Algebra I: Final 2003

June 19, 2003

解答用紙のすべてに ID と名前を書いて下さい。

1. H を群 G の空でない部分集合とする。このとき、次を示せ。

$$H^{-1}H \subset H \Rightarrow (HH \subset H) \wedge (H^{-1} \subset H)$$

2. H を群 G の部分群とする。このとき、次を示せ。

$$xH = yH \Leftrightarrow x^{-1}y \in H$$

3. $f : G \longrightarrow G'$ を、群 G から群 G' への準同型写像とする。また、
   $K = Kerf = \{x \in G \mid f(x) = 1\}$ とする。

   (a) $H \leq G$ とする。このとき、$f^{-1}(f(H)) = HK \leq G$ であることを証明せよ。

   (b) $HK/K \simeq f(H) \simeq H/(H \cap K)$ であることを証明せよ。

4. p を素数とし、H を群 G の正規部分群で、位数 $|H|$ が p であるとする。

   (a) $a \in H$ が G の単位元でなければ、$H =< a >$ であることを示せ。

   (b) $H^* = H \setminus \{1\}$ すなわち H の単位元以外の元全体からなる集合を表すとする。

$$f : H^* \times G \longrightarrow H^* \ ((a, x) \mapsto x^{-1}ax)$$

   とする。f は G の H^* 上の作用を定義することを示せ。

   (c) $x \in G$ とする。このとき、$i \in \{1, 2, \ldots, p-1\}$ で、どの元 $a \in H^*$ に対しても、$f(a, x) = a^i$ となるものが存在することを証明せよ。(Hint: (a) 参照。)

   (d) $x \in G$ とする。x の位数 $o(x) = | < x > |$ が $p-1$ と互いに素であれば $x \in C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$。すなわち、$x$ は H のすべての元と交換可能であることを示せ。(Hint: 前問の様に i を選んだ時、$f(a, x^2), f(a, x^3), \ldots$ がどうなるか考えよ。)

5. $G = \boldsymbol{Z}_{15}^*$ とする。$\boldsymbol{Z}_{15} = \{\bar{0}, \bar{1}, \ldots, \overline{14}\}$ は、演算 $\cdot$ を $\bar{i} \cdot \bar{j} = \overline{i \cdot j \text{ を } 15 \text{ で割った余り}}$ で定義すると、$(\boldsymbol{Z}_{15}, \cdot)$ はモノイドになるが、その正則元（逆元をもつもの）全体を $\boldsymbol{Z}_{15}^*$ と書く。これは群となる。

   (a) $a \in G$ とすると、$a^4 = 1$ であることを示せ。ただし 1 は G の単位元とする。

   (b) G と同型な群で、巡回群の直積となっているものを一つ上げよ。

   (c) n を 3 でも 5 でも割れない自然数とする。このとき、$n^4 - 1$ は 15 で割り切れることを示せ。

Message をお願いします: 「ホームページ掲載不可」の場合は明記のこと
(1) この授業または群論について。特に授業の改善点について。
(2) ICU の教育一般について。特に改善点について。

Solutions to Final 2003

June 26, 2003

1. H を群 G の空でない部分集合とする。このとき、次を示せ。

$$H^{-1}H \subset H \Rightarrow (HH \subset H) \wedge (H^{-1} \subset H)$$

H は空ではないから、$a \in H$ をとることができる。$1 = a^{-1}a \in H^{-1}H \subset H$ だから $1 \in H$ である。ここで、$x \in H$ とすると、$x^{-1} = x^{-1}1 \in H^{-1}H \subset H$ だから $x^{-1} \in H$ である。x は H の任意の元だったから $H^{-1} \subset H$ が言えた。さらに、$y \in H$ とすると、$xy = (x^{-1})^{-1}y \in H^{-1}H \subset H$ だから $xy \in H$ であり、x, y は H の任意の元だったから $HH \subset H$ である。最初 $H \neq \emptyset$ を用いる部分も論理的には重要です。

2. H を群 G の部分群とする。このとき、次を示せ。

$$xH = yH \Leftrightarrow x^{-1}y \in H$$

$xH = yH \Leftrightarrow H = x^{-1}yH$ は明らか。H は G の部分群だから $1 \in H$。従って、$x^{-1}y = x^{-1}y1 \in x^{-1}yH = H$ となり、$x^{-1}y \in H$ を得る。逆に、$x^{-1}y \in H$ とすると、$x^{-1}yH \subset HH \subset H \subset x^{-1}y(x^{-1}y)^{-1}H \subset x^{-1}yHH \subset x^{-1}yH$。これより、$x^{-1}yH = H$ を得る。$aH = H \Leftrightarrow a \in H$ を利用していた人もたくさんいました。良いことにしましたが、やはり使わずに証明して欲しかったですね。

