2022 年度全学共通科目「現代の数学と数理解析」　山下担当回レポート問題の講評と解説

講評：
テーマについて: 近年 Dasgupta と Kakde により Hilbert 第 12 問題について大きな進展があったので, (彼らの仕事の解説ではなく入門的内容であるが) 類体論を本講義のテーマに選んだ.

講義について: 類体論の正確な定式化を説明するのではなく, 類体論的現象について多く具体例を挙げて説明した. 非可換類体論のごく簡単な例も挙げる時間があった.

レポートについて: ヒントを多く出し解答しやすいようにした.

レポート提出 23 名 (1 回生 6 名, 2 回生 15 名, 3 回生 0 名, 4 回生以上 2 名). レポート提出者数は例年より少な目.
配点 : 1 : 1 と 2 が各 3 点, 3 が各 4 点, 2 : 5 点, 3 : 5 点, 4 : 各 5 点, 5 : 各 5 点, 6 : 各 5 点, 7 : 各 5 点, 8 : 各 5 点, 9 : 5 点, の 100 点満点.

評価 : 5(優+) : 81〜100 点, 4(優) : 61〜80 点, 3(良+) : 41〜60 点,
2(良) : 21〜40 点, 1(可) : 1〜20 点, 0(不可) : 0 点.
集計 : 5(優+) : 1 名, 4(優) : 4 名, 3(良+) : 5 名, 2(良) : 7 名, 1(可) : 5 名, 0(不可) : 1 名.

1 : 計算間違いや該当素数の漏れがある人が意外といた.
2 : 意外と出来ていなかった.
3 : 概ねよく出来ていた.
4, 5 : 豊富にヒントを出したためかそこそこ出来ていた.
6 : ((1) も (2) も)N が素数か合成数かという必要のない議論をしている人がそこそこいた.
7 : 解答者はいなかった.
8 : 難しくない問題にも関わらず解答者は少なかった. 一見難しそうと思ってしまうからだろうか. 深い内容を含む事柄を簡単な問題で出して奥深さを感じ取って欲しいことからこの問題を出題したが, 難しいと錯覚して敬遠されてしまったのなら残念だ.
9 : 興味深く読ませてもらった.
10 : 以前 (コロナ以前) は講義へのコメントはほぼすべての人が書いていたのだが, 今回は書いている人が少なかった.

(次ページに続く)

1 (1). $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$, $37 = 6^2 + 1^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$, $61 = 6^2 + 5^2$, $73 = 8^2 + 2^2$, $89 = 8^2 + 5^2$, $97 = 9^2 + 4^2$.

(2). $3 = 1^2 + 2 \cdot 1^2$, $11 = 3^2 + 2 \cdot 1^2$, $17 = 4^2 + 2 \cdot 1^2$, $19 = 1^2 + 2 \cdot 3^2$, $41 = 3^2 + 2 \cdot 4^2$, $43 = 5^2 + 2 \cdot 3^2$, $59 = 3^2 + 2 \cdot 5^2$, $67 = 7^2 + 2 \cdot 3^2$, $73 = 1^2 + 2 \cdot 6^2$, $83 = 9^2 + 2 \cdot 1^2$, $89 = 9^2 + 2 \cdot 2^2$, $97 = 5^2 + 2 \cdot 6^2$.

(3). $7 = 3^2 - 2 \cdot 1^2$, $17 = 5^2 - 2 \cdot 2^2$, $23 = 5^2 - 2 \cdot 1^2$, $31 = 7^2 - 2 \cdot 3^2$, $41 = 7^2 - 2 \cdot 2^2$, $47 = 7^2 - 2 \cdot 1^2$, $71 = 11^2 - 2 \cdot 5^2$, $73 = 9^2 - 2 \cdot 2^2$, $79 = 9^2 - 2 \cdot 1^2$, $89 = 11^2 - 2 \cdot 4^2$, $97 = 13^2 - 2 \cdot 6^2$.

2 $0 < a < p$ とする. a と p は互いに素なので Euclid の互除法により $na + mp = 1$ となる整数 n, m が存在する. この時, $na \equiv 1 \pmod{p}$ である (存在). もし他にも $n'a \equiv 1 \pmod{p}$ となる n' が存在した時, $n' \equiv n'(na) \equiv n(n'a) \equiv n \pmod{p}$) より, n と n' は p で割った余りが一致する (一意性). n を p で割った余りが $\mathbb{F}_p$ での a の逆数になる. a による割り算はその a の逆数を掛けることで得られる.

