Bab 10

Matematika III - Dasar untuk PKC

Di bab ini kita akan bahas berbagai topik matematika yang merupakan dasar dari kriptografi *public key* (PKC).

10.1 Fermat's Little Theorem

Teorema kecil Fermat (*Fermat's little theorem*) adalah teorema sangat penting dalam teori bilangan yang menjadi dasar dari berbagai teknik enkripsi asimetris.

Teorema 30 (Fermat's Little Theorem) *Untuk bilangan prima p dan bilangan bulat a, $a^p \equiv a \pmod{p}$ dan jika a tidak dapat dibagi oleh p, maka $a^{p-1} \equiv 1 \pmod{p}$.*

Untuk membuktikan teorema ini, pertama kita tunjukkan bahwa jika $p \not| a$, maka

$$\{0a, 1a, 2a, 3a, \ldots, (p-1)a\}$$

merupakan himpunan lengkap dari *residue classes modulo p*. Dengan kata lain, setiap elemen merupakan representasi dari satu kelas yang unik (elemen yang berbeda merepresentasikan kelas yang berbeda), dan setiap kelas mempunyai representasi dalam himpunan. Untuk itu, kita ambil $0 \leq i < p$ dan $0 \leq j < p$ dengan $i \neq j$. Jika ia dan ja berada dalam kelas yang sama, maka

$$ia \equiv ja \pmod{p},$$

yang berarti $p|(i-j)a$, dan karena $p \not| a$ maka $p|(i-j)$. Karena $i < p$ dan $j < p$, maka ini hanya bisa terjadi jika $i = j$, suatu kontradiksi karena $i \neq j$.

Jadi setiap elemen merepresentasikan kelas yang unik, dan karena ada p kelas yang berbeda, maka semua kelas ada dalam himpunan, jadi himpunan adalah himpunan lengkap dari *residue classes modulo p*. Selanjutnya, jelas bahwa $0a = 0$, jadi $1, 2, 3, \ldots, p-1$ dan $1a, 2a, 3a, \ldots (p-1)a$ hanya berbeda urutan jika setiap bilangan dianggap modulo p, dan produk dari deretan menjadi ekuivalen modulo p:

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p},$$

jadi $p|((p-1)!(a^{p-1}-1))$. Karena p tidak membagi $(p-1)!$, maka $p|a^{p-1}-1$, yang berarti

$$a^{p-1} \equiv 1 \pmod{p}$$

untuk $p \not| a$. Jika kita kalikan kedua sisi dengan a kita dapatkan

$$a^p \equiv a \pmod{p}$$

untuk $p \not| a$. Untuk $p|a$ pembuktian

$$a^p \equiv a \pmod{p}$$

sangat mudah karena $a^p \equiv 0 \equiv a \pmod{p}$. Lengkaplah pembuktian teorema 30 (*Fermat's Little Theorem*).

Teorema 30 dapat digunakan untuk mempermudah kalkulasi pemangkatan modulo bilangan prima. Sebagai contoh, kita coba kalkulasi $2^{58} \pmod{19}$. Karena 19 adalah bilangan prima dan 2 tidak dapat dibagi 19, maka teorema 30 dapat digunakan untuk mengkalkulasi

$$\begin{aligned} 2^{18} &\equiv 2^{19-1} \pmod{19} \\ &\equiv 1 \pmod{19}. \end{aligned}$$

Jadi

$$2^{58} = (2^{18})^3 \times 2^4 \equiv 1^3 \times 2^4 \equiv 16 \pmod{19}.$$

Meskipun dapat digunakan untuk mempermudah kalkulasi, dalam kriptografi, peran terpenting dari *Fermat's little theorem* adalah sebagai dasar dari berbagai teknik enkripsi asimetris.

10.2 Chinese Remainder Theorem

Seperti halnya dengan algoritma Euclid, *Chinese Remainder Theorem* merupakan penemuan penting dibidang teori bilangan yang telah berumur ribuan tahun. Aplikasi jaman dahulu mungkin untuk astronomi dimana r *events* berulang secara periodis, setiap *event* i mempunyai periode m_i, *event* i akan muncul secepatnya dalam waktu a_i, dan kita ingin mengetahui kapan semua *events* akan muncul secara bersamaan. Suatu contoh aplikasi ini adalah untuk memprediksi kapan akan terjadi gerhana.

Teorema 31 (Chinese Remainder Theorem) *Jika kita mempunyai beberapa persamaan dengan modulus berbeda sebagai berikut*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\dots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

dimana setiap pasangan modulus adalah koprima ($\gcd(m_i, m_j) = 1$ *untuk* $i \neq j$)*, maka terdapat solusi untuk* x*. Jika* x_1 *dan* x_2 *merupakan solusi untuk* x*, maka* $x_1 \equiv x_2 \pmod{M}$ *dimana* $M = m_1 m_2 \dots m_r$*.*

Pembuktian bahwa sistem persamaan seperti diatas mempunyai solusi untuk x bersifat konstruktif, jadi menghasilkan algoritma untuk mencari solusi. Kita definisikan $M_i = M/m_i$, jadi M_i merupakan produk dari semua modulus kecuali m_i. Karena $\gcd(m_i, M_i) = 1$, maka terdapat bilangan bulat N_i (*inverse* yang dapat dicari menggunakan *extended Euclidean algorithm*) dimana $M_i N_i \equiv 1 \pmod{m_i}$. Maka suatu solusi untuk x adalah

$$x = \sum_{j=1}^{r} a_j M_j N_j.$$

Untuk setiap i, karena semua suku kecuali suku i dapat dibagi dengan m_i, maka hanya suku i yang tidak $\equiv 0 \pmod{m_i}$, jadi

$$x \equiv a_i M_i N_i \equiv a_i \pmod{m_i}$$

seperti yang dikehendaki. Untuk menunjukkan bahwa solusi x unik modulo M, kita tunjukkan bahwa jika x_1 dan x_2 adalah solusi untuk x, maka $x_1 \equiv x_2 \pmod{M}$. Untuk setiap i, $x_1 \equiv x_2 \equiv a_i \pmod{m_i}$, atau $x_1 - x_2 \equiv 0 \pmod{m_i}$. Jadi $x_1 - x_2 \equiv 0 \pmod{M}$, yang berarti $x_1 \equiv x_2 \pmod{M}$.

Sebagai contoh kalkulasi dengan angka menggunakan *Chinese Remainder Theorem*, kita gunakan

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.$$

Setelah kita periksa bahwa

$$\gcd(3,5) = 1,\ \gcd(3,7) = 1,\ \gcd(5,7) = 1,$$

kita lanjutkan kalkulasi dan dapatkan

$$M = 105,\ M_1 = 35,\ M_2 = 21,\ M_3 = 15.$$

Kita dapatkan masing-masing *inverse* (bisa menggunakan *extended Euclidean algorithm*):

$$N_1 \equiv 2 \pmod 3, \quad N_2 \equiv 1 \pmod 5, \quad N_3 \equiv 1 \pmod 7.$$

Solusinya:

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233 \equiv 23 \pmod{105},$$

atau

$$x = 23 + 105n$$

dimana n adalah bilangan bulat apa saja.

10.3 Fungsi Euler

Fermat's little theorem (teorema 30) berlaku untuk modulus prima. Euler berhasil membuat generalisasi teorema 30 dengan menggunakan fungsi Euler phi (ϕ). Definisi fungsi ϕ, untuk $n > 0$, adalah sebagai berikut:

Definisi 17 (Fungsi Euler)

$$\phi(n) = \sharp\{0 \leq b < n | \gcd(b, n) = 1\}.$$

Dengan kata lain hasil fungsi adalah banyaknya bilangan bulat non-negatif dan lebih kecil dari n yang koprima dengan n. Jadi $\phi(1) = 1$ dan untuk bilangan prima p, $\phi(p) = p - 1$ karena $1, 2, 3, \ldots, p - 1$ semua koprima terhadap p, sedangkan $\gcd(p, 0) = p \neq 1$. Untuk bilangan prima p,

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Untuk membuktikan ini, perhatikan bahwa bilangan antara 0 dan p^α yang tidak koprima dengan p^α adalah yang dapat dibagi dengan p, yang banyaknya adalah $p^{\alpha-1}$, jadi $p^{\alpha-1}$ harus dikurangkan dari p^α.

Dengan menggunakan konsep fungsi Euler ϕ, *Fermat's little theorem* dapat digeneralisasi sebagai berikut:

Teorema 32

$$a^{\phi(m)} \equiv 1 \pmod m$$

jika $\gcd(a, m) = 1$.

Untuk $m = p$ bilangan prima, $\phi(p) = p - 1$, dan $\gcd(a, p) = 1$ berarti a tidak dapat dibagi oleh p, jadi kita dapatkan *Fermat's little theorem* dalam bentuk orisinil. Jadi teorema jelas berlaku jika m adalah bilangan prima. Untuk m

bukan bilangan prima, pembuktiannya menggunakan sifat *multiplicative* fungsi ϕ:

$$\phi(mn) = \phi(m)\phi(n)$$

jika $\gcd(m, n) = 1$. Untuk membuktikan sifat *multiplicative*, kita harus hitung semua bilangan bulat antara 0 dan $mn - 1$ yang koprima dengan mn (jadi tidak ada faktor bilangan yang lebih besar dari 1 yang juga merupakan faktor mn). Kita beri label j untuk bilangan yang kita hitung. Kita beri label j_1 untuk *residue* non-negatif terkecil j modulo m dan j_2 untuk *residue* non-negatif terkecil j modulo n, jadi $0 \leq j_1 < m$, $0 \leq j_2 < n$,

$$\begin{aligned} j &\equiv j_1 \pmod{m}, \\ j &\equiv j_2 \pmod{n}. \end{aligned}$$

Berdasarkan teorema 31 (*Chinese Remainder Theorem*), untuk setiap pasangan j_1, j_2, hanya ada satu j antara 0 dan $mn - 1$ yang mengakibatkan kedua persamaan diatas berlaku. Juga perhatikan bahwa j koprima dengan mn jika dan hanya jika j koprima dengan m dan n. Jadi banyaknya j yang harus dihitung sama dengan banyaknya kombinasi pasangan j_1, j_2. Banyaknya j_1 yang koprima dengan m dimana $0 \leq j_1 < m$ adalah $\phi(m)$, sedangkan banyaknya j_2 yang koprima dengan n dimana $0 \leq j_2 < n$ adalah $\phi(n)$. Jadi banyaknya j adalah $\phi(m)\phi(n)$. Selesailah pembuktian sifat *multiplicative* ϕ. Kembali ke teorema 32, kita sudah buktikan untuk m prima. Kita ingin buktikan juga untuk m berupa bilangan prima p dipangkatkan ($m = p^\alpha$). Pembuktian kita lakukan dengan cara induksi. Untuk $\alpha = 1$, kita dapatkan bentuk asli teorema 30, jadi sudah terbukti. Tinggal kita buktikan bahwa jika teorema 32 berlaku untuk $\alpha - 1$, maka ia juga berlaku untuk α (dengan $\alpha \geq 2$). Untuk $\alpha - 1$ kita dapatkan

$$\begin{aligned} a^{\phi(p^{\alpha-1})} &\equiv 1 \pmod{p^{\alpha-1}}, \text{ jadi} \\ a^{p^{\alpha-1}-p^{\alpha-2}} &\equiv 1 \pmod{p^{\alpha-1}}, \text{ yang berarti} \\ a^{p^{\alpha-1}-p^{\alpha-2}} &= 1 + p^{\alpha-1}b \text{ untuk suatu } b. \end{aligned}$$