3. $f : G \longrightarrow G'$ を、群 G から群 G' への準同型写像とする。また、
$K = Kerf = \{x \in G \mid f(x) = 1\}$ とする。

   (a) $H \leq G$ とする。このとき、$f^{-1}(f(H)) = HK \leq G$ であることを証明せよ。
   $x \in f^{-1}(f(H))$ とすると、$f(x) \in f(H)$。従って、$h \in H$ で $f(x) = f(h)$ となるものが存在する。ここで、$f(h^{-1}x) = f(h)^{-1}f(x) = f(x)^{-1}f(x) = 1$ だから $h^{-1}x \in K$。従って、$x \in hK \subset HK$ となる。x は任意だから、$f^{-1}(f(H)) \subset HK$。逆に $h \in H$、$k \in K$ とすると、$f(hk) = f(h)f(k) = f(h) \in f(H)$ だから、$hk \in f^{-1}(f(H))$ である。これは、$HK \subset f^{-1}(f(H))$ を意味する。上で示したことより $f^{-1}(f(H)) = HK$ である。
   $x, y \in f^{-1}(f(H))$ とする。$f(x), f(y) \in f(H)$ だから $f(x) = f(h)$、$f(y) = f(h')$ となる $h, h' \in H$ をとる。$f(x^{-1}y) = f(x)^{-1}f(y) = f(h)^{-1}f(h') = f(h^{-1}h')$ で、H が G の部分群であることより、$h^{-1}h' \in H$ 従って、$x^{-1}y \in f^{-1}(f(H))$ となる。これは、問題 1 より、$f^{-1}(f(H)) \leq G$ を意味する。
   K が G の正規部分群であることを使えば、$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$ だから、$(HK)^{-1}HK = K^{-1}H^{-1}HK \subset KHK = HKK \subset HK$ となり、$HK \leq G$ が言える。ほかにも何を仮定するかにより、証明も変わるが、一番原始的な方法を用いた。

   (b) $HK/K \simeq f(H) \simeq H/(H \cap K)$ であることを証明せよ。
   $f(HK) = f(H)$ だから、核を考える。$f_{|HK} : HK \to G'$ と考えると、$K = Ker(f_{|HK})$ である。$f_{|H} : H \to G'$ と考えると、$K \cap H = Ker(f_{|H})$ である。あとは、準同型定理により、$HK/K \simeq f(H) \simeq H/(H \cap K)$ がえられる。$f_{|HK}, f_{|H}$ は f の定義域をもともと G 全体だったものを HK や H に制限したものと言う意味で、どの元に何を対応させるかは変えないというものです。

4. p を素数とし、H を群 G の正規部分群で、位数 $|H|$ が p であるとする。

(a) $a \in H$ が G の単位元でなければ、$H =< a >$ であることを示せ。

ラグランジュの定理により、$| < a > |$ は $|H|$ の約数であるが、$a \neq 1$ だから $| < a > | \neq 1$ である。$|H| = p$ は素数だから、$| < a > | = p$。$< a > \subset H$ だから、$< a >= H$ となる。

(b) $H^* = H \setminus \{1\}$ すなわち H の単位元以外の元全体からなる集合を表すとする。

$$f : H^* \times G \longrightarrow H^* \ ((a, x) \mapsto x^{-1}ax)$$

とする。f は G の H^* 上の作用を定義することを示せ。

$a \in H^*$ ならば、H が正規部分群であることより、$x \in G$ に対して、いつでも、$x^{-1}ax = f(a, x) \in H$ である。また、$a \neq 1$ だから、$x^{-1}ax \neq 1$ も明らか。従って、$f(a, x) \in H^*$。さらに、$f(a, 1) = 1^{-1}a1 = a$。また、$f(a, xy) = (xy)^{-1}a(xy) = y^{-1}(x^{-1}ax)y = f(f(a, x), y)$ だから f は G の H^* 上の作用を定義する。

$f(a, x) = a^x$ と書いたとすると、f が上の定義域、値域をもった写像であることを確認すること、さらに、$a^1 = a$、$a^{xy} = (a^x)^y$ であることを確認することが、この問題の中心部分です。

(c) $x \in G$ とする。このとき、$i \in \{1, 2, \ldots, p-1\}$ で、どの元 $a \in H^*$ に対しても、$f(a, x) = a^i$ となるものが存在することを証明せよ。(Hint: (a) 参照。)

$1 \neq h \in H$ とする。$f(h, x) \in H^*$ でかつ、(a) より $H =< h >$ だから $f(h, x) = h^i$ となる、$i \in \{1, 2, \ldots, p-1\}$ が存在する。$f(h, x) \neq 1$ だから $i \neq 0$ であることも明らか。ここで、$a \in H^*$ とすると、$a = h^j$ となる $j \in \{1, 2, \ldots, p-1\}$ が存在する。すると、

$$f(a, x) = x^{-1}ax = x^{-1}h^jx = (x^{-1}hx)^j = f(h, x)^j = (h^i)^j = (h^j)^i = a^i$$