3 $0 < i < p$ に対して $\binom{p}{i} \equiv 0 \pmod{p}$ なので自然数 m, n に対して $(m+n)^p = \sum_{0 \le i \le p} \binom{p}{i} m^i n^{p-i} \equiv m^p + n^p \pmod{p}$. よって $a^p = (1 + 1 + \cdots (a \text{ 個}) \cdots + 1)^p \equiv 1 + 1 + \cdots (a \text{ 個}) \cdots + 1 = a \pmod{p}$. $\mathbb{F}_p$ 内で $a \neq 0$ なので, 2 より, a で割ると $a^{p-1} \equiv 1 \pmod{p}$.

4 (1). n の約数 d をとる. d と互いに素な 1 以上 d 以下の自然数 m (そのような m は定義より $\varphi(d)$ 個ある) に対して $a = (n/d)m$ は n との最大公約数が n/d である 1 以上 n 以下の自然数である. 逆に, 1 以上 n 以下の自然数 a に対して $d := n/(a, n)$ とすると, $m := a/(a, n)$ は 1 以上 d 以下の自然数で d と互いに素である. この対応により $n = \sum_{d|n} \varphi(d)$ が示された.

(2). $a \in \mathbb{F}_p^\times$ の位数を n, $p - 1 = mn + r$, $0 \le r < n$ とする. 3 より $a^{p-1} = 1$ であるが, 一方 $a^{p-1} = (a^n)^m a^r = a^r$. 条件 $0 \le r < n$ と位数の定義より $r = 0$. よって n は $p - 1$ の約数.

(3). $\mathbb{F}_p^\times$ の中で位数 d の元のなす集合を $H(d)$ と書く. 位数 d の元 $x \in \mathbb{F}_p^\times$ が存在するとして $f(d) = \varphi(d)$ を示す. $H(d)$ のどの元 a も $a^d = 1$ を満たす. $\mathbb{F}_p$ は 2 で示したように足し算引き算掛け算 0 以外による割り算ができるので, $\mathbb{F}_p$ 係数の多項式に対して因数 $X - \alpha$ (α は根) で割っていくというアルゴリズムが実数係数の時と同様に実行できることに注意すると, $a^d = 1$ を満たす $a \in \mathbb{F}_p^\times$ の個数は高々 d 個. 一方, x が生成する部分集合 $A := \{x, x^2, \ldots, x^d\}$(部分群になる) のどの元 a も $a^d = 1$ を満たす. x の位数は d のため $\#A = d$ であるので, A は $a^d = 1$ をみたす元全体である. 特に $H(d) \subset A$ と分かる. 従って A の中で位数 d のなす元の個数が $f(d)$ である. A の元 x^i $(1 \le i \le d)$ に対して, i と d の最大公約数を k とする. x^i の位数は d/k であることを示す. $(x^i)^{d/k} = (x^d)^{i/k} = 1$. 一方, $1 \le j < d/k$ に対して ij が d で割り切れると仮定する. $ij = ld$ と置く. k は i と d の最大公約数なので i/k と d/k は互いに素. よって, $(i/k)j = l(d/k)$ より j は d/k で割り切れることになるがこれは $1 \le j < d/k$ に矛盾する. 従って ij は d で割り切れないのでその余りを $1 \le r < d$ とすると x の位数は d なので $(x^i)^j = x^{ij} = x^r \neq 1$. このことから x^i の位数は d/k と示された. 特に, A の中で位数 d の元全体は d と互いに素な i に対する x^i たちである. これの個数は $\varphi(d)$ である. よって $f(d) = \varphi(d)$ が示された.

(4). (1) より $\sum_{d|p-1} \varphi(d) = p - 1$, (2) より $\sum_{d|p-1} f(d) = p - 1$ である. (3) より $f(d) = 0, \varphi(d)$

であるが, $\sum_{d|p-1} f(d) = \sum_{d|p-1} \varphi(d)$ より任意の $d \mid p-1$ に対して $f(d) = \varphi(d)$ を分かる. 特に $f(p-1) = \varphi(p-1) \neq 0$ より位数 $p-1$ の元, つまり生成元が存在することが示された.