Kita pangkatkan kedua sisi persamaan dengan p. Untuk sisi kiri persamaan kita dapatkan $a^{p^\alpha - p^{\alpha-1}}$ atau $a^{\phi(p^\alpha)}$. Untuk sisi kanan, $(1+p^{\alpha-1}b)^p$ mempunyai koefisien binomial yang dapat dibagi oleh p kecuali untuk 1 dan $(p^{\alpha-1}b)^p$. Jadi semua suku kecuali 1 dapat dibagi dengan p^α, dan sisi kanan menjadi $1 + bp^\alpha$ untuk suatu b. Persamaan menjadi

$$\begin{aligned} a^{\phi(p^\alpha)} &= 1 + bp^\alpha, \text{ yang berarti} \\ a^{\phi(p^\alpha)} &\equiv 1 \pmod{p^\alpha}. \end{aligned}$$

Selesailah pembuktian untuk $m = p^\alpha$. Selanjutnya, berdasarkan *fundamental theorem of arithmetic*, setiap bilangan dapat diuraikan menjadi

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

dimana untuk $1 \leq i \leq n$ setiap p_i merupakan bilangan prima unik. Dengan memangkatkan kedua sisi dari

$$a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$$

dengan pangkat yang sesuai, kita dapatkan

$$a^{\phi(m)} \equiv 1 \pmod{p_i^{\alpha_i}}$$

untuk $1 \leq i \leq n$. Karena untuk $i \neq j$, $p_i^{\alpha_i}$ koprima dengan $p_j^{\alpha_j}$, maka kita dapatkan

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Selesailah pembuktian teorema 32. Satu lagi teorema mengenai fungsi ϕ Euler adalah sebagai berikut:

Teorema 33

$$\sum_{d|n} \phi(d) = n.$$

Untuk membuktikan teorema 33, kita beri notasi $f(n) = \sum_{d|n} \phi(d)$, jadi $f(n)$ merupakan penjumlahan $\phi(d)$ untuk semua d yang membagi n. Kita harus tunjukkan bahwa $f(n) = n$, tetapi pertama kita tunjukkan lebih dahulu bahwa $f(n)$ bersifat *multiplicative*, yaitu $f(mn) = f(m)f(n)$ jika $\gcd(m, n) = 1$. Kita mengetahui bahwa pembagi $d|mn$ dapat diuraikan menjadi $d_1 \cdot d_2$ jika $\gcd(m, n) = 1$, dimana $d_1|m$ dan $d_2|n$. Karena $\gcd(d_1, d_2) = 1$, kita dapatkan $\phi(d) = \phi(d_1)\phi(d_2)$. Untuk mencari semua $d|mn$, kita harus mencari semua kombinasi d_1, d_2 dimana $d_1|m$ dan $d_2|n$. Jadi

$$\begin{aligned} f(mn) &= \sum_{d_1|m} \sum_{d_2|n} \phi(d_1)\phi(d_2) \\ &= (\sum_{d_1|m} \phi(d_1))(\sum_{d_2|n} \phi(d_2)) \\ &= f(m)f(n). \end{aligned}$$

Kembali ke pembuktian teorema 33, berdasarkan *fundamental theorem of arithmetic*, setiap n dapat diuraikan dalam bentuk $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, dimana setiap p_i adalah bilangan prima yang unik. Karena f bersifat *multiplicative*, $f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r})$. Jadi kita cukup menunjukkan bahwa $f(p^\alpha) = p^\alpha$. Karena p merupakan bilangan prima, pembagi dari p^α adalah p^j untuk $0 \leq j \leq \alpha$. Jadi

$$f(p^\alpha) = \sum_{j=0}^{\alpha} \phi(p^j)$$

$$\begin{aligned} &= 1 + \sum_{j=1}^{\alpha} p^j - p^{j-1} \\ &= p^\alpha. \end{aligned}$$

Selesailah pembuktian teorema 33.

10.4 Group of Units

Kerap untuk suatu *finite ring* $\mathbf{Z}/n\mathbf{Z}$ (yang merupakan *finite field* jika n prima), kita ingin fokus pada elemen-elemen yang mempunyai *inverse* (elemen-elemen yang merupakan *unit*). Ternyata elemen-elemen tersebut membentuk suatu *multiplicative group* $(\mathbf{Z}/n\mathbf{Z})^*$ karena

- untuk *unit* $[a]$ dan $[b]$, $[a][b] = [ab]$ merupakan *unit* karena jika $[a]$ mempunyai *inverse* $[a]^{-1} = [u]$ dan $[b]$ mempunyai *inverse* $[b]^{-1} = [v]$ maka $[ab][uv] = [au][bv] = 1$, jadi $[ab]$ mempunyai *inverse* $[uv]$ (*closure*);
- untuk *unit* $[a]$, $[b]$ dan $[c]$, $([a][b])[c] = [a]([b][c])$ (*associativity*);
- terdapat elemen *identity* $[1]$ (*identity*); dan
- setiap elemen mempuyai *inverse*.

Patut diperhatikan bahwa untuk bilangan prima p dan bilangan $n > 1$, $\mathbf{Z}/p^n\mathbf{Z}$ tidak sama dengan $\mathbf{GF}(p^n)$: $\mathbf{Z}/p^n\mathbf{Z}$ merupakan *finite ring* tetapi bukan *finite field*, sedangkan $\mathbf{GF}(p^n)$ merupakan *finite field*. $\mathbf{GF}(p^n)^*$ akan dibahas di bagian 10.7.

Untuk setiap elemen $[a] \in (\mathbf{Z}/n\mathbf{Z})^*$, kita ketahui bahwa $\gcd(a, n) = 1$, jadi banyaknya elemen dalam $(\mathbf{Z}/n\mathbf{Z})^*$ adalah $\phi(n)$. Suatu *multiplicative group* $(\mathbf{Z}/n\mathbf{Z})^*$ disebut *cyclic* jika mempunyai elemen a dengan *order* (pangkat positif terkecil dari a yang menghasilkan 1) $\phi(n)$, dan elemen a disebut *generator* karena setiap elemen dalam *group* merupakan pemangkatan dari a.

Teorema 34 *Jika a adalah elemen dari $(\mathbf{Z}/n\mathbf{Z})^*$ untuk suatu bilangan n, maka order dari a (yang kita beri label d) membagi $\phi(n)$.*

Pembuktian teorema 34 menggunakan teorema 32 yang mengatakan bahwa $a^{\phi(n)} = 1$ (dalam $(\mathbf{Z}/n\mathbf{Z})$). Jika d tidak membagi $\phi(n)$, maka terdapat $0 < r < d$ dimana

$$bd + r = \phi(n)$$

untuk suatu b, dan

$$a^r = a^{\phi(n)-bd} \equiv 1 \pmod{n}.$$

Ini adalah suatu kontradiksi karena d merupakan pangkat positif a terkecil yang menghasilkan 1. Jadi d membagi $\phi(n)$, dan selesailah pembuktian teorema 34.

Karena setiap elemen a dalam $(\mathbf{Z}/n\mathbf{Z})^*$ mempunyai *order* (sebut saja d), a menjadi *generator* untuk suatu *cyclic subgroup*:

$$G_a = \{a^1, a^2, \ldots, a^d = a^0\}$$

karena kita dapatkan:

- jika $x, y \in G_a$ (jadi terdapat $1 \leq i \leq d$ dan $1 \leq j \leq d$ dimana $x = a^i, y = a^j$), maka $xy \in G_a$ (karena $xy = a^{ij} = a^{ij \bmod d}$), jadi kita dapatkan *closure*;
- jika $x, y, z \in G_a$ (jadi terdapat $1 \leq i \leq d$, $1 \leq j \leq d$ dan $1 \leq k \leq d$ dimana $x = a^i, y = a^j, z = a^k$), maka $(xy)z = x(yz)$ (karena $(xy)z = (a^i a^j)a^k = a^i(a^j a^k) = x(yz)$), jadi kita dapatkan *associativity*;
- kita dapatkan $a^d = a^0 = 1 \in G_a$, jadi G_a memiliki *identity*; dan
- untuk a^i dengan $1 \leq i \leq d$, kita dapatkan a^{d-i} yang juga merupakan elemen dari G_a dengan $a^i a^{d-i} = a^d = 1$, jadi setiap elemen dalam G_a mempunyai *inverse* dalam G_a.

Tentunya *order* dari *generator* untuk suatu *cyclic group* sama dengan banyaknya elemen dalam *group* tersebut. Istilah *order* juga kerap digunakan untuk banyaknya elemen dalam *group*. Untuk *cyclic group*, *order* dari *group* sama dengan *order* dari *generator*.

Kita mulai pembahasan struktur $(\mathbf{Z}/n\mathbf{Z})^*$ dengan membahas struktur dari $(\mathbf{Z}/2^e\mathbf{Z})^*$.

Teorema 35 *Multiplicative group* $(\mathbf{Z}/2^e\mathbf{Z})^*$ *cyclic hanya untuk* $e = 1, 2$.

Untuk $e = 1$ kita dapatkan $(\mathbf{Z}/2^1\mathbf{Z})^* = \{1\}$ *cyclic* karena elemen 1 mempunyai *order* $\phi(2) = 1$. Untuk $e = 2$ kita dapatkan $(\mathbf{Z}/2^2\mathbf{Z})^* = \{1, 3\}$ *cyclic* karena elemen 3 mempunyai *order* $\phi(4) = 2$. Untuk $e > 2$ kita harus tunjukkan bahwa $(\mathbf{Z}/2^e\mathbf{Z})^*$ tidak mempunyai elemen dengan *order* $\phi(2^e) = 2^e - 2^{e-1} = 2^{e-1}$. Ini kita lakukan dengan menunjukkan bahwa

$$a^{2^{e-2}} \equiv 1 \pmod{2^e} \tag{10.1}$$

untuk setiap bilangan ganjil a (untuk a genap, $\gcd(a, 2^e) > 1$, jadi bukan elemen *group*). Kita buktikan ini dengan cara induksi. Untuk *base case* $e = 3$ kita harus buktikan

$$a^2 \equiv 1 \pmod{8}$$

untuk setiap bilangan ganjil a. Karena terdapat bilangan b dimana $a = 2b + 1$, kita dapatkan

$$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1 \equiv 1 \pmod{8}.$$

Jika persamaan 10.1 berlaku untuk suatu $e \geq 3$, maka untuk setiap bilangan ganjil a kita dapatkan

$$a^{2^{e-2}} = 1 + 2^e k$$

untuk suatu bilangan k. Kita kuadratkan:

$$\begin{aligned} a^{2^{(e+1)-2}} &= (1 + 2^e k)^2 \\ &= 1 + 2^{e+1} k + 2^{2e} k^2 \\ &= 1 + 2^{e+1}(k + 2^{2e-1} k^2) \\ &\equiv 1 \pmod{2^{e+1}} \end{aligned}$$

yang berarti persamaan 10.1 berlaku untuk $e+1$. Selesailah pembuktian induksi untuk persamaan 10.1. Walaupun $(\mathbf{Z}/2^e\mathbf{Z})^*$ untuk $e \geq 3$ bukan merupakan *cyclic group*, kita akan tunjukkan bahwa $(\mathbf{Z}/2^e\mathbf{Z})^*$ merupakan produk dari dua *cyclic group*.

