I216e Discrete Math (for Review)

Nov 22nd, 2017

To check your understanding. Proofs of $*$ do not appear in the exam.

1 Monoid

Let $(G, \circ)$ be a monoid.

Proposition 1 (Uniquness of Identity) An idenity e is *unique*,
i.e., If there are two identies, e, e', then $e = e'$.

Proposition 2 (Uniqueness of Inverse) An inverse of a, a^{-1}, is *unique* if a is an invertible element.

The above does not always hold for a magma $(G, \circ)$, which does not hold the associative law.

Proposition 3 For an invertible element $a \in G$, the solution of $a \circ x = b$ is unique, in addition $x = a^{-1} \circ b$.

Proposition 4 The inverse of identity e is e.

Proposition 5 If $a, b \in G$ are both invertible, $a \circ b$ is also invertible, and

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

Proposition 6 If $a \in G$ is invertible, then a^{-1} is also invertible, and $(a^{-1})^{-1} = a$.

Proposition 7 $(G^{\times}, \circ)$ turns out a group.

NOTE: Propositions, 1 – 7, hold in any group because a group is a monoid. (The only difference is that $G^{\times} = G$ when $(G, \cdot)$ is a group.)

2 Group

Let G be a group.

Theorem 1 H is a subgroup of G if and only if

$$\forall a, b \in H \quad [a \circ b^{-1} \in H]$$

3 Equivalence Class

Proposition 8 * Let $C(a)$ be the equivalence class of a in set S by equivalence relation $\sim$.

- $a \in C(a)$.
- If $b \in C(a)$, then $C(b) = C(a)$.
- If $C(a) \neq C(b)$, then $C(a) \bigcap C(b) = \emptyset$.

4 Lagrange's Theorem

Theorem 2 (Lagrange's Theorem) Let H be a subgroup of G. Then,

- $|G| = [G : H]|H|$.
- Let G be a finite group. Then, the order of H divides the order of G, i.e., $|H|$ divides $|G|$.

5 Normal Subgroup and Residue Class Group

Theorem 3 Let N be a subgroup of G. Then, all the following conditions are equivalent:

1. N is a normal subgroup of G.
2. For all $a \in G$, $aN = Na$.
3. For all $a \in G$, $aN \subset Na$.
4. For all $a \in G$, $Na \subset aN$.
5. For all $a \in G$, $N = aNa^{-1}$.
6. For all $a \in G$, $N \subset aNa^{-1}$.
7. For $a \in G$, $aNa^{-1} \subset N$.

Proposition 9 Let N be a normal subgroup of G. Then $G/N = G\backslash N$ as partition of G.

Theorem 4 (Residue Class Group) Let N be a normal subgroup of G. Define (appropriate) binary operations on G/N and $G\backslash N$, respectively. Then $G/N = G\backslash N$ as group.

6 Group Homomorphisim

Proposition 10 