5 (1). $x^2, y^2 \equiv 0, 1 \pmod 4$ より $p = x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. p は素数なので $p = 2$ か $p \equiv 1 \pmod 4$ である.

(2). $a^2 = -1$ となる $a \in \mathbb{F}_p^\times$ が存在することは $\mathbb{F}_p^\times$ に位数 4 の元が存在することと同値. 4 の (3) の証明中に $\mathbb{F}_p^\times$ の生成元 x に対して x^i の位数は $(p-1)/(i, p-1)$ であることを示したのを思い出すと, これは $4(i, p-1) = p-1$ となる $1 \leq i \leq p-1$ が存在することと同値. このような i が存在すればこの等号から $p \equiv 1 \pmod 4$ である. 逆に $p \equiv 1 \pmod 4$ であれば $i = (p-1)/4$ とすれば $4(i, p-1) = p-1$ を満たすので主張が証明された.

(3). $0 \leq x_1, y_1 < \sqrt{p}$ となる x_1, y_1 の個数は $(\lfloor \sqrt{p} \rfloor + 1)^2$ である. $(\lfloor \sqrt{p} \rfloor + 1)^2 > ((\sqrt{p} - 1) + 1) = p$ なので鳩ノ巣原理より, $0 \leq x_1, y_1, x_2, y_2 < \sqrt{p}$, $\overline{x_1} - a\overline{y_1} = \overline{x_2} - a\overline{y_2}$, となる組 $(x_1, y_1) \neq (x_2, y_2)$ が存在する.

(4). $(\overline{x_1} - \overline{x_2})^2 = a^2(\overline{y_1} - \overline{y_2})^2 = -(\overline{y_1} - \overline{y_2})^2$ より, $x := |x_1 - x_2|$, $y := |y_1 - y_2|$ とすると $\overline{x}^2 + \overline{y}^2 = 0$. よって $x^2 + y^2$ は p で割り切れる. $0 \leq x, y < \sqrt{p}$, $(x, y) \neq (0, 0)$ より $0 < x^2 + y^2 < 2p$. よって $x^2 + y^2 = p$.

6 (1). $p \equiv 3 \pmod 4$ となる素数が $p_1, \ldots, p_n$ と有限個と仮定する. $N := 4p_1 \cdots p_n - 1$ とする. N を割る素数 q を取る. N は $p_1, \ldots, p_n$ では割り切れず N は奇数なので, q は $q \equiv 1 \pmod 4$ となる素数である. N を割る任意の素数が $\equiv 1 \pmod 4$ であるので N も $\equiv 1 \pmod 4$ である. けれども $N = 4p_1 \cdots p_n - 1 \equiv 3 \pmod 4$ より矛盾.

(2). $p \equiv 1 \pmod 4$ となる素数が $p_1, \ldots, p_n$ と有限個と仮定する. $N := (2p_1 \cdots p_n)^2 + 1$ とする. N を割る素数 q を取る. N は $p_1, \ldots, p_n$ では割り切れず N は奇数なので, q は $q \equiv 3 \pmod 4$ となる素数である. また, $(2p_1 \cdots p_n)^2 = N - 1 \equiv -1 \pmod q$ である. 5 の (2) より $q \equiv 1 \pmod 4$ であるが, これは $q \equiv 3 \pmod 4$ に矛盾.

7 (1). $\mathbb{Q}(\sqrt{-5})$ のイデアル類群は $\mathbb{Z}/2\mathbb{Z}$ であり, **全てのイデアルが単項であるとは限らないことから合同 (による) 判定条件にズレが生じる**. $\mathbb{Q}(\sqrt{-5})$ の素イデアルが単項であるための必要十分条件は $\mathbb{Q}(\sqrt{-5})$ の **Hilbert 類体** $H_1 := \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ で (完全) 分解することである. $\mathbb{Q}(\sqrt{-5})$ で $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解する (p) (つまり $p \equiv 1, 3, 7, 9 \pmod{20}$) に対して

$$\mathfrak{p} \text{ が } H_1 \text{ で分解する } \Leftrightarrow (p) \text{ が } \mathbb{Q}(\sqrt{-1}) \text{ で分解する } \Leftrightarrow p \equiv 1 \pmod 4$$