Teorema 36 *Untuk $e \geq 3$, $(\mathbf{Z}/2^e\mathbf{Z})^*$ merupakan produk dari dua cyclic group dengan generator 5 dan -1.*

Dengan menggunakan persamaan 10.1 kita dapatkan untuk $e \geq 3$:

$$5^{2^{e-2}} \equiv 1 \pmod{2^e}. \tag{10.2}$$

Kita ingin juga tunjukkan bahwa untuk $e \geq 3$:

$$5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}. \tag{10.3}$$

Ini kita lakukan dengan induksi. Untuk $e = 3$ kita dapatkan

$$\begin{aligned} 5^{2^{e-3}} &= 5^{2^{3-3}} \\ &= 5^{2^0} \\ &= 5 \\ &= 1 + 2^{3-1} \\ &= 1 + 2^{e-1}. \end{aligned}$$

Untuk langkah induksi kita umpamakan

$$5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$$

jadi

$$5^{2^{e-3}} = 1 + n2^{e-1}$$

untuk suatu bilangan ganjil n (karena jika n genap maka $5^{2^{e-3}} = 1 + n2^{e-1}$ berarti $5^{2^{e-3}} \equiv 1 \pmod{2^e}$, bukan $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$). Kita harus tunjukkan bahwa

$$5^{2^{e-2}} \equiv 1 + 2^e \pmod{2^{e+1}}.$$

Kita dapatkan

$$\begin{aligned} 5^{2^{e-2}} &= (5^{2^{e-3}})^2 \\ &= (1+n2^{e-1})^2 \\ &= 1+2n2^{e-1}+n^2 2^{2e-2} \\ &= 1+n2^e+n^2 2^{2e-2} \\ &\equiv 1+2^e \pmod{2^{e+1}} \end{aligned}$$

karena 2^{2e-2} dapat dibagi oleh 2^{e+1} untuk $e \geq 3$ dan $n2^e$ menyisakan 2^e jika dibagi oleh 2^{e+1} (karena n ganjil). Selesailah pembuktian persamaan 10.3 dengan induksi. Dari persamaan 10.2 dan 10.3 kita dapatkan 2^{e-2} sebagai *order* dari 5, jadi 5 adalah *generator* untuk *cyclic subgroup* dengan 2^{e-2} elemen:

$$\{5 \pmod{2^e}, 5^2 \pmod{2^e}, \ldots, 5^{2^{e-2}} \equiv 1 \pmod{2^e}\}.$$

Meneruskan pembuktian teorema 36, -1 merupakan *generator* untuk *cyclic subgroup* $\{-1, 1\}$. Kita ingin tunjukkan bahwa produk dua *cyclic group*, berupa himpunan semua elemen berbentuk $5^i(-1)^j$ dengan $0 \leq i < 2^{e-2}$ dan $0 \leq j < 2$, menghasilkan *group* $(\mathbf{Z}/2^e\mathbf{Z})^*$ yang merupakan himpunan bilangan ganjil $\{1, 3, 5, 2^e - 1\}$. Karena $5 \equiv 1 \pmod 4$, maka $\{5^i \pmod{2^e} | 0 \leq i < 2^{e-2}\}$ membentuk setengah dari $(\mathbf{Z}/2^e\mathbf{Z})^*$, sedangkan sisanya setengah lagi dibentuk oleh $\{-(5^i) \pmod{2^e} | 0 \leq i < 2^{e-2}\}$, jadi

$$(\mathbf{Z}/2^e\mathbf{Z})^* = \{5^i(-1)^j \pmod{2^e} | 0 \leq i < 2^{e-2}, 0 \leq j < 2\}.$$

Selesailah pembuktian teorema 36.

Teorema 37 *Jika p adalah bilangan prima, maka terdapat $\phi(d)$ elemen dengan order d dalam $(\mathbf{Z}/p\mathbf{Z})^*$, untuk setiap d yang membagi $p-1$.*

Untuk setiap $d|p-1$ kita definisikan

$$\Omega_d = \{a \in (\mathbf{Z}/p\mathbf{Z})^* | a \text{ mempunyai } \textit{order } d\} \text{ dan } \omega(d) = |\Omega_d|$$

jadi $\omega(d)$ adalah banyaknya elemen yang mempunyai *order* d dalam $(\mathbf{Z}/p\mathbf{Z})^*$. Jadi kita harus tunjukkan bahwa

$$\omega(d) = \phi(d)$$

untuk setiap $d|p-1$. Teorema 34 mengatakan bahwa setiap elemen mempunyai *order* yang membagi $\phi(p) = p-1$, jadi himpunan-himpunan Ω_d mempartisi $(\mathbf{Z}/p\mathbf{Z})^*$, oleh karena itu

$$\sum_{d|p-1} \omega(d) = p-1.$$

Teorema 33 dengan $p-1$ menggantikan n menghasilkan

$$\sum_{d|p-1} \phi(d) = p-1,$$

jadi

$$\sum_{d|p-1} (\phi(d) - \omega(d)) = 0.$$

Jika kita dapat tunjukkan bahwa $\omega(d) \leq \phi(d)$ untuk setiap $d|p-1$, karena total penjumlahan adalah 0, maka $\omega(d) = \phi(d)$. Untuk Ω_d yang kosong jelas $\omega(d) \leq \phi(d)$, jadi kita dapat mengumpamakan terdapat elemen $a \in \Omega_d$. Berdasarkan definisi Ω_d, setiap hasil pemangkatan

$$a^1, a^2, \ldots a^d$$

berbeda, dan

$$(a^i)^d = 1$$

untuk $i = 1, 2, \ldots, d$. jadi setiap a^i merupakan akar dari *polynomial* $f(x) = x^d - 1$ dalam $(\mathbf{Z}/p\mathbf{Z})$. Karena banyaknya akar untuk $f(x)$ maksimum d, maka $a^1, a^2, \ldots a^d$ membentuk himpunan akar yang komplit. Kita ingin tunjukkan bahwa Ω_d terdiri dari akar-akar a^i dimana $\gcd(i,d) = 1$. Jika $b \in \Omega_d$, maka $b = a^i$ untuk suatu $1 \leq i \leq d$. Dengan $j = \gcd(i,d)$,

$$b^{d/j} = a^{id/j} = (a^d)^{i/j} = 1^{i/j} = 1$$

dalam $(\mathbf{Z}/p\mathbf{Z})$. Tetapi b mempunyai *order* d, jadi tidak ada pangkat dari b yang lebih kecil dari d yang menghasilkan 1, jadi $j = 1$. Jadi setiap elemen $b \in \Omega_d$ mempunyai bentuk a^i dengan $1 \leq i \leq d$ dan $\gcd(i,d) = 1$, jadi terdapat $\phi(d)$ elemen dalam Ω_d. Jadi kita sudah tunjukkan bahwa $\omega(d) = \phi(d)$ dan selesailah pembuktian teorema 37. Sebagai konsekuensi dari teorema 37, kita dapatkan $(\mathbf{Z}/p\mathbf{Z})^*$ merupakan *cyclic group* karena terdapat $\phi(p-1) = \phi(\phi(p))$ elemen dengan *order* $p-1 = \phi(p)$.

Teorema 38 *Untuk bilangan prima p yang ganjil dan $e \geq 1$, $(\mathbf{Z}/p^e\mathbf{Z})^*$ merupakan cyclic group.*

Kita sudah tunjukkan ini untuk $e = 1$. Untuk $e \geq 2$ kita akan buktikan teorema 38 dengan membuktikan bahwa terdapat *generator* untuk $(\mathbf{Z}/p^e\mathbf{Z})^*$. Kita mulai dengan *generator* untuk $(\mathbf{Z}/p^2\mathbf{Z})^*$. Karena $(\mathbf{Z}/p\mathbf{Z})^*$ *cyclic* maka terdapat *generator* g untuk $(\mathbf{Z}/p\mathbf{Z})^*$ dimana

$$g^{p-1} \equiv 1 \pmod{p}$$

tetapi

$$g^i \not\equiv 1 \pmod{p}$$

untuk $1 \leq i < p-1$. Karena $\gcd(g,p) = 1$, maka $\gcd(g^2,p) = 1$, jadi g juga merupakan elemen (tetapi belum tentu *generator*) untuk $(\mathbf{Z}/p^2\mathbf{Z})^*$. Jika d adalah *order* dari g dalam $(\mathbf{Z}/p^2\mathbf{Z})^*$, maka teorema 34 mengatakan bahwa $d|\phi(p^2)$, jadi d membagi $p(p-1)$. Karena $g^d \equiv 1 \pmod{p^2}$ maka $g^d \equiv 1 \pmod{p}$. Tetapi g mempunyai *order* $p-1$ dalam $(\mathbf{Z}/p\mathbf{Z})^*$, jadi $p-1|d$. Karena $d|p(p-1)$, $p-1|d$ dan p adalah bilangan prima, maka hanya ada dua kemungkinan:

$$\begin{aligned} d &= p-1 \text{ atau} \\ d &= p(p-1). \end{aligned}$$

Jika $d = p(p-1)$ maka g menjadi *generator* untuk $(\mathbf{Z}/p^2\mathbf{Z})^*$ dan kita selesai, jadi kita lanjutkan dengan $d = p-1$. Kita buat $h = g+p$, jadi $h \equiv g \pmod{p}$ yang berarti h adalah *generator* untuk $(\mathbf{Z}/p\mathbf{Z})^*$, jadi seperti halnya dengan g, h mempunyai *order* $p-1$ atau $p(p-1)$ dalam $(\mathbf{Z}/p^2\mathbf{Z})^*$. Karena $g^{p-1} \equiv 1 \pmod{p^2}$, kita dapatkan

$$\begin{aligned} h^{p-1} &= (g+p)^{p-1} \\ &= g^{p-1} + (p-1)g^{p-2}p + \ldots \\ &= g^{p-1} + p^2g^{p-2} - pg^{p-2} + \ldots \\ &\equiv 1 - pg^{p-2} \pmod{p^2} \end{aligned}$$

