implies c \text{ adalah unit,} \end{aligned}$$

suatu kontradiksi karena c adalah non-unit. Jadi $\delta(b) < \delta(a)$.

Untuk membuktikan fakta 2, karena R adalah *Euclidean domain*, terdapat $q, r \in R$ dengan

$$1 = qa + r, \delta(r) < \delta(a) \text{ atau } r = 0.$$

Jadi $r = 0$ karena tidak mungkin $\delta(r) < 0$, jadi $qa = 1$ yang berarti a adalah *unit*.

Untuk membuktikan fakta 3, jika a *non-unit* dan mempunyai uraian *non-trivial* $a = bc$, menurut fakta 1, $\delta(b) < \delta(a) = 1$ dan $\delta(c) < \delta(a) = 1$, jadi $\delta(b) = \delta(c) = 0$. Berdasarkan fakta 2, ini berarti b dan c adalah *unit* yang juga berarti a adalah *unit*, suatu kontradiksi. Jadi a tidak mempunyai uraian *non-trivial*, dan karena a *non-unit*, berarti a *irreducible*.

Teorema 25 (Unique Factorization) *Jika R suatu Euclidean domain,*

1. *Suatu non-unit $a \in R$ dapat diuraikan menjadi produk dari satu atau lebih faktor irreducible.*

2. *Jika*

$$a = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$$

dengan p_i, q_j irreducible untuk $1 \leq i \leq m$ dan $1 \leq j \leq n$, maka $m = n$ dan urutan faktor dapat diubah sehingga $p_i = u_i q_i$ dengan u_i berupa unit untuk setiap $1 \leq i \leq m = n$. Jadi untuk setiap i, p_i berasosiasi dengan q_i.

Untuk bagian pertama dari teorema 25, pembuktian menggunakan induksi dengan variabel induksi $k = \delta(a)$. Sebagai dasar induksi, $k = 1$ karena $\delta(a) = 0$ berarti a suatu *unit* (fakta 2 untuk *Euclidean domain*). Fakta 3 untuk *Euclidean domain* mengatakan bahwa a *irreducible* jika $\delta(a) = k = 1$, jadi uraian *non-trivial* menghasilkan satu faktor yaitu a sendiri. Sekarang kita tunjukkan langkah induksi untuk $k > 1$:

- Jika a *irreducible* kita selesai dengan uraian *non-trivial* untuk a terdiri dari satu faktor yaitu a sendiri.

- Jika tidak, berarti ada uraian *non-trivial* $a = bc$ dimana b dan c *non-unit* dan fakta 1 untuk *Euclidean domain* mengatakan $\delta(b) < \delta(a)$ dan $\delta(c) < \delta(a)$. Hipotesis induksi mengatakan b dan c masing-masing mempunyai uraian faktor *irreducible*, jadi kedua uraian dapat digabung menjadi uraian faktor *irreducible* untuk a.

Pembuktian bagian kedua dari teorema 25 menggunakan induksi dengan variabel induksi m dan dasar induksi $m = 1$. Jika $m = 1$ maka $n = 1$ karena jika $n > 1$ maka

$$p_1 = (q_1 \dots q_{n-1})q_n$$

merupakan uraian *non-trivial* untuk p_1, sesuatu yang tidak mungkin. Jadi $m = n = 1$ dan $p_1 = q_1$. Untuk langkah induksi, $m > 1$,

$$p_1 | p_1 \dots p_m \Longrightarrow p_1 | q_1 \dots q_n$$

dan karena p_1 *irreducible* maka p_1 prima menurut teorema 20 (*Euclidean domain* merupakan PID). Jadi terdapat j dengan $1 \leq j \leq n$ dimana $p_1 | q_j$. Dengan mengubah urutan jika perlu, kita dapatkan $p_1 | q_1$ dan karena p_1 dan q_1 keduanya *irreducible* berarti p_1 berasosiasi dengan q_1 (karena jika tidak maka terdapat uraian *non-trivial* $q_1 = p_1 r$, sesuatu yang tidak mungkin jika q_1 *irreducible*). Jadi terdapat *unit* u dimana $q_1 = up_1$. Setelah melakukan substitusi $q_1 = up_1$ dan menghilangkan p_1 dari persamaan, kita dapatkan

$$p_2 \dots p_m = uq_2 \dots q_n$$

dengan uq_2 *irreducible*. Hipotesis induksi menghasilkan $m = n$ dan dengan mengubah urutan jika perlu, p_i berasosiasi dengan q_i untuk $2 \leq i \leq m$. Selesai sudah pembuktian teorema 25.