と $p \equiv 1, 3, 7, 9 \pmod{20}$ かつ $p \equiv 1 \pmod 4$ $\Leftrightarrow$ $p \equiv 1, 9 \pmod{20}$ から

$$\text{素数 } p \neq 5 \text{ が } p = x^2 + 5y^2 \ (x, y \in \mathbb{Z}) \text{ と書ける } \Leftrightarrow p \equiv 1, 9 \pmod{20}$$

と分かる. あるいは,

$$\mathfrak{p} \text{ が } H_1 \text{ で分解する } \Leftrightarrow (p) \text{ が } \mathbb{Q}(\sqrt{5}) \text{ で分解する } \Leftrightarrow p \equiv 1, 4 \pmod 5$$

と $p \equiv 1, 3, 7, 9 \pmod{20}$ かつ $p \equiv 1, 4 \pmod 5$ $\Leftrightarrow$ $p \equiv 1, 9 \pmod{20}$ でもよい.
円分体を用いた別証明: $\zeta := e^{2\pi i/20}$ とする. $\zeta^5 = \sqrt{-1}$, $\frac{-1+\sqrt{5}}{4} = \cos\frac{2\pi}{5} = \frac{\zeta^4 + \zeta^{-4}}{2}$ (正五角形を

思出せ) より, $H_1 = \mathbb{Q}(\sqrt{-1}, \sqrt{5}) = \mathbb{Q}(\zeta^5, \zeta^4 + \zeta^{-4})$ は円分体 $\mathbb{Q}(\zeta)$ の部分体である. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(20) = 8$, $[H_1 : \mathbb{Q}] = [H_1 : \mathbb{Q}(\sqrt{-5})][\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 4$ なので $[\mathbb{Q}(\zeta) : H_1] = 2$ である. 一方, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/20\mathbb{Z})^\times$ の元 $\overline{9} : \zeta \mapsto \zeta^9$ に対して

$$\overline{9} : \zeta^5 \mapsto (\zeta^9)^5 = \zeta^{45} = \zeta^5, \quad \zeta^4 + \zeta^{-4} \mapsto (\zeta^9)^4 + (\zeta^9)^{-4} = \zeta^{36} + \zeta^{-36} = \zeta^{-4} + \zeta^4$$

より, H_1 は $\overline{9}$ で固定されるため, 上の同一視のもとで $\mathrm{Gal}(\mathbb{Q}(\zeta)/H_1) = \{\overline{1}, \overline{9}\}$ と分かった. 従って, (p) が H_1 で完全分解 $\Leftrightarrow p \equiv 1, 9 \pmod{20}$ と分かった.
Gauss の種の理論を用いた別証明: $\mathbb{Q}(\sqrt{-5})$ のイデアル類群を Cl と置く. $\mathbb{Q}(\sqrt{-5})$ の判別式 -20 は $(-4)\cdot 5$ と 2 つの基本判別式の積で書けるので $\mathbb{Q}(\sqrt{-5})$ の種の数は $2^{2-1} = 2$. 種の指標は 2 つあり, そのうち 1 つは自明指標であるので, $\mathbb{Q}(\sqrt{-5})$ で $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解する (p) (つまり $p \equiv 1, 3, 7, 9 \pmod{20}$) に対して

$$\begin{aligned}\mathfrak{p} \text{ が } H_1 \text{ で分解} &\Leftrightarrow \mathfrak{p} \text{ が } \mathrm{Cl} \text{ で自明} \Leftrightarrow \mathfrak{p} \text{ が } \mathrm{Cl}/2\mathrm{Cl} \text{ で自明} \\ &\Leftrightarrow \mathfrak{p} \text{ が全ての種の指標で自明} \Leftrightarrow \mathfrak{p} \text{ が唯一の非自明な種の指標で自明.}\end{aligned}$$

χ を分解 $-20 = (-4)\cdot 5$ に対応する種の指標, χ_{-4} を $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ の指標 (あるいは χ_5 を $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ の指標) とすると, $\chi(\mathfrak{p}) = \chi_{-4}(N\mathfrak{p}) = \chi_{-4}(p) = (\frac{-1}{p})$ より, $\chi(\mathfrak{p}) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$ (あるいは $\chi(\mathfrak{p}) = \chi_5(N\mathfrak{p}) = \chi_5(p) = (\frac{5}{p}) = (\frac{p}{5})$ より, $\chi(\mathfrak{p}) = 1 \Leftrightarrow p \equiv 1, 4 \pmod{5}$) なので, (p) が H_1 で完全分解 $\Leftrightarrow p \equiv 1, 9 \pmod{20}$ が分かった.