karena suku-suku yang direpresentasikan oleh ... semua dapat dibagi oleh p^2. Karena $\gcd(g,p) = 1$, maka $pg^{p-2} \not\equiv 0 \pmod{p^2}$, jadi $h^{p-1} \not\equiv 1 \pmod{p^2}$ yang berarti *order* dari h bukan $p-1$. Jadi *order* dari h dalam $(\mathbf{Z}/p^2\mathbf{Z})^*$ adalah $p(p-1)$ yang berarti kita mempunyai *generator* h untuk $(\mathbf{Z}/p^2\mathbf{Z})^*$. Selesailah pembuktian untuk $e = 2$. Untuk $e \geq 2$ kita akan buktikan dengan induksi bahwa *generator* h untuk $(\mathbf{Z}/p^2\mathbf{Z})^*$ juga merupakan *generator* untuk $(\mathbf{Z}/p^e\mathbf{Z})^*$. Apabila h adalah suatu *generator* untuk $(\mathbf{Z}/p^e\mathbf{Z})^*$, karena $\gcd(h,p^e) = 1$, maka $\gcd(h,p^{e+1}) = 1$. Jadi h merupakan elemen (walaupun belum tentu *generator* untuk $(\mathbf{Z}/p^{e+1}\mathbf{Z})^*$. Jika d adalah *order* dari h dalam $(\mathbf{Z}/p^{e+1}\mathbf{Z})^*$, maka teorema 34 mengatakan bahwa $d|\phi(p^{e+1})$, jadi d membagi $p^e(p-1)$. Karena $h^d \equiv 1 \pmod{p^{e+1}}$, maka $h^d \equiv 1 \pmod{p^e}$. Tetapi h mempunyai *order* $p^{e-1}(p-1)$ dalam $(\mathbf{Z}/p^e\mathbf{Z})^*$, jadi $p^{e-1}(p-1)$ membagi d. Karena $d|p^e(p-1)$, $p^{e-1}(p-1)|d$ dan p merupakan bilangan prima, maka hanya ada dua kemungkinan:

$$\begin{aligned} d &= p^e(p-1) \text{ atau} \\ d &= p^{e-1}(p-1). \end{aligned}$$

Jika $d = p^e(p-1)$, maka h merupakan *generator* untuk $(\mathbf{Z}/p^{e+1}\mathbf{Z})^*$. Kita ingin tunjukkan bahwa $d = p^{e-1}(p-1)$ adalah sesuatu yang tidak mungkin, jadi kita ingin tunjukkan bahwa $h^{p^{e-1}(p-1)} \not\equiv 1 \pmod{p^{e+1}}$. Karena h merupakan *generator* untuk $(\mathbf{Z}/p^e\mathbf{Z})^*$, maka h mempunyai *order* $\phi(p^e) = p^{e-1}(p-1)$ dalam

$(\mathbf{Z}/p^e\mathbf{Z})^*$, jadi $h^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$. Akan tetapi $p^{e-2}(p-1) = \phi(p^{e-1})$, jadi $h^{p^{e-2}(p-1)} \equiv 1 \pmod{p^{e-1}}$. Jadi kita dapatkan $h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$. Kita pangkatkan kedua sisi persamaan dengan p:

$$\begin{aligned} h^{p^{e-1}(p-1)} &= (1 + kp^{e-1})^p \\ &= 1 + pkp^{e-1} + \frac{p(p-1)}{2}(kp^{e-1})^2 + \dots \\ &= 1 + kp^e + \frac{1}{2}k^2p^{2e-1}(p-1) + \dots \end{aligned}$$

dimana suku-suku yang direpresentasikan oleh $\dots$ dapat dibagi oleh $(p^{e-1})^3$, jadi dapat dibagi oleh p^{e+1} karena $3(e-1) \geq e+1$ untuk $e \geq 2$, jadi

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e + \frac{1}{2}k^2p^{2e-1}(p-1) \pmod{p^{e+1}}.$$

Karena p ganjil, maka $\frac{1}{2}k^2p^{2e-1}(p-1)$ dapat dibagi oleh p^{e+1} karena $2e-1 \geq e+1$ untuk $e \geq 2$, jadi

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \pmod{p^{e+1}}.$$

Karena p tidak membagi k, maka $kp^e \not\equiv 0 \pmod{p^{e+1}}$, jadi

$$h^{p^{e-1}(p-1)} \not\equiv 1 \pmod{p^{e+1}}.$$

Selesailah pembuktian induksi dan selesailah pembuktian teorema 38.

10.5 Homomorphism Theorem

Di bagian 5.2 kita telah membahas konsep *homomorphism* dan *ideal* untuk struktur *ring*. Disini akan kita lanjutkan pembahasan *homomorphism*, dimulai dengan pembahasan *homomorphism theorem* sampai dengan teorema *isomorphism*, yang akan digunakan dalam pembahasan *field extension* di bagian 10.6.

Untuk suatu *homomorphism* $\varphi : R \to S$ antar dua *ring*, dan setiap $a, b \in R$,

$$\varphi(a) = \varphi(b) \iff \varphi(a-b) = 0 \iff (a-b) \in \ker(\varphi).$$

Jadi φ mengumpulkan elemen-elemen R yang perbedaannya berada dalam *ideal* $\ker(\varphi)$. Jika *ideal* $I \subseteq \ker(\varphi)$, maka kita dapat uraikan efek dari φ menjadi dua langkah:

1. Kita kumpulkan elemen-elemen yang perbedaannya berada dalam *ideal* I melalui R/I.

2. Karena $I \subseteq \ker(\varphi)$ maka elemen-elemen yang perbedaannya berada dalam *ideal* I juga telah dikumpulkan oleh φ, jadi kita dapat melanjutkan dari R/I ke S sehingga komposisi langkah 1 dan 2 menghasilkan φ.

Inilah isi dari teorema berikut.

Teorema 39 (Homomorphism Theorem) *Jika $\varphi : R \longrightarrow S$ merupakan homomorphism antar ring, I merupakan ideal dari R dengan $I \subseteq ker(\varphi)$ dan kita beri label χ untuk canonical homomorphism dari R ke R/I, maka pemetaan ψ:*

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

telah didefinisikan dengan baik (well-defined). ψ adalah homomorphism antar ring yang mematuhi $\psi \circ \chi = \varphi$.

$$\begin{array}{ccc} R & \overset{\varphi}{\longrightarrow} & S \\ \chi \downarrow & \nearrow \psi & \\ R/I & & \end{array}$$

ψ surjective jika dan hanya jika φ surjective. ψ injective jika dan hanya jika $I = ker(\varphi)$.

Untuk menunjukkan bahwa ψ telah didefinisikan dengan baik, kita harus tunjukkan bahwa nilai $\varphi(a)$ tidak tergantung pada representasi $a + I$ yang dipilih. Jika $a, a' \in R$ dengan $a + I = a' + I$, maka

$$a - a' \in I \subseteq \ker(\varphi),$$

yang berarti

$$0 = \varphi(a - a') = \varphi(a) - \varphi(a').$$

Jadi $\varphi(a) = \varphi(a')$, yang berarti nilai $\varphi(a)$ independen dari representasi $a + I$ yang dipilih. Untuk menunjukkan bahwa ψ adalah suatu *homomorphism*, kita dapatkan

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

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

$$\psi(1+I) = \varphi(1_R) = 1_S.$$

Untuk menunjukkan bahwa $\psi \circ \chi = \varphi$, jika $a \in R$,

$$\psi(\chi(a)) = \psi(a+I) = \varphi(a).$$

Jika φ *surjective*, maka $\psi \circ \chi$ *surjective*, jadi ψ *surjective*. Sebaliknya, jika ψ *surjective*, maka φ yang merupakan komposisi dua pemetaan *surjective* $(\psi \circ \chi)$ juga surjective. Jika ψ *injective*, untuk $a \in \ker(\varphi)$,

$$\psi(a+I) = \varphi(a) = 0.$$

Karena ψ *injective*, maka $a + I = 0_{R/I} = I$, jadi $a \in I$. Jadi $\ker(\varphi) \subseteq I$, dan karena $I \subseteq \ker(\varphi)$, maka $I = \ker(\varphi)$. Sebaliknya, dengan $I = \ker(\varphi)$, untuk menunjukkan bahwa ψ *injective*, kita harus tunjukkan bahwa $\ker(\psi) = \{0\} = \{I\}$. Jika $a + I \in \ker(\psi)$, maka $\varphi(a) = \psi(a + I) = 0$. Jadi $a \in \ker(\varphi)$, yang berarti $a \in I$. Jadi $a + I = I$, yang berarti $\ker(\psi)$ hanya berisi I. Selesailah pembuktian teorema 39.

Tiga teorema berikut adalah teorema mengenai *isomorphism* yang sudah merupakan standard dalam aljabar abstrak.

Teorema 40 (First Isomorphism Theorem) *Jika $\varphi : R \longrightarrow S$ merupakan homomorphism antar ring, maka*

$$R/ker(\varphi) \simeq \varphi(R).$$

Untuk membuktikan teorema ini, kita gunakan teorema 39 dengan $I = \ker(\varphi)$, dengan hasil *injective homomorphism* ψ:

$$\begin{aligned}R/\ker(\varphi) &\longrightarrow S\\ \psi(a+\ker(\varphi)) &\mapsto \varphi(a).\end{aligned}$$

Karena $\psi \circ \chi = \varphi$, dimana χ adalah *canonical homomorphism* dari R ke $R/\ker(\varphi)$, kita dapatkan $\psi(R/\ker(\varphi)) = \varphi(R)$. Jadi sebagai pemetaan dari $R/\ker(\varphi)$ ke $\psi(R/\ker(\varphi))$, ψ bersifat *surjective*. Karena bersifat *injective* dan *surjective*, ψ dari $R/\ker(\varphi)$ ke $\psi(R/\ker(\varphi))$ bersifat *bijective*, jadi (karena $\psi(R/\ker(\varphi)) = \varphi(R)$)

$$R/\ker(\varphi) \simeq \varphi(R).$$

Selesailah pembuktian teorema 40.

Sebelum membahas teorema kedua mengenai *isomorphism*, kita perlu definisikan terlebih dahulu konsep *subring* dan *subfield*.

Definisi 18 (Subring) *Untuk ring R dan $S \subseteq R$, jika*

- $1 \in S$,
- $a - b \in S$ *untuk setiap* $a, b \in S$ *dan*
- $ab \in S$ *untuk setiap* $a, b \in S$,

maka S adalah subring dari R.

Tidak terlalu sulit untuk menunjukkan bahwa $0 \in S$ karena $a - a \in S$, jadi S juga mempunyai struktur *ring*. Jika S merupakan suatu *field*, maka S disebut *subfield* dari R. Jika S dan R merupakan *field*, maka R adalah *field extension* dari S. Dalam teori mengenai *field*, biasanya kita hanya ingin menunjukkan bahwa K *isomorphic* dengan *subfield* dari F, dimana K dan F keduanya merupakan *field*. Untuk itu kita hanya perlu menunjukkan bahwa terdapat *injective field homomorphism* dari K ke F. Ini dapat ditunjukkan menggunakan teorema 40 (*First Isomorphism Theorem*) dengan $R = K, S = F,$ dan $\ker(\varphi) = \{0\}$.

Teorema 41 (Second Isomorphism Theorem) *Jika R adalah suatu ring, S merupakan subring dari R, I merupakan proper ideal dari R, maka*

$$S/(S \cap I) \simeq (S + I)/I$$

dimana $S + I = \{s + a | s \in S, a \in I\}$.

