VE203 Discrete Math

Spring 2022 — HW4 Solutions

April 5, 2022

Exercise 4.1

Let $d = \gcd(a, b)$ and $a = a' \cdot d, b = b' \cdot d$, then a' and b' are co-prime. So we have

$$
\begin{aligned}
\frac{a}{\gcd(a,b)} \mid c \quad &\Leftrightarrow \quad \frac{a'd}{d} \mid c \\
&\Leftrightarrow \quad a' \mid b'c \\
&\Leftrightarrow \quad a'd \mid b'dc \\
&\Leftrightarrow \quad a \mid bc
\end{aligned}
$$

Exercise 4.2

(i) Suppose that there are only finite of them, and the largest of them is the m-th prime $p_m = 3k + 2$. Consider $N = 3p_1p_2 \cdots p_m - 1$, it is not divisible by any primes among $p_1, p_2, \ldots p_m$, so all the prime factor of N is in the form of $3n + 1$. But all the $3n + 1$ form primes times up would give a number in the form of $3n + 2$ like N, contradiction.

(ii) From (i) we know there are infinite primes of form $3n + 2$, namely in the form of $6n + 2$ or $6n + 5$. Since $6n + 2$ is even and all the primes greater than 2 is odd, we must have infinite primes in the form of $6n + 5$.

Exercise 4.3

(i) We prove a more general form: for $n, m \in \mathbb{N}, n \neq m, \gcd(F_n, F_m) = 1$.

Proof. Just assume that $n > m$, let $n = m + k$, we have

$$
\begin{aligned}
F_m &= 2^{2^m} + 1 \\
F_{m+k} &= 2^{2^{m+k}} + 1 = 2^{2^m \cdot 2^k} + 1
\end{aligned}
$$

So

$$F_{m+k} - 2 = 2^{2^m \cdot 2^k} - 1 = (2^{2^m})^{2^k} - 1$$

Since

$$2^{2^m} + 1 \mid (2^{2^m})^{2^k} - 1 \Rightarrow F_m \mid F_{m+k} - 2$$

Considering F_n, F_m are odd numbers, so $\gcd(F_n, F_m) = 1$. □

(ii) There are infinite Fermat numbers, and each of them can be decomposed into product of primes. From (i) we know that they are pairwise co-prime, so all the primes among these decomposition are different. Namely there are infinite primes.

Exercise 4.4

(i) Since a is even, we write $a = 2k, k \in \mathbb{Z}$. Let $d_1 = \gcd(k, b), k = k_1 \cdot d_1, b = b_1 \cdot d_1$, where b_1 and k_1 are co-prime. Then

$$\gcd(a, b) = \gcd(2k_1 d_1, b_1 d_1) = d_1 \cdot \gcd(b_1, 2k_1) = d_1 = \gcd(a/2, b).$$

(ii) We write $a = 2m, b = 2n,\ m, n \in \mathbb{Z}$. Let $d_2 = \gcd(m, n), m = m_1 \cdot d_2, n = n_1 \cdot d_2$, where m_1 and n_1 are co-prime. Then

$$\gcd(a, b) = \gcd(2m_1 d_2, 2n_1 d_2) = 2d_2 \gcd(m_1, n_1) = 2\gcd(a/2, b/2).$$

Exercise 4.5

(i) The left hand side is even but the right hand side is odd, so there is no solution.

(ii) (...procedure omitted)

The solution is given by

$$\begin{cases} x = -25272 + 439k \\ y = -4896 + 84k \end{cases}, k \in \mathbb{Z}$$

Exercise 4.6

(i) As the generated product is defined as $S \times S \to S$, it satisfies closure.

(ii) $a, b, c \in G, (a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c)$, L.H.S $= c \boxtimes (b \boxtimes a) = (c \boxtimes b) \boxtimes a =$ R.H.S

(iii) $\exists 1$ s.t. $1 \cdot a = a \cdot 1 = a,\ 1 \boxtimes a = a \boxtimes 1 = a$

(iv) $\forall a, \exists b, a \cdot b = b \cdot a = 1,\ a \boxtimes b = b \boxtimes a = 1$

Hence, it is a group.

Exercise 4.7

(i) $\forall x, y \in G \Rightarrow x \cdot y \in G\ x^2 = y^2 = (xy)^2 = 1$

$yx \cdot xy \cdot xy = yx$

$y \cdot 1 \cdot y \cdot xy = yx$

$xy = yx$

Hence, G is abelian.

(ii) Let the order of ab be m, that of ba be n.

Assume $m > n$.

$$\overbrace{ab \cdot ab \cdot ab \cdot a \underbrace{\cdots ba \cdot ba \cdot ba \cdots}_{kn} \cdot b \cdot ab \cdot ab}^{m} = 1$$

$(ab)^{m-kn} = 1$ and $m - kn < m$, contradicts to m is the order.