(2). $\mathbb{Q}(\sqrt{3})$ の (広義) イデアル類群は自明なので $\mathbb{Q}(\sqrt{3})$ で $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解する素数 p に対して $(p) = (x + \sqrt{3}y)(x - \sqrt{3}y) = (x^2 - 3y^2)$ となる $x, y \in \mathbb{Z}$ が存在するが, ここで $-p = x^2 - 3y^2$ となることがある. 一般に実 2 体の基本単数 ϵ のノルム $N\epsilon$ が -1 であれば $(\epsilon(x + \sqrt{3}y))(\epsilon'(x - \sqrt{3}y)) = (N\epsilon)(x^2 - 3y^2) = -(x^2 - 3y^2)$ (ϵ' は ϵ の $\mathbb{Q}$ 上の共役) と, ϵ 倍することでノルムの符号を変えることが出来るが, 基本単数のノルムが $+1$ の時, すべての単数のノルムが $+1$ となり単数倍を掛けることでノルムの符号を変えることが出来ない. いま $\mathbb{Q}(\sqrt{3})$ の基本単数 $2 + \sqrt{3}$ のノルムは $2^2 - 3 = +1$ である. 基本単数のノルムが $+1$ の時, 狭義イデアル類群は (広義) イデアル類群と (2 倍) ズレる. $\mathbb{Q}(\sqrt{3})$ の場合, 狭義イデアル類群は $\mathbb{Z}/2\mathbb{Z}$ となり**全てのイデアルが総正な元で生成されるとは限らないことから合同 (による) 判定条件にズレが生じる**. $\mathbb{Q}(\sqrt{3})$ の素イデアルが総正な元で単項生成されるための必要十分条件は $\mathbb{Q}(\sqrt{3})$ の**狭義 Hilbert 類体** $H_2 := \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ で (完全) 分解することである. $\mathbb{Q}(\sqrt{3})$ で $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解する (p) (つまり $p \equiv 1, 11 \pmod{12}$) に対して

$$\mathfrak{p} \text{ が } H_2 \text{ で分解する} \Leftrightarrow (p) \text{ が } \mathbb{Q}(\sqrt{-1}) \text{ で分解する} \Leftrightarrow p \equiv 1 \pmod{4}$$

と $p \equiv 1, 11 \pmod{12}$ かつ $p \equiv 1 \pmod{4} \Leftrightarrow p \equiv 1 \pmod{12}$ から

$$\text{素数 } p \text{ が } p = x^2 - 3y^2 \ (x, y \in \mathbb{Z}) \text{ と書ける} \Leftrightarrow p \equiv 1 \pmod{12}$$

と分かる. あるいは,

$$\mathfrak{p} \text{ が } H_2 \text{ で分解する} \Leftrightarrow (p) \text{ が } \mathbb{Q}(\sqrt{-3}) \text{ で分解する} \Leftrightarrow p \equiv 1 \pmod{3}$$

と $p \equiv 1, 11 \pmod{12}$ かつ $p \equiv 1 \pmod{3} \Leftrightarrow p \equiv 1 \pmod{12}$ でもよい.
円分体を用いた別証明: $\zeta' := e^{2\pi i/12}$ とする. $\zeta'^3 = \sqrt{-1}$, $\frac{\sqrt{3}}{2} = \sin\frac{2\pi}{3} = \frac{\zeta'^4 - \zeta'^{-4}}{2\sqrt{-1}}$ より, $H_2 = \mathbb{Q}(\sqrt{-1}, \sqrt{3}) = \mathbb{Q}(\zeta'^5, \zeta'^4 - \zeta'^{-4})$ は円分体 $\mathbb{Q}(\zeta')$ の部分体である. $[\mathbb{Q}(\zeta') : \mathbb{Q}] = \varphi(12) = 4$, $[H_2 :$