Mari kita buktikan teorema 41. Jika $\iota : S \longrightarrow (S + I)$ dan $\chi : (S + I) \longrightarrow (S + I)/I$ adalah *homomorphism* dengan

$$\begin{aligned} \iota : s &\mapsto s \\ \chi : a &\mapsto a + I \end{aligned}$$

maka $\varphi = \chi \circ \iota$ juga merupakan *homomorphism* dari S ke $(S + I)/I$, jadi

$$S/\ker(\varphi) \simeq \varphi(S).$$

Jadi jika kita dapat tunjukkan bahwa $\ker(\varphi) = S \cap I$ dan $\varphi(S) = (S + I)/I$ (φ *surjective*) maka selesailah pembuktian kita. Jika $s \in \ker(\varphi)$ maka $s \in I$, dan karena $s \in S$, maka $s \in S \cap I$. Sebaliknya jika $s \in S \cap I$ maka $\varphi(s) = I$, jadi $s \in \ker(\varphi)$. Jadi kita sudah tunjukkan bahwa $\ker(\varphi) = S \cap I$. Untuk menunjukkan bahwa φ *surjective*, kita harus tunjukkan bahwa untuk sembarang $b + I \in (S + I)/I$ terdapat $s \in S$ dimana $\varphi(s) = b + I$. Jika kita pilih $s \in S$ dan $a \in I$ dimana $b = s + a$ maka

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

Selesailah pembuktian teorema 41.

Sebelum membahas teorema ketiga mengenai *isomorphism*, kita perlu definisikan dahulu notasi J/I untuk I dan J berupa *ideal*, dan buat teorema mengenai *bijection* antara himpunan *ideal*.

Definisi 19 *Jika I merupakan proper ideal dalam R dan J merupakan ideal dalam R dengan $I \subseteq J$, maka*

$$J/I = \{a + I | a \in J\}.$$

Jadi J/I merupakan *image* dari J berdasarkan *canonical homomorphism* dari R ke R/I dan tidak terlalu sulit untuk melihat bahwa J/I merupakan *ideal* dalam R dan dalam R/I.

Teorema 42 *Jika I merupakan proper ideal dalam ring R, maka terdapat bijection dari himpunan ideal yang mencakup I dalam R ke himpunan ideal dalam R/I. Bijection tersebut mempunyai pemetaan sebagai berikut:*

$$J \mapsto J/I.$$

Kita mulai pembuktian teorema 42 dengan membuat

$$\varphi : R \longrightarrow R/I$$

sebagai *canonical homomorphism*, jadi $\ker(\varphi) = I$. Tidak terlalu sulit untuk melihat bahwa φ memetakan suatu *homomorphism* J ke J/I sesuai teorema 42. Jika $\mathcal{I}_\varphi$ merupakan himpunan semua *ideal* dalam R yang mencakup I dan $\mathcal{I}_S$ merupakan himpunan semua *ideal* dalam R/I, kita ingin tunjukkan bahwa pemetaan

$$\begin{array}{rcl} \chi : \mathcal{I}_\varphi & \longrightarrow & \mathcal{I}_S \\ J_\varphi & \mapsto & \varphi(J_\varphi) \end{array}$$

merupakan pemetaan yang *bijective*, dimana $\varphi(J_\varphi)$ merupakan *image* dari J_φ menurut φ. Jadi kita harus tunjukkan bahwa dengan pemetaan

$$\begin{array}{rcl} \kappa : \mathcal{I}_S & \longrightarrow & \mathcal{I}_\varphi \\ J_S & \mapsto & \varphi^{-1}(J_S) \end{array}$$

maka

$$\kappa \circ \chi = \mathrm{id}_{\mathcal{I}_\varphi}$$

dan

$$\chi \circ \kappa = \mathrm{id}_{\mathcal{I}_S},$$

dimana $\varphi^{-1}(J_S)$ adalah *inverse image* dari J_S menurut φ. Untuk menunjukkan persamaan pertama, kita harus tunjukkan bahwa

$$\varphi^{-1}(\varphi(J_S)) = J_S$$

untuk setiap $J_S \in \mathcal{I}_S$. Jelas bahwa $J_S \subseteq \varphi^{-1}(\varphi(J_S))$. Untuk menunjukkan bahwa $\varphi^{-1}(\varphi(J_S)) \subseteq J_s$, mari kita lihat apa konsekuensi dari $a \in \varphi^{-1}(\varphi(J_S))$. Karena $\varphi(a) \in \varphi(J_S)$ maka terdapat $a' \in J_S$ dimana $\varphi(a) = \varphi(a')$. Jadi $a - a' \in \ker(\varphi) \subseteq J_S$, jadi

$$a = a' + (a - a') \in J_S.$$

Untuk menunjukkan persamaan kedua, kita harus tunjukkan bahwa

$$\varphi(\varphi^{-1}(J_\varphi)) = J_\varphi$$

untuk setiap $J_\varphi \in \mathcal{I}_\varphi$, yang jelas terpenuhi karena φ *surjective*. Selesailah pembuktian teorema 42.

Teorema 43 (Third Isomorphism Theorem) *Jika R adalah suatu ring, I dan J merupakan proper ideal dari R dengan $I \subseteq J$ maka*

$$R/J \simeq (R/I)/(J/I).$$

Jika

$$\chi_1 : R \longrightarrow R/I \text{ dan } \chi_2 : R/I \longrightarrow (R/I)/(J/I)$$

keduanya merupakan *canonical homomorphism*, maka

$$\varphi = \chi_2 \circ \chi_1$$

yang merupakan komposisi dari dua *surjective homomorphism* merupakan suatu *surjective homomorphism*. Berarti

$$R/\ker(\varphi) \simeq \varphi(R) = (R/I)/(J/I).$$

Jadi kita tinggal menunjukkan bahwa $\ker(\varphi) = J$. Jika $a \in \ker(\varphi)$ maka

$$\varphi(a) = (a + I) + J/I = J/I$$

karena J/I merupakan 0 dalam $(R/I)/(J/I)$. Jadi $a+I \in J/I$ dan berdasarkan teorema 42, $a \in J$. Sebaliknya jika $a \in J$, maka berdasarkan definisi dari J/I, $a + I \in J$, jadi

$$\varphi(a) = (a + I) + J/I = J/I$$

yang berarti $a \in \ker(\varphi)$. Selesailah pembuktian teorema 43.

10.6 Field Extension

Kita akan bahas konsep *field extension*, tetapi sebelumnya perlu dijelaskan konsep *restriction* yang berlaku pada relasi (termasuk fungsi dan *morphism*). Suatu relasi dapat dipandang sebagai himpunan dari pasangan berurut (*ordered pair*), dimana elemen pertama dalam suatu pasangan berasal dari *domain* relasi dan elemen kedua berasal dari *range* relasi. Untuk suatu relasi R, R *restricted* pada D (diberi notasi $R \restriction D$) adalah subrelasi dari R yang terdiri dari semua pasangan dalam R yang elemen pertamanya berada dalam D. Kita definisikan *restriction* secara formal:

Definisi 20 (Restriction)

$$R \restriction D = \{x | x \in R \text{ dan } fst(x) \in D\}$$

dimana fst adalah fungsi yang memberi elemen pertama dalam pasangan berurut.

Jika F dan K keduanya merupakan *field*, K merupakan *subfield* dari F, dan $A = \{a_1, a_2, \ldots, a_n\} \subseteq F$, maka dengan "menambahkan" (*adjoining*) A pada K (yang diberi notasi $K(A)$) kita dapatkan *field extension* yang merupakan *intersection* dari semua *subfield* F yang mencakup K dan A. $K(A)$ terdiri dari semua elemen F yang dapat ditulis sebagai

$$f(a_1, a_2, \ldots, a_n) \cdot (g(a_1, a_2, \ldots, a_n))^{-1},$$

dimana $f, g \in K[x_1, x_2, \ldots, x_n]$, $a_1, a_2, \ldots, a_n \in A$ dan $g(a_1, a_2, \ldots, a_n) \neq 0$. ($K(A)$ merupakan himpunan semua ekspresi rasional yang melibatkan elemen dari K dan A.) Jika $A = \{a\}$, notasi $K(a)$ sering digunakan untuk $K(\{a\})$, dan *extension* disebut *simple extension*. Kita akan fokus pada *simple extension* karena *extension* dengan beberapa elemen dapat dipandang sebagai runtunan dari beberapa *simple extension*.

Definisi 21 (Algebraic) *Elemen $a \in F$ disebut algebraic atas K jika terdapat polynomial $0 \neq f \in K[x]$ dengan $f(a) = 0$ (a merupakan akar dari polynomial f). Extension dengan elemen algebraic disebut algebraic extension.*

Jika elemen $a \in F$ tidak *algebraic* atas K maka a disebut *transcendental* atas K dan *extension* dengan a disebut *transcendental extension*. Untuk elemen a yang *algebraic*, karena terdapat *polynomial* $0 \neq f \in K[x]$ dengan akar a, maka terdapat *polynomial* dengan *degree* minimal dengan akar a. Lebih dari itu, terdapat *monic polynomial* f dengan akar a yang mempunyai *degree* minimal karena setiap koefisien berasal dari *field* K (jadi dapat dikalikan dengan elemen *inverse* dari K juga untuk menghasilkan 1). Kita ingin tunjukkan bahwa *monic polynomial* dengan *degree* minimal itu unik. Jadi, jika $0 \neq f, g \in K[x]$ keduanya merupakan *monic polynomial* dengan *degree* minimal yang mempunyai akar

a dan $\deg(f) = \deg(g)$), kita ingin tunjukkan bahwa $f = g$. Karena $K[x]$ merupakan *Euclidean domain* (lihat bagian 5.6), maka terdapat $q, r \in K[x]$ dengan

$$f = qg + r \text{ dan } \deg(r) < \deg(g) \text{ atau } r = 0.$$

Kita dapatkan

$$r(a) = f(a) - q(a)g(a) = 0,$$

dan karena f dan g mempunyai *degree* minimal untuk *polynomial* dengan akar a, maka tidak mungkin $\deg(r) < \deg(g)$. Jadi $r = 0$ dan

$$f = qg.$$

Karena f dan g merupakan *monic polynomial* dengan *degree* yang sama, maka $q = 1$ dan $f = g$ seperti yang diharapkan. *Polynomial* seperti diatas disebut *minimal polynomial* dari a atas K dengan notasi $\min_K^a$. Jadi kita baru saja membuktikan teorema berikut:

Teorema 44 *Jika $a \in F$ algebraic atas K, maka terdapat suatu monic polynomial unik dengan degree minimal (polynomial diberi notasi $\min_K^a$) dimana $\min_K^a(a) = 0$.*

Sekarang kita ingin buktikan teorema berikut:

Teorema 45 *Jika $a \in F$ algebraic atas K dan $f \in K[x]$, maka $f(a) = 0$ jika dan hanya jika $\min_K^a$ membagi f dalam struktur ring $K[x]$.*

Jika $\min_K^a$ membagi f dalam $K[x]$ maka terdapat $q \in K[x]$ dimana $f = q \min_K^a$, jadi

$$f(a) = q(a)\min_K^a(a) = q(a) \cdot 0 = 0.$$

Sebaliknya, jika $f(a) = 0$, maka terdapat $q, r \in K[x]$ dimana

$$f = q \min_K^a + r$$

dan

$$\deg(r) < \deg(\min_K^a) \text{ atau } r = 0.$$

Dengan argumentasi yang sama seperti dalam pembuktian teorema 44 kita dapatkan $r = 0$, jadi $f = q \min_K^a$.