Selain $K[x]$, $\mathbf{Z}$ juga merupakan *Euclidean domain*, dengan $\delta(a) = |a|$. Untuk setiap bilangan *irreducible* $a \in \mathbf{Z}$ terdapat bilangan *irreducible* $a' > 0$ dan *unit* u dimana

$$a = ua'.$$

Jika $a > 0$, kita gunakan $u = 1$ jadi $a' = a$. Jika $a < 0$, kita gunakan $u = -1$ jadi $a' = -a > 0$.

Jadi untuk $\mathbf{Z}$, setiap faktor *irreducible* dalam uraian berasosiasi dengan faktor *irreducible* positif. Setiap bilangan $a \neq 0$ *non-unit* dapat diuraikan sebagai berikut (dengan bagian 2 dari teorema 25 juga berlaku):

$$a = up_1 p_2 \dots p_n$$

dimana u adalah 1 atau -1 dan p_i adalah bilangan positif *irreducible* (jadi merupakan bilangan prima) untuk setiap $1 \leq i \leq n$. Fakta ini kerap disebut sebagai *fundamental theorem of arithmetic*. Tentunya uraian dapat mengandung suatu bilangan prima lebih dari satu kali, sebagai contoh

$$20 = 2 \cdot 2 \cdot 5.$$

Untuk $K[x]$, konsep bilangan positif *irreducible* (bilangan prima) diganti oleh konsep *monic irreducible polynomial* dimana suku dengan pangkat tertinggi dalam *irreducible polynomial* mempunyai koefisien 1. Setiap *irreducible polynomial* berasosiasi dengan suatu *monic irreducible polynomial*, jadi setiap *polynomial* f dengan $\deg(f) > 0$ (jadi $f \neq 0$ bukan *unit*) dapat diuraikan sebagai berikut:

$$f = uf_1f_2 \ldots f_n$$

dimana u adalah *unit* (jadi $u \in K$) dan f_i adalah *monic irreducible polynomial* untuk setiap $1 \leq i \leq n$. Untuk $K[x]$, setiap $a \in K$ adalah konstan dan merupakan *unit*.

Extended Euclidean algorithm dapat digunakan untuk *polynomial*, dengan input $f, g \in K[x]$ kita dapatkan $d, s, t \in K[x]$ dimana

$$d = fs + gt$$

dan d merupakan gcd dari f dan g. Tentunya kalkulasi *quotient* dan *residue* dilakukan menggunakan *long division* untuk *polynomial*. Jika hasil untuk d berupa konstan, maka f dan g koprima dan ini dapat digunakan untuk kalkulasi *inverse* modulo *irreducible polynomial* (lihat pembahasan kalkulasi *inverse* modulo bilangan yang koprima menggunakan *extended Euclidean algorithm* di bagian 3.5). Jika $d = 1$ maka *inverse* langsung didapat, sedangkan jika $d \neq 1$ merupakan konstan, maka

$$dd^{-1} = 1 = fsd^{-1} + gtd^{-1}$$

jadi kita tinggal kalikan s dan t dengan d^{-1}.

Bagaimana kita dapat memastikan bahwa suatu *monic polynomial* dengan koefisien dari suatu *finite field* merupakan *irreducible polynomial*? Seperti halnya dengan bilangan prima, algoritma deterministik untuk menentukan *irreducibility* tidak efisien, akan tetapi mempunyai kompleksitas *polynomial time*. Secara naif kita dapat mencoba membagi dengan setiap *monic polynomial* dengan *degree* tidak lebih dari setengah *degree polynomial* yang sedang diperiksa. Jika tidak ada yang dapat membagi maka *polynomial* yang diperiksa adalah *monic irreducible polynomial*. Untuk algoritma yang lebih efisien, silahkan membaca [bac96] (teorema 7.6.2), dimana pembuktiannya menggunakan konsep aljabar Berlekamp.