$[H_2:\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=4$ なので $\mathbb{Q}(\zeta')=H_2$ である. よって, $\mathrm{Gal}(\mathbb{Q}(\zeta')/\mathbb{Q})\cong(\mathbb{Z}/12\mathbb{Z})^\times$ の同一視のもとで $\mathrm{Gal}(\mathbb{Q}(\zeta')/H_2)=\{\overline{1}\}$ と分かった. 従って, (p) が H_2 で完全分解 $\Leftrightarrow$ $p\equiv 1\,(\mathrm{mod}\,12)$ と分かった.

Gauss の種の理論を用いた別証明: $\mathbb{Q}(\sqrt{3})$ の狭義イデアル類群を Cl^* と置く. $\mathbb{Q}(\sqrt{3})$ の判別式 12 は $(-4)\cdot(-3)$ と 2 つの基本判別式の積で書けるので $\mathbb{Q}(\sqrt{3})$ の種の数は $2^{2-1}=2$. 種の指標は 2 つあり, そのうち 1 つは自明指標であるので, $\mathbb{Q}(\sqrt{3})$ で $(p)=\mathfrak{p}\overline{\mathfrak{p}}$ と分解する (p) (つまり $p\equiv 1,11\,(\mathrm{mod}\,12)$) に対して

$$\mathfrak{p}\text{ が }H_2\text{ で分解}\Leftrightarrow\mathfrak{p}\text{ が }\mathrm{Cl}^*\text{ で自明}\Leftrightarrow\mathfrak{p}\text{ が }\mathrm{Cl}^*/2\mathrm{Cl}^*\text{ で自明}$$
$$\Leftrightarrow\mathfrak{p}\text{ が全ての種の指標で自明}\Leftrightarrow\mathfrak{p}\text{ が唯一の非自明な種の指標で自明.}$$

χ を分解 $12=(-4)\cdot(-3)$ に対応する種の指標, χ_{-4} を $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ の指標 (あるいは χ_{-3} を $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ の指標) とすると, $\chi(\mathfrak{p})=\chi_{-4}(N\mathfrak{p})=\chi_{-4}(p)=(\frac{-1}{p})$ より, $\chi(\mathfrak{p})=1\Leftrightarrow p\equiv 1\,(\mathrm{mod}\,4)$ (あるいは $\chi(\mathfrak{p})=\chi_{-3}(N\mathfrak{p})=\chi_{-3}(p)=(\frac{-3}{p})=(\frac{p}{3})$ より, $\chi(\mathfrak{p})=1\Leftrightarrow p\equiv 1\,(\mathrm{mod}\,3)$) なので, (p) が H_2 で完全分解 $\Leftrightarrow$ $p\equiv 1\,(\mathrm{mod}\,12)$ が分かった.

8 (1). (a). $f=q\prod_{n\geq 1}(1-q^n)(1-q^{23n})$ の q^2 及び q^3 の項は $q\cdot(-q^1)=q^2$ 及び $q\cdot(-q^2)=-q^3$ なので $a_2=a_3=-1$.
(b). (2) は $\mathbb{Q}(\sqrt{-23})$ において $(2)=(2,\frac{3+\sqrt{-23}}{2})(2,\frac{3-\sqrt{-23}}{2})$ と分解する. (3) は $\mathbb{Q}(\sqrt{-23})$ において $(3)=(3,2+\sqrt{-23})(3,2-\sqrt{-23})$ と分解する. しかし, $2=x^2+23y^2$ 及び $3=x^2+23y^2$ $(x,y\in\mathbb{Z})$ とは書けない ($y=0$ だと $2=x^2$, $3=x^2$ となる $x\in\mathbb{Z}$ は存在せず, $y\geq 1, y\leq -1$ だと $x^2+23y^2\geq 23$) ので, $\mathfrak{p}=(2,\frac{3+\sqrt{-23}}{2})$ あるいは $\mathfrak{p}=(3,2+\sqrt{-23})$ は H で分解しない.