Teorema 46 *Jika $a \in F$ algebraic atas K, maka $\min_K^a$ merupakan monic irreducible polynomial unik dalam $K[x]$ dengan akar a.*

Untuk membuktikan teorema ini, kita harus tunjukkan bahwa $\min_K^a$ *irreducible* dan satu-satunya *monic irreducible polynomial* dalam $K[x]$ dengan akar a. Jika $\min_K^a$ dapat diuraikan dalam $K[x]$, misalnya

$$\min_K^a = fg$$

maka

$$\deg(f) < \deg(\min\nolimits_K^a) \text{ dan } \deg(g) < \deg(\min\nolimits_K^a),$$

dan $f(a) = 0$ atau $g(a) = 0$ karena $f(a)g(a) = \min_K^a(a) = 0$. Tetapi ini merupakan kontradiksi, karena $\min_K^a$ minimal (tidak mungkin $f(a) = 0$ atau $g(a) = 0$). Jadi $\min_K^a$ *irreducible*. Untuk menunjukkan bahwa *monic irreducible polynomial* dalam $K[x]$ dengan akar a harus sama dengan $\min_K^a$, teorema 45 mengatakan *polynomial* tersebut harus merupakan kelipatan dari $\min_K^a$, dan karena *irreducible*, maka harus sama dengan $\min_K^a$.

Mari kita lihat apa yang terjadi jika kita lakukan *simple extension* yang bersifat *transcendental* terhadap suatu *field*. Jika K merupakan suatu *field* dan F merupakan *rational function field* atas K (F terdiri dari semua pecahan dengan *numerator* dan *denominator* dari $K[x]$, tentunya dengan pengecualian *denominator* tidak boleh 0), maka F merupakan *field extension* dari K. Karena dalam F, $g = g(x) = 0$ jika dan hanya jika g merupakan *zero polynomial*, maka x *transcendental* atas K. Jika kita lakukan *simple extension* terhadap K menggunakan x, maka kita dapatkan F. Jadi *simple extension* terhadap K menggunakan x yang *transcendental* terhadap K menghasilkan *rational function field* $K(x)$. Karena *rational function field* tidak *finite* (banyaknya *polynomial* adalah *infinite*), maka *field extension* yang bersifat *transcendental* tidak mungkin menghasilkan *finite field*.

Sekarang kita lihat apa yang terjadi jika kita lakukan *simple extension* yang bersifat *algebraic* terhadap suatu *field*. Jika g merupakan *monic irreducible polynomial* dalam $K[x]$, maka teorema 26 (lihat bagian 5.7) mengatakan bahwa $K[x]/gK[x]$ merupakan suatu *field*. Mari kita beri notasi $\overline{f}$ untuk *residue class* $f + gK[x]$. Kita teliti bagian dari *canonical homomorphism*

$$\begin{array}{rcl} \varphi : K[x] & \longrightarrow & K[x]/gK[x] \\ f & \mapsto & \overline{f} \end{array}$$

yang berlaku pada K (yaitu $\varphi \restriction K$). Karena semua elemen dari K merupakan konstan dalam $K[x]$, maka $\varphi(K) = K$, jadi K merupakan *subfield* dari $K[x]/gK[x]$.

Jika $f = \sum_{i=1}^m a_i x^i \in K[x]$, sifat *homomorphism* dari φ menghasilkan

$$\overline{f} = \overline{\sum_{i=1}^m a_i x^i} = \sum_{i=1}^m a_i \overline{x}^i = f(\overline{x}).$$

Jadi $g(\overline{x}) = \overline{g} = 0$, dan $f(\overline{x}) = \overline{f} \neq 0$ jika $\deg(f) < \deg(g)$. Jika kita buat $F = K[x]/gK[x]$, maka $\overline{x} \in F$ bersifat *algebraic* atas K dengan *minimal polynomial* $g \in K[x]$. Lebih dari itu, elemen-elemen dari F mempunyai format $\overline{f} = f(\overline{x})$ dengan $f \in K[x]$ (karena F merupakan *quotient ring* dari $K[x]$). Karena F juga merupakan suatu field, maka *elemen* F yang bukan 0 mempunyai *inverse*

yang juga *elemen* F yang bukan 0. Jadi sebenarnya elemen-elemen dari F meliputi semua ekspresi yang mempunyai format

$$f(\overline{x}) \cdot (h(\overline{x}))^{-1},$$

dimana $f, h \in K[x]$, dan $h(\overline{x}) \neq 0$. (F merupakan himpunan semua ekspresi rasional yang melibatkan elemen dari K dan $\{\overline{x}\}$.) Jadi $K(\overline{x}) = F$.

Kita telah membuktikan teorema berikut mengenai *simple field extension*:

Teorema 47 *Untuk suatu field K:*

1. *Jika F merupakan rational function field atas K dengan variabel x, maka F adalah simple extension dari K dengan elemen transcendental x.*

2. *Jika g merupakan monic irreducible polynomial dalam $K[x]$, maka $F = K[x]/gK[x]$ adalah simple extension dari K dengan elemen algebraic $\overline{x}$ yang mempunyai minimal polynomial g.*

Karena *field extension* menggunakan elemen *transcendental* akan menghasilkan *field* yang tidak *finite*, maka untuk mendapatkan *finite field*, *field extension* harus menggunakan elemen *algebraic* (dan *extension* harus dilakukan pada *finite field*).

Berikut kita ingin tunjukkan bahwa *simple field extension* selalu menghasilkan *extension field* yang unik (*up to isomorphism*[1]). *Isomorphism* antara *field extension* yang sama adalah *isomorphism* yang khusus: jika K' dan K'' keduanya merupakan *field extension* dari K, maka K' disebut *K-isomorphic* dengan K'' jika terdapat *isomorphism*

$$\varphi : K' \longrightarrow K''$$

dengan $\varphi \restriction K = \mathrm{id}_K$. Jadi *isomorphism* diantara kedua *extension field* mempertahankan struktur *base field*.

Teorema 48 *Untuk $a \in K'$ dimana K' merupakan field extension dari K, jika a transcendental atas K maka $K(a)$ K-isomorphic dengan $K(x)$ dimana x dipetakan ke a. Jika a algebraic atas K maka $K(a)$ K-isomorphic dengan $K[x]/\min_K^a K[x]$ dimana $\overline{x} = x + \min_K^a K[x]$ dipetakan ke a.*

Untuk pembuktian teorema 48 kita gunakan *homomorphism*:

$$\begin{array}{rcl} \varphi : K[x] & \longrightarrow & K' \\ f & \mapsto & f(a). \end{array}$$

[1]Dalam aljabar abstrak, unik selalu berarti *up to isomorphism* karena dua struktur yang *isomorphic* dari sudut pandang abstrak dianggap sama.

Jika a *transcendental* atas K maka $\ker(\varphi) = \{0\}$, jadi φ bersifat *injective* dan dapat diperluas menjadi *homomorphism*:

$$\psi : K(x) \quad \longrightarrow \quad K'$$

dengan $\psi \restriction K[x] = \varphi$ dan $\psi(f/g) = \varphi(f) \cdot (\varphi(g))^{-1}$. Tidak terlalu sukar untuk melihat bahwa ψ bersifat *injective* dan $\psi(K(x)) = K(a)$. Jika a *algebraic* atas K maka dengan menggunakan teorema 45 kita dapatkan $\ker(\varphi) = \min_K^a K[x]$. Berdasarkan teorema 40, $K[x]/\min_K^a K[x]$ *isomorphic* dengan $\varphi(K[x])$ menggunakan:

$$\begin{array}{rcl} \psi : K[x]/\min_K^a K[x] & \longrightarrow & \varphi(K[x]) \\ \overline{f} & \mapsto & f(a). \end{array}$$

Jelas bahwa $\psi \restriction K = \mathrm{id}_K$ jadi ψ merupakan suatu K-*isomorphism*. Jadi kita dapatkan $\psi(K[x]/\min_K^a K[x])$ yang merupakan *subfield* dari K' yang mencakup seluruh K dan mempunyai a sebagai elemen, dan setiap elemennya mempunyai bentuk $f(a)$ dimana $f \in K[x]$. Jadi $\psi(K[x]/\min_K^a K[x])$ harus sama dengan $K(a)$. Selesailah pembuktian teorema 48.

Sekarang mari kita tunjukkan bahwa *field extension* dengan elemen *algebraic* dapat dipandang sebagai ruang vektor, dimana *field* semula menjadi *scalar*. Kita beri label K untuk field semula dan label a untuk elemen *algebraic* yang digunakan oleh *field extension*. Jadi terdapat *minimal polynomial* $\min_K^a$ yang kita beri label g dan mempunyai format:

$$g = x^n + b_{n-1}x^{n-1} + \ldots + b_0.$$

Kita ingin tunjukkan bahwa $\{1, a, a^2, \ldots, a^{n-1}\}$ merupakan basis untuk $K(a)$ sebagai ruang vektor atas K. Untuk menunjukkan bahwa pangkat-pangkat a tersebut independen secara linear sangat mudah karena jika ada dependensi linear maka terdapat *polynomial* dengan *degree* kurang dari n yang mempunyai akar a, sesuatu yang kontradiksi dengan minimalitas dari g. Untuk menunjukkan bahwa pangkat-pangkat a tersebut merupakan *spanning set* untuk ruang vektor, kita mengetahui bahwa $K(a)$ terdiri dari semua elemen yang dapat diekspresikan sebagai *polynomial* dengan a menggantikan variabel x. Untuk pemangkatan a dengan $r > n-1$, kita gunakan fakta bahwa $g(a) = 0$. Jadi

$$\begin{array}{rcl} a^{r-n}g(a) & = & 0, \\ a^{r-n}(a^n + b_{n-1}a^{n-1} + \ldots + b_0) & = & 0, \\ a^r & = & -b_{n-1}a^{r-1} - \ldots - b_0a^{r-n}. \end{array}$$

Dengan menggunakan prinsip induksi kita dapatkan bahwa setiap pemangkatan a dengan $r > n-1$ dapat digantikan dengan kombinasi linear pemangkatan a yang merupakan elemen-elemen dari $\{1, a, a^2, \ldots, a^{n-1}\}$. Jadi selesai sudah

pembuktian bahwa $\{1, a, a^2, \ldots, a^{n-1}\}$ merupakan basis untuk $K(a)$ sebagai ruang vektor.

Berikutnya kita akan bahas konsep *algebraic closure*.