5.7 Polynomial Field

Kita mulai pembahasan *polynomial field* dengan teorema mengenai konstruksi *polynomial field* sebagai *quotient ring* dari *polynomial ring.*

Teorema 26 (Polynomial Field) *Jika K adalah suatu field dan $g(x)$ adalah irreducible polynomial dalam $K[x]$, maka $K[x]/g(x)K[x]$ adalah suatu field.*

Karena K merupakan *field*, teorema 23 mengatakan bahwa $K[x]$ adalah *Euclidean domain*, yang juga berarti bahwa $K[x]$ adalah PID (teorema 24). Karena $g(x)$ *irreducible*, teorema 21 mengatakan bahwa $g(x)K[x]$ adalah *ideal* maksimal. Jadi menurut bagian kedua teorema 17, $K[x]/g(x)K[x]$ adalah suatu *field*, dinamakan *polynomial field.*

Sebagai contoh, mari kita bahas *polynomial field* yang digunakan dalam algoritma enkripsi AES. *Field* untuk koefisien yang digunakan adalah $K = \mathbf{Z}/2\mathbf{Z}$, jadi aritmatika untuk koefisien adalah aritmatika modulo 2, dimana operasi pertambahan dan pengurangan menjadi operasi *exclusive or* dan operasi pengalian menjadi *logical and. Irreducible polynomial* yang digunakan adalah

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

yang mempunyai *degree* 8, jadi operasi *polynomial field* adalah operasi terhadap data sebesar 8 bit yang diinterpretasikan sebagai *polynomial* dengan *degree* maksimum 7 (setiap bit merepresentasikan koefisien dari suatu suku).

Karena *polynomial field* merupakan *quotient ring* dari *polynomial ring*, aritmatika *polynomial field* mirip dengan aritmatika *polynomial ring* (lihat bagian 5.5). Pertambahan *polynomial* dalam *polynomial field* sama dengan pertambahan *polynomial* dalam *polynomial ring.* Untuk perkalian, hasil perkalian adalah *residue* (sisa setelah dibagi dengan *irreducible polynomial*) dari perkalian *polynomial* sebagai operasi *polynomial ring.* Algoritma *long division* dapat digunakan untuk mendapatkan residue. Kita gunakan

$$\begin{aligned} f_1 &= x^6 + x^4 + x^2 + x + 1 \\ f_2 &= x^7 + x + 1 \end{aligned}$$

dengan aritmatika *polynomial field* AES sebagai contoh. Untuk pertambahan,

$$\begin{aligned} f_1 + f_2 &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\ &= x^7 + x^6 + x^4 + x^2. \end{aligned}$$

Untuk perkalian, kita lakukan perkalian dalam *polynomial ring* $K[x]$ dahulu:

$$\begin{aligned} f_1 f_2 &= x^{13} + x^{11} + x^9 + x^8 + x^7 + \\ &\quad x^7 + x^5 + x^3 + x^2 + x + \\ &\quad x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

lalu kita lakukan *long division* dengan $g(x)$ untuk mendapatkan *residue*.

$$\begin{aligned}
r_0 = f_1 f_2 &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\
x^5 g(x) &= x^{13} + x^9 + x^8 + x^6 + x^5 \\
r_1 = r_0 - x^5 g(x) &= x^{11} + x^4 + x^3 + 1 \\
x^3 g(x) &= x^{11} + x^7 + x^6 + x^4 + x^3 \\
r_2 = r_1 - x^3 g(x) &= x^7 + x^6 + 1
\end{aligned}$$

dan kita selesai karena r_2 tidak dapat dibagi oleh $g(x)$. Jadi untuk *polynomial field* AES, hasil perkalian menjadi

$$f_1 f_2 = r_2 = x^7 + x^6 + 1.$$

Dengan komputer, pertambahan untuk *polynomial field* AES dapat dilakukan secara sangat efisien menggunakan *bitwise exclusive or* dengan *operand* masing-masing 8 bit. Perkalian dapat dilakukan melalui kombinasi *shift* dan *exclusive or* dengan akumulator sebesar 16 bit. Kalkulasi *inverse* dapat dilakukan menggunakan *extended Euclidean algorithm* untuk *polynomial*.

Finite field, termasuk juga *polynomial field*, dinamakan juga *Galois field* dan diberi notasi **GF**. *Polynomial field* untuk AES diberi notasi $\mathbf{GF}(2^8)$ karena mempunyai 2^8 elemen.

5.8 Ringkasan

Tujuan utama dari bab ini adalah untuk menjelaskan *polynomial field*. Berbagai konsep digunakan untuk menjelaskan *polynomial field*, antara lain *homomorphism*, *ideal*, *principal ideal domain*, *polynomial ring* dan *Euclidean domain*. Konsep dan teorema yang berada dalam bab ini juga akan digunakan pada pembahasan *finite field* di bab 10.