(2). (a). f の q^5 及び q^7 の項は $q\cdot(-q^4+q^{1+3})=0$, $q\cdot(-q^6+q^{1+5}+q^{2+4}-q^{1+2+3})=0$ なので $a_5=a_7=0$.
(b). $\beta:=\frac{1+\sqrt{-23}}{2}$ は $\beta^2-\beta+6=0$ を満たす. (5) が $\mathbb{Q}(\sqrt{-23})$ で $(5)=\mathfrak{p}\overline{\mathfrak{p}}$ と分解したとすると, $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]/\mathfrak{p}\cong\mathbb{F}_5$ で $\overline{\beta}^2-\overline{\beta}+6=\overline{\beta}^2-\overline{\beta}+1=0$ を満たす ($\mathbb{F}_5$ 内での等号. $\overline{\beta}$ は β の $\mathbb{F}_5$ での像). けれども, x^2-x+1 に $x=0,1,2,-2,-1$ を入れても $0-0+1=1\neq 0$, $1-1+1=1\neq 0$, $4-2+1=3\neq 0$, $4+2+1=2\neq 0$, $1+1+1=3\neq 0$ ($\mathbb{F}_5$ 内での等号) とどれも根にはならない. これは矛盾. (7) が $\mathbb{Q}(\sqrt{-23})$ で $(7)=\mathfrak{p}\overline{\mathfrak{p}}$ と分解したとすると, $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]/\mathfrak{p}\cong\mathbb{F}_7$ で $\overline{\beta}^2-\overline{\beta}+6=\overline{\beta}^2-\overline{\beta}-1=0$ を満たす ($\mathbb{F}_7$ 内での等号. $\overline{\beta}$ は β の $\mathbb{F}_7$ での像). けれども, x^2-x-1 に $x=0,1,2,3,-3,-2,-1$ を入れても $0-0-1=-1\neq 0$, $1-1-1=-1\neq 0$, $4-2-1=1\neq 0$, $9-3-1=5\neq 0$, $9+3-1=4\neq 0$, $4+2-1=5\neq 0$, $1+1-1=1\neq 0$ ($\mathbb{F}_7$ 内での等号) とどれも根にはならない. これは矛盾.

(3). (a). **Euler の五角数定理**を用いる.

n	1	2	3	4	5	6	7	8	9
$\frac{n(3n-1)}{2}$	1	5	12	22	35	51	70	92	117
$\frac{n(3n+1)}{2}$	2	7	15	26	40	57	77	100	126

上の表より, $58\,(=59-1)$ は $\frac{n(3n-1)}{2}$ や $\frac{n(3n+1)}{2}$ の形には書けない. 一方, $35\,(=59-1-23)$ は $n=5$ の時 $\frac{n(3n-1)}{2}=35$ と書ける. また, $12\,(=59-1-2\cdot 23)$ も $n=3$ の時 $\frac{n(3n-1)}{2}=12$ と書ける. 従って, f の q^{59} の項は $q\cdot(0+(-q^{35})(-q^{23})+(-q^{12})(-q^{2\cdot 23}))=2q^{59}$ なので $a_{59}=2$. $100\,(=101-1)$ は $n=8$ の時 $\frac{n(3n+1)}{2}=100$ と書け, $77\,(=101-1-23)$ は $n=7$ の時 $\frac{n(3n+1)}{2}=77$ と書ける. 一方, 上の表より $54\,(=101-1-2\cdot 23)$ と $31\,(=101-1-3\cdot 23)$ と $8\,(=101-1-4\cdot 23)$ は $\frac{n(3n-1)}{2}$ や $\frac{n(3n+1)}{2}$

の形には書けない. 従って, f の q^{101} の項は $q\cdot((+q^{100})+(-q^{77})(-q^{23})+0+0+0)=2q^{101}$ なので $a_{101}=2$.

(b). $59=6^2+23\cdot 1^2$ 及び $101=3^2+23\cdot 2^2$ より, $(59)=(6+\sqrt{-23})(6-\sqrt{-23})$, $(101)=(3+2\sqrt{-23})(3-2\sqrt{-23})$ と $\mathbb{Q}(\sqrt{-23})$ と分解し (単項イデアルである) $(6+\sqrt{-23})$, $(3+2\sqrt{-23})$ も H で完全分解する.