Definisi 22 (Algebraically Closed) *Field F disebut algebraically closed jika setiap polynomial f dalam $F[x]$ dengan $deg(f) > 0$ mempunyai akar (solusi x untuk $f(x) = 0$) dalam F.*

Sebagai contoh, berdasarkan *Fundamental Theorem of Algebra*, $\mathbf{C}$ (*field* untuk bilangan kompleks) merupakan *field* yang *algebraically closed*.

Definisi 23 (Algebraic Closure) *Algebraic closure dari suatu field K adalah suatu algebraic field extension F atas K dimana F merupakan field yang algebraically closed.*

Tentunya jika K adalah suatu *field* yang *algebraically closed*, maka *algebraic closure* dari K adalah K. Setiap *field* memiliki *algebraic closure*, akan tetapi kita tidak akan membuktikan itu disini karena pembuktiannya cukup rumit dan memerlukan penggunaan *Axiom of Choice*.

10.7 Finite Field

Konsep *finite field* telah diperkenalkan pada bab-bab sebelum ini, dengan contoh aplikasi *polynomial field* yang digunakan oleh enkripsi AES. Sebenarnya *polynomial field* adalah cara pandang atau implementasi dari *finite field*, dengan kata lain setiap *finite field* dapat diimplementasi sebagai *polynomial field*. Di bagian ini kita akan bahas esensi dari *finite field* terlepas dari implementasi. Kita akan mendalami lebih lanjut teori mengenai *finite field*, termasuk pembahasan konsep *characteristic* dan *generator*.

Untuk suatu *field*, jika kelipatan dari 1 tidak akan dapat menghasilkan 0, maka *characteristic* dari *field* tersebut adalah 0. Jika dapat menghasilkan 0, maka *characteristic* adalah kelipatan terkecil p dari 1 yang menghasilkan 0:

$$\underbrace{1 + 1 + \ldots + 1}_{p} = 0.$$

Characteristic dari suatu *field* harus berupa bilangan prima (kecuali jika *characteristic* $= 0$), karena jika *characteristic* tidak prima dan dapat diuraikan, misalnya $p = mn$ dimana $1 < m, n < p$, maka

$$0 = \underbrace{1 + 1 + \ldots + 1}_{p} = (\underbrace{1 + 1 + \ldots + 1}_{m})(\underbrace{1 + 1 + \ldots + 1}_{n}),$$

yang berarti $\underbrace{1 + 1 + \ldots + 1}_{m} = 0$ atau $\underbrace{1 + 1 + \ldots + 1}_{n} = 0$, sesuatu yang mustahil karena p adalah kelipatan terkecil dari 1 dengan hasil 0. *Characteristic*

dari suatu *finite field* $\mathbf{F}$ harus berupa bilangan prima karena jika 0, maka himpunan dari semua elemen $\mathbf{F}$ harus mencakup $\mathbf{N}$ dan juga $\mathbf{Q}$ ($\mathbf{Q}$ merupakan *subfield* dari $\mathbf{F}$), jadi $\mathbf{F}$ tidak *finite* — suatu kontradiksi. Suatu *finite field* dengan *characteristic* p mempunyai $\mathbf{F}_p$ (atau $\mathbf{GF}(p)$, *Galois field* dengan p elemen) sebagai *subfield*. Sebetulnya lebih tepat jika dikatakan bahwa $\mathbf{F}_p$ *isomorphic* dengan *subfield* yang bersangkutan, tetapi dalam teori *finite field*, dua *field* yang *isomorphic* dianggap sama, hanya implementasinya mungkin berbeda. Mari kita coba buktikan bahwa $\mathbf{F}_p$ *isomorphic* dengan *subfield* dari *field* dengan *characteristic* p. Jadi harus kita tunjukkan bahwa terdapat *injective homomorphism* φ dari $\mathbf{F}_p$ ke $\mathbf{F}$, dimana $\mathbf{F}$ merupakan *field* dengan *characteristic* p. Kita definisikan

$$\begin{aligned} \varphi : \mathbf{F}_p &\longrightarrow \mathbf{F} \\ m &\mapsto m \cdot 1_{\mathbf{F}}. \end{aligned}$$

Definisi diatas merupakan definisi yang baik (*well-defined*) karena jika $m = n$ dalam $\mathbf{F}_p$, maka $p|(m-n)$, yang berarti

$$\begin{aligned} (m-n)1_{\mathbf{F}} &= 0, \\ m \cdot 1_{\mathbf{F}} &= n \cdot 1_{\mathbf{F}}. \end{aligned}$$

Definisi juga menghasilkan φ yang *injective* karena jika $m, n \in \mathbf{F}_p$ keduanya dipetakan ke elemen $\mathbf{F}$ yang sama, maka

$$\begin{aligned} m \cdot 1_{\mathbf{F}} &= n \cdot 1_{\mathbf{F}}, \\ (m-n)1_{\mathbf{F}} &= 0, \end{aligned}$$

jadi karena $p|(m-n)$ dan $m, n \in \mathbf{F}_p$ maka $m = n$, yang berarti φ adalah *injective*. Sekarang tinggal kita tunjukkan bahwa φ merupakan *field homomorphism*. Dari definisi φ kita dapatkan $\varphi(1) = 1_{\mathbf{F}}$ dan $\varphi(0) = 0_{\mathbf{F}}$. Untuk $m + n$ kita dapatkan

$$\begin{aligned} \varphi(m+n) &= (m+n) \cdot 1_{\mathbf{F}} \\ &= m \cdot 1_{\mathbf{F}} + n \cdot 1_{\mathbf{F}} \\ &= \varphi(m) + \varphi(n). \end{aligned}$$

Untuk mn kita dapatkan

$$\begin{aligned} \varphi(mn) &= mn \cdot 1_{\mathbf{F}} \\ &= mn \cdot 1_{\mathbf{F}} \cdot 1_{\mathbf{F}} \\ &= (m \cdot 1_{\mathbf{F}})(n \cdot 1_{\mathbf{F}}) \\ &= \varphi(m)\varphi(n). \end{aligned}$$

Jadi φ merupakan *field homomorphism*.

Untuk suatu *finite field* $\mathbf{F}_q$, terdapat $q-1$ elemen non 0. Kumpulan dari elemen non 0 membentuk suatu *multiplicative group* $\mathbf{F}_q^*$, dan setiap elemen a dalam *group* tersebut mempunyai *order*, yaitu pangkat positif terkecil dari a yang menghasilkan 1. Untuk melihat bahwa suatu elemen non 0 a dalam $\mathbf{F}_q^*$ mempunyai *order* positif, jika semua pangkat a berbeda, maka *field* tidak *finite*, suatu kontradiksi. Jadi terdapat $m > n, a^m = a^n$, atau $a^{m-n} = 1$, yang berarti ada pangkat positif dari a yang menghasilkan 1. Karena pangkat positif merupakan subset dari $\mathbf{N}$, prinsip *well-ordering* mengatakan terdapat pangkat positif terkecil dari a yang menghasilkan 1, pangkat tersebut merupakan *order* dari a dalam $\mathbf{F}_q^*$.

Teorema 49 *Jika a adalah elemen non* 0 *dari finite field* $\mathbf{F}_q$*, order dari a (yang kita beri label d) membagi* $q-1$.

Pertama kita tunjukkan dahulu bahwa $a^{q-1} = 1$. Untuk itu, kita deretkan semua elemen $\mathbf{F}_q^*$ sebanyak $q-1$ elemen:

$$a_1, a_2, \ldots, a_{q-1}$$

dan ambil produknya:

$$p_1 = a_1 a_2 \ldots a_{q-1}.$$

Jika kita kalikan setiap elemen dalam deretan dengan a, maka akan kita dapatkan deretan dengan $q-1$ elemen juga:

$$b_1, b_2, \ldots, b_{q-1}$$

dimana $b_i = a_i a$. Kita ambil produk deretan kedua:

$$p_2 = b_1 b_2 \ldots b_{q-1}.$$

Karena dua elemen $\mathbf{F}_q^*$ yang berbeda jika masing-masing dikalikan dengan a menghasilkan dua elemen $\mathbf{F}_q^*$ yang berbeda juga, maka semua elemen dalam deretan kedua berbeda, jadi deretan kedua terdiri dari semua elemen $\mathbf{F}_q^*$. Perbedaan antara deretan pertama dengan deretan kedua hanya terletak pada urutan elemen. Jadi

$$p_1 = p_2 = p_1 a^{q-1}$$

yang berarti $a^{q-1} = 1$. Kembali ke pembuktian semula yaitu menunjukkan bahwa d membagi $q-1$, jika d tidak membagi $q-1$, maka terdapat $0 < r < d$ dimana

$$q - 1 = bd + r$$

untuk suatu b, dan

$$a^r = a^{q-1-bd} = 1.$$

Ini adalah suatu kontradiksi karena d merupakan pangkat positif a terkecil yang menghasilkan 1. Jadi d membagi $q-1$, dan selesailah pembuktian teorema 49.

Definisi 24 (Generator) *Elemen dari* $\mathbf{F}_q^*$ *yang mempunyai order* $q-1$ *disebut generator dari* $\mathbf{F}_q^*$. *Setiap elemen* $\mathbf{F}_q^*$ *merupakan hasil pemangkatan generator, jadi hasil-hasil pemangkatan generator "mengunjungi" semua elemen* $\mathbf{F}_q^*$.

Teorema 50 *Setiap finite field* $\mathbf{F}_q$ *mempunyai generator untuk multiplicative group* $\mathbf{F}_q^*$. *Jika* g *adalah generator untuk* $\mathbf{F}_q^*$, *maka* g^j *juga merupakan generator untuk* $\mathbf{F}_q^*$ *jika dan hanya jika* $\gcd(j, q-1) = 1$. *Jadi terdapat* $\phi(q-1)$ *generator untuk* $\mathbf{F}_q^*$.