Therefore, $m \leq n$. Similarly, we can get $n \leq m$. Hence, $m = n$.

Exercise 4.8

(i) *Proof*

$\forall x, y \in G$,

$f(x) = e^{ix}, f(y) = e^{iy}$.

$x + y \in G$,

$f(x+y) = e^{i(x+y)} = e^{ix} * e^{iy} = f(x) * f(y)$.

Hence, f is a homomorphism.

Proved

(ii) $\ker f = \{x \in \mathbb{R} \mid x = 2k\pi, k \in \mathbb{Z}\}$

(iii) $\operatorname{im} f = \{x \in \mathbb{C} || x |= 1\}$

Exercise 4.9

(i) *Proof*

As G is cyclic,

$\exists x \in G, \forall a \in G, \exists m \in \mathbb{Z}, a = x^m$

Assume $\phi(x) = y \in G'$,

$\forall b \in G', b = \phi\left(x^m\right) = \phi(x) * \phi\left(x^{m-1}\right) = \ldots = \phi(x)^m = y^m$

Hence, G' is cyclic.

Proved

(ii) *Proof*

As G is abelian,

$\forall x_1, x_2 \in G, x_1 x_2 = x_2 x_1$

Considering $\forall y_1, y_2 \in G$,

$\exists x_1, x_2, y_1 = \phi\left(x_1\right),$

$y_2 = \phi(x_2)$

$y_1 y_2 = \phi(x_1) * \phi(x_2) = \phi(x_1 x_2) = \phi(x_2 x_1) = \phi(x_2) * \phi(x_1) = y_2 y_1$

Hence, G' is abelian.

Proved

Exercise 4.10

(1) $(i) \to (ii)$

As G is abelian,

$\forall x_1, x_2 \in G, x_1 x_2 = x_2 x_1$

$f(x_1) = x_1^{-1}, f(x_2) = x_2^{-1}$

$f(x_1) * f(x_2) = x_1^{-1} x_2^{-1}$

$(x_1 x_2)(f(x_1) * f(x_2)) = (x_1 x_2)\left(x_1^{-1} x_2^{-1}\right) = x_1 x_1^{-1} x_2 x_2^{-1} = 1$

Hence, f is homomorphism.

(2) $(ii) \to (i)$

As f is homomorphism,

$x_1 x_2 = f\left(x_2^{-1} x_1^{-1}\right) = f\left(x_2^{-1}\right) * f\left(x_1^{-1}\right) = x_2 x_1$

Hence, G is abelian.

Hence, according to (1) & (2), (i) & (ii) are equivalent.

Exercise 4.11

We just need to verify that all the group elements of

$$B := \{1, (12)(34), (13)(24), (14)(23)\}$$

are in A_4 and verify that it is still a group, then we are done.

First note that for any transposition $\tau, \operatorname{sgn}(\tau) = -1$ and for any two of the transpositions $\tau, \sigma, \operatorname{sng}(\tau \circ \sigma) = 1$. We further note that $\operatorname{sng}(1) = 1$. Then since all the group elements except 1 of group B is a composition of two transpositions, and with $\operatorname{sng}(1) = 1$, we know that $B \subset A_4$.

We now try to verify that B is still a group.

1. We check whether the identity element exists. This is clear since we have $1 \in B$. 2. Then we check any two group elements do group action are still in the group.

(1) $((12)(34)) = ((12)(34))(1) = (12)(34) \in B$
(1) $((13)(24)) = ((13)(24))(1) = (13)(24) \in B$
(1) $((14)(23)) = ((14)(23))(1) = (14)(23) \in B$
$((12)(34))((13)(24)) = (14)(23) \in B$

$((13)(24))((12)(34)) = (14)(23) \in B$
$((13)(24))((14)(23)) = (12)(34) \in B$
$((14)(23))((13)(24)) - (12)(34) \in B$
$((12)(34))((14)(23)) = (13)(24) \in B$
$((14)(23))((12)(34)) = (13)(24) \in B$

3. Lastly, we check that for every group elements, there is a inverse element.

$$\begin{aligned} ((12)(34))^{-1} &= (12)(34) \in B \\ ((13)(24))^{-1} &= (13)(24) \in B \\ ((14)(23))^{-1} &= (14)(23) \in B \\ (1)^{-1} &= 1 \end{aligned}$$

Hence B is indeed a group. Furthermore, since $B \subset A_4$, we conclude that B is a subgroup if A_4.