となる。この問題の大切なところは、一つの h に対して決めた i がほかの $a \in H^*$ についても、変わらないという部分です。

(d) $x \in G$ とする。x の位数 $o(x) = | < x > |$ が $p-1$ と互いに素であれば $x \in C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$。すなわち、 x は H のすべての元と交換可能であることを示せ。(Hint: 前問の様に i を選んだ時、$f(a, x^2), f(a, x^3), \ldots$ がどうなるか考えよ。)

$o(x) = m$ とする。前問のように、i を決めると、$f(a, x) = a^i$。$f(a, x^2) = a^{i^2}$、となっていくから、$a = f(a, 1) = f(a, x^m) = a^{i^m}$ となるから、$i^m - 1$ は、p で割り切れる。しかし、$\boldsymbol{Z}_p^*$ は乗法に関して位数 $p-1$ の群だから、$i \in \{1, 2, \ldots, p-1\}$ に注意すると、$i^{p-1} - 1$ は p で割り切れる。(5 参照) ここで、$gm + h(p-1) = 1$ となる $g, h \in \boldsymbol{Z}$ をとると、$\boldsymbol{Z}_p^*$ の中で、$i = i^{gm+h(p-1)} = (i^m)^g \cdot (i^{p-1})^h = 1$。これは、$x^{-1}ax = a$ すなわち、$x \in C_G(H)$ を意味する。

5. $G = \boldsymbol{Z}_{15}^*$ とする。$\boldsymbol{Z}_{15} = \{\bar{0}, \bar{1}, \ldots, \overline{14}\}$ は、演算 $\cdot$ を $\bar{i} \cdot \bar{j} = \overline{i \cdot j \text{ を } 15 \text{ で割った余り}}$ で定義すると、$(\boldsymbol{Z}_{15}, \cdot)$ はモノイドになるが、その正則元（逆元をもつもの）全体を $\boldsymbol{Z}_{15}^*$ と書く。これは群となる。

   (a) $a \in G$ とすると、$a^4 = 1$ であることを示せ。ただし 1 は G の単位元とする。

   正則元は、15 と互いに素なものが対応している。なぜなら、a が 15 と互いに素ならば、$ba + 15c = 1$ となる、$b, c \in \boldsymbol{Z}$ が存在するが、これは、$\bar{b}\bar{a} = 1$ を意味している。そこで、$\boldsymbol{Z}_{15} = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$ で、位数はそれぞれ、$1, 4, 2, 4, 4, 2, 4, 2$ である。

   (b) G と同型な群で、巡回群の直積となっているものを一つ上げよ。

   まず、G は位数 8 のアーベル群である。有限生成アーベル群の定理より、すべての有限アーベル群は、巡回群の直積と同型で、かつ、位数 8 の群は、$8 = e_1 e_2 \cdots e_r$ かつ、$e_i | e_{i+1}$ が $i = 1, 2, \ldots, r-1$ について成り立つような 2 以上の自然数の組 $(e_1, e_2, \ldots, e_r)$ に対応していたから、この組は、(8), $(2, 4)$, $(2, 2, 2)$ のいずれかで、$\boldsymbol{Z}_8$、$\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$ または $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ と同型である。前の問題よりこの群の元には、位数が 4 の（4 乗して始めて 1 となる）ものはあるが、位数が 8 のものは無いので、$\boldsymbol{Z}_8$ とも $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ とも同型ではないので、$\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$ と同型である。

   (c) n を 3 でも 5 でも割れない自然数とする。このとき、$n^4 - 1$ は 15 で割り切れることを示せ。

   n は 15 と互いに素である。従って、n を 15 で割ったあまりを $\bar{n}$ とすると、$\bar{n} \in \boldsymbol{Z}_{15}$。(a) より、$\bar{n}^4 = \bar{1}$。かけ算の定義から、$n^4 - 1$ を 15 で割ったあまりは、0 であることが分かる。これが求めることであった。正確に、15 で割ったあまりとして、計算していくなら、もう少し丁寧にすべきであるが、実はあまりの部分だけの計算で良いことは、$(a + 15\boldsymbol{Z}) * (b + 15\boldsymbol{Z}) = ab + 15\boldsymbol{Z}$ と定義するとこれにより、$\boldsymbol{Z}/15\boldsymbol{Z}$ がモノイドになり、その正則元の全体が $\boldsymbol{Z}_{15}^*$ と同型であることを確かめれば、あまりだけ計算すれば良いことが分かる。a と b が それぞれを 15 で割ったあまりが等しい時、$a \equiv b \pmod{15}$ などと書く。