Untuk pembuktian teorema 50, mari kita fokus pada suatu elemen $a \in \mathbf{F}_q^*$ yang mempunyai *order* d (jadi $a^d = 1$ dan tidak ada pemangkatan a dengan sesuatu yang lebih kecil dari d yang menghasilkan 1). Teorema 49 mengatakan bahwa $d|q-1$. Juga, karena a^d merupakan pemangkatan terkecil yang menghasilkan 1, maka $a, a^2, \ldots, a^d$ semua merupakan elemen yang berbeda. Kita ingin tunjukkan bahwa elemen-elemen yang mempunyai *order* d adalah yang bernilai a^j dimana $\gcd(j, d) = 1$, jadi ada $\phi(d)$ elemen yang mempunyai order d. Kita ketahui bahwa setiap pemangkatan a diatas merupakan solusi dari persamaan $x^d = 1$, jadi semua merupakan akar dari $x^d - 1$. Kita juga mengetahui bahwa $x^d - 1$ tidak mempunyai akar ganda karena $x^d - 1$ dan derivatifnya (dx^{d-1}) tidak mempunyai pembagi persekutuan. Alhasil hanya pemangkatan a yang dapat menjadi akar dari $x^d - 1$, jadi elemen dengan *order* d harus merupakan pemangkatan dari a. Namun tidak semua pemangkatan a merupakan elemen dengan *order* d, karena jika $\gcd(j, d) = d' > 1$, maka a^j mempunyai order lebih kecil dari d yaitu d/d'. (d/d' dan j/d' keduanya merupakan bilangan bulat, dan $(a^j)^{(d/d')} = (a^d)^{j/d'} = 1$.) Kita juga harus tunjukkan bahwa jika $\gcd(j, d) = 1$ maka a^j mempunyai *order* d. Untuk itu kita tunjukkan bahwa jika *order* dari a^j lebih kecil dari d, sebut saja d'', maka kita akan dapatkan suatu kontradiksi. Karena d'' merupakan *order* dari a^j maka

$$(a^j)^{d''} = 1 = (a^{d''})^j.$$

Kita juga mengetahui bahwa

$$(a^{d''})^d = 1.$$

Jadi $a^{d''}$ dipangkatkan dengan $\gcd(j, d) = 1$ akan menghasilkan 1, dengan kata lain $a^{d''} = 1$. Tetapi ini merupakan suatu kontradiksi karena tidak ada pemangkatan a dengan sesuatu yang lebih kecil dari d yang dapat menghasilkan 1. Jadi kita sudah buktikan bahwa jika suatu elemen a mempunyai *order* d, maka terdapat $\phi(d)$ elemen dengan *order* d. Sekarang tinggal menunjukkan bahwa untuk setiap $d|q-1$ terdapat elemen dengan *order* d. Kita gunakan teorema 33 yang mengatakan bahwa

$$\sum_{d|q-1} \phi(d) = q - 1.$$

Jika terdapat $d|q-1$ dimana tidak ada elemen dengan *order* d, karena teorema 49 mengatakan *order* dari setiap elemen dari $\mathbf{F}_q^*$ membagi $q-1$, maka jumlah elemen dari $\mathbf{F}_q^*$ akan lebih kecil dari $q-1$, suatu kontradiksi. Jadi kita sudah buktikan bahwa untuk setiap $d|q-1$, terdapat $\phi(d)$ elemen dengan *order* d, jadi terdapat $\phi(q-1)$ elemen dengan *order* $q-1$, dengan kata lain terdapat $\phi(q-1)$ *generator* untuk $\mathbf{F}_q^*$. Selesailah pembuktian teorema 50.

Satu lagi konsep yang perlu dijelaskan sebelum penjelasan hasil terpenting mengenai *finite field* adalah konsep *splitting field*. Untuk suatu *field* K dan *polynomial* non-konstan f dalam $K[x]$, jika f dapat diuraikan menjadi produk dari *polynomial* linear dalam $K[x]$, dengan kata lain

$$f = f_1 f_2 \dots f_n$$

dimana setiap f_i untuk $1 \leq i \leq n$ adalah *poynomial* linear dalam $K[x]$, maka f disebut *splits* dalam K. Untuk suatu *field* F dan *polynomial* f dalam $F[x]$, *field* K adalah *splitting field* untuk f jika K adalah *field extension* terkecil dari F dimana f *splits* dalam K.

Teorema 51 *Untuk suatu field F dan polynomial non-konstan f dalam $F[x]$, terdapat splitting field untuk f yang unik (up to isomorphism).*

Splitting field untuk f unik *up to isomorphism* yang berarti jika K dan K' keduanya merupakan *splitting field* untuk f, maka K *isomorphic* dengan K'. Untuk membuktikan teorema 51, kita gunakan induksi pada *degree* dari f. Jika *degree* dari f adalah 1, maka $f = ax + b$ dimana $a, b \in F$, jadi $K = F(-b/a) = F$ karena $-b/a \in F$. Sekarang kita harus buktikan bahwa jika teorema 51 berlaku untuk *degree* n maka teorema juga berlaku untuk *degree* $n+1$. Jika f mempunyai *degree* $n+1$, maka terdapat faktor *irreducible* f_0 dari f dan teorema 26 mengatakan bahwa $K = F[x]/f_0F[x]$ adalah suatu *field*. Jadi terdapat $\theta_0 \in K$ yang merupakan akar dari f_0, oleh karena itu kita dapat uraikan $f = g \cdot h$ dimana $g = x - \theta_0$. *Degree* dari h adalah n, jadi dengan menggunakan hipotesis induksi terdapat *splitting field* unik L untuk h yang merupakan *field extension* dari K. Karena h dapat diuraikan dalam $L[x]$ sebagai berikut:

$$h = a_{n+1} \prod_{i=1}^{k} (x - \theta_i)^{e_i},$$

maka

$$L = K(\theta_1, \theta_2, \dots, \theta_k)$$

dan f dapat diuraikan sebagai berikut:

$$f = a_{n+1}(x - \theta_0) \prod_{i=1}^{k} (x - \theta_i)^{e_i},$$

jadi $f \in L[x]$. Karena

$$K = F(\theta_0, \theta_{i_1}, \theta_{i_2}, \ldots, \theta_{i_m})$$

dimana $\{\theta_{i_1}, \theta_{i_2}, \ldots, \theta_{i_m}\} \subseteq \{\theta_1, \theta_2, \ldots, \theta_k\}$, maka

$$L = F(\theta_0, \theta_1, \theta_2, \ldots, \theta_k)$$

merupakan *splitting field* untuk f. Karena *field extension* unik (lihat teorema 48) maka *splitting field* juga unik. Selesailah pembuktian teorema 51.

Sekarang kita tiba pada hasil terpenting mengenai *finite field* yaitu teorema mengenai struktur dari *finite field*.

Teorema 52

- *Banyaknya elemen dalam suatu finite field adalah p^n dimana p adalah characteristic dari field berupa suatu bilangan prima dan n adalah bilangan bulat positif.*
- *Untuk setiap bilangan prima p dan bilangan bulat positif n terdapat suatu finite field dengan p^n elemen.*
- *Setiap finite field isomorphic dengan finite field yang mempunyai jumlah elemen yang sama.*

Untuk menunjukkan bahwa banyaknya elemen dalam suatu *finite field* F mempunyai bentuk p^n dimana p adalah bilangan prima dan n adalah bilangan bulat positif, kita mengetahui bahwa *characteristic* dari suatu *finite field* adalah suatu bilangan prima. Jadi p merupakan *characteristic* dari F dan elemen-elemen

$$0, 1, 2, \ldots, p-1$$

dimana $2 = 1+1$, $3 = 1+1+1$ dan seterusnya, membuat suatu *subfield* dari F yang *isomorphic* dengan Z/pZ. F merupakan ruang vektor atas *subfield* diatas dan dimensi dari ruang vektor adalah n. Karena ada p kemungkinan untuk setiap koordinat, maka terdapat p^n elemen secara keseluruhan.

Untuk menunjukkan bahwa terdapat *finite field* dengan p^n elemen untuk setiap bilangan prima p dan bilangan positif n, kita gunakan *polynomial*

$$f = x^q - x$$

dimana $q = p^n$. Kita dapat membuat suatu F yang mempunyai Z/pZ sebagai subfield dan merupakan *splitting field* untuk f atas Z/pZ. Jadi f dapat diuraikan sebagai berikut:

$$f = (x - r_1)(x - r_2)\ldots(x - r_q)$$

dimana $r_i \in F$ untuk $i = 1, 2, \ldots, q$. Setiap akar r_i berbeda ($r_i \neq r_j$ jika $i \neq j$) karena derivatif dari f:

$$qx^{q-1} - 1 \equiv -1 \pmod{p}$$

tidak mempunyai akar yang sama dengan akar dari f. Kita kumpulkan akar-akar tersebut dalam suatu himpunan R:

$$R = \{r_1, r_2, \ldots, r_q\}.$$

Kita ingin tunjukkan bahwa R adalah suatu *field*. 0 dan 1 merupakan elemen dari R karena 0 dan 1 keduanya merupakan akar dari f. Untuk $+$, kita dapatkan:

$$\begin{aligned}(a+b)^q &= a^q + \ldots + b^q \\ &\equiv a + b \pmod{p}\end{aligned}$$

karena semua suku kecuali a^q dan b^q mempunyai koefisien yang dapat dibagi oleh p jadi $\equiv 0 \pmod{p}$ (koefisien binomial $\begin{pmatrix} q \\ i \end{pmatrix}$ dapat dibagi oleh p untuk $0 < i < q$ dan $= 1$ untuk $i = 0$ dan $i = q$). Jadi jika $a, b \in R$, karena $(a+b)$ merupakan akar dari f, maka $(a+b) \in R$. Untuk perkalian kita dapatkan:

$$\begin{aligned}(ab)^q &= a^q b^q \\ &= ab,\end{aligned}$$

jadi jika $a, b \in R$, karena ab merupakan akar dari f, maka $ab \in R$. Untuk *inverse* kita dapatkan:

$$\begin{aligned}(a^{-1})^q &= (a^q)^{-1} \\ &= a^{-1},\end{aligned}$$

jadi jika $a \in R$, karena a^{-1} merupakan akar dari f, maka $a^{-1} \in R$. Jadi R adalah *field* dengan p^n elemen.

Untuk menunjukkan bahwa semua *finite field* dengan jumlah elemen yang sama *isomorphic*, kita umpamakan K_1 dan K_2 keduanya adalah *finite field* dengan p^n elemen. Jadi K_1 dan K_2 keduanya merupakan *field extension* dari Z/pZ dan masing-masing memiliki p^n elemen. Setiap elemen dalam K_1 dan K_2 harus mematuhi persamaan $x^q = x$ dimana $q = p^n$, jadi karena keduanya merupakan *splitting field* dari $x^q - x$ maka K_1 dan K_2 *isomorphic*. Selesailah pembuktian teorema 52.

Teorema 52 menunjukkan bahwa dua *finite field* dengan jumlah elemen yang sama adalah *isomorphic*. Dari segi teori abstrak mengenai *finite field*, dua *finite field* yang *isomorphic* dianggap sama, hanya implementasinya saja yang dapat berbeda. *Finite field* disebut juga *Galois field* (**GF**) atas nama Évariste Galois yang sangat berjasa dalam pengembangan teori *finite field*. Suatu *finite field* dengan p^n elemen diberi notasi $\mathbf{GF}(p^n)$. Notasi $\mathbf{F}_p$ juga digunakan untuk $\mathbf{GF}(p)$ dan $\mathbf{F}_q$ untuk $\mathbf{GF}(q)$ dimana $q = p^n$.

10.8 Ringkasan

Dalam bab ini kita telah kembangkan lebih lanjut matematika yang diperlukan untuk *public key cryptography*, antara lain *Fermat's Little Theorem*, *Chinese Remainder Theorem*, Fungsi Euler, dan teori mengenai *finite field* (setelah terlebih dahulu menjelaskan *group of units*, *homomorphism theorem* dan *field extension*).

Fermat's Little Theorem merupakan dasar dari banyak konsep dalam *public key cryptography*. Fungsi Euler memungkinkan *Fermat's Little Theorem* digeneralisasi untuk modulus non-prima, dengan menggunakan *Chinese Remainder Theorem* untuk menjelaskannya. *Chinese Remainder Theorem* juga akan digunakan dalam test bilangan prima. Teori mengenai *finite field* tentunya sangat penting karena *public key cryptography* mengandalkan struktur aljabar *finite field*.