Exercise 4.12

We pair any two elements in the group G if

$$g^2 \neq e \Leftrightarrow g \neq g^{-1} \Leftrightarrow \exists \left(g, g^{-1}\right) \text{ such that } g \neq g^{-1}.$$

But notice that e has no pairing, since

$$e^2 = e \Leftrightarrow e = e^{-1}$$

Since $2||G\,|$, we know that there must exist another element g in the group such that

Exercise 4.13

1. We prove this by given a counter example. Consider S_4 and its two subgroups, which are
$$A := \langle (12)(34) \rangle \quad , \quad B := \{(12)(34), (13)(42), (23)(41), e\}$$
We see that
$$A \trianglelefteq B \wedge B \trianglelefteq S_4$$
but
$$A \ntrianglelefteq S_4$$
This can be shown easily by while
$$\underset{b \in B}{\forall} bAb^{-1} = A$$
$$(1234)((12)(34))(1284)^{-1} \notin A$$
where $(1234) \in S_4$, hence
$$A \ntrianglelefteq S_4$$

2. Suppose the index of $H \leq G$ is 2 . Then, we only have 2 left cosets of H, namely, H and gH for some $g \in G$.

   If $gh \in H$, then $gH = H = Hg$.

   If $gh \in gH \neq H$, then $gH = G - H$.

   Also, $Hg = G - H$. Therefore, $gH = Hg$.

   The above two conditions show that H is normal.

3. Simply take
$$G = S_3 \quad , \quad A := \langle \tau \rangle$$
where $\tau = (12)$. Since we know that the index of $\langle \tau \rangle$ is clearly $3!/2 = 3$, while
$$(23)(12)(23)^{-1} \notin A$$
hence
$$A \ntrianglelefteq S_4$$

Exercise 4.14

1. From Lagrange's Theorem, we know that if we have a subgroup $\langle g \rangle$ where $g \in G$ is not identity. We note that since $p \geq 2$, hence $|G| \geq 4$, so there exists some element $g \neq e$. Then we know that
$$|\langle g \rangle|||G| = p^2$$
From the property of prime, we know that $|\langle g \rangle|$ can only be Since $g \neq e$ by assumption(otherwise it will just be a trivial subgroup, not in our interest), then $|\langle g \rangle|$ can only be p, p^2 If $|\langle g \rangle| = p$, then we are done. Now if $|\langle g \rangle| = p^2$, then we know that in this case,
$$\langle g \rangle = G$$
, which can't always be true since $|G| = p^2 \notin \mathbb{P}$. Hence, we can always choose some g such that $|\langle g \rangle| = p$.

2. Proceed from (i). Suppose we now know there exist only one subgroup of order p, then we note that the number of the elements in G which is not in $\langle g \rangle$ is
$$p^2 - p = p(p-1)$$
Noting that this is actually equal to
$$\varphi\left(p^2\right)$$
which indicate that all elements not in $\langle g \rangle$ are generators of G since where $g' \notin \langle g \rangle$, with the fact that since only one subgroup has order p, which is $\langle g \rangle$ but not $\langle g' \rangle$.

Exercise 4.15

However, this does not hold in general: given a finite group G and a divisor d of $|G|$, there does not necessarily exist a subgroup of G with order d. The alternating group $G = A_4$, which has 12 elements has no subgroup of order 6 . We prove it below.

G consists of:

- The identity or neutral element e.

- The three elements that are product of disjoint transpositions. Those 3 elements with e make up a subgroup $V \subset H$(V is isomorphic to the Klein four-group)

- The eight 3-cycles.

Suppose that $H \subset G$ is a subgroup of order 6 and that H' denotes the intersection $H \cap V.H'$ is a subgroup of H and V.

By Lagrange's theorem, H' order divides 4 and 6 . So $|H'|$ is equal to 1 or to 2 .

If $|H'| = 1$, the map$(h, v) \mapsto h \cdot v$ defined from $H \times V$ to G is one-to-one. Which doesn't make sense as G would have at least 24 elements. Therefore $|H'| = 2$ and H is made up the identity e, an element v which is product of two disjoint transpositions and six 3-cycles.

Also the index $|G : H|$ is equal to 2 and consequently H is a normal subgroup of G. We recall the argument. For $a \in G \backslash H$ the left cosets H, aH form a partition of G. Similarly, the right cosets H, Ha form a partition of G. As $aH \neq H$, we have $aH = Ha$ which allows to conclude.

We denote $v = (i, j)(k, l)$ with $\{i, j, k, l\} = \{1, 2, 3, 4\}$ and t the 3-cycle (i, j, k). We have $tvt^{-1} = (j, k)(i, l) \neq (i, j)(k, l)$ and $tvt^{-1} \in H$ as $H \triangleleft G$. In contradiction with the cardinality of $|H'| = |H \cap V| = 2$. We have finally proven that A_4 has no subgroup of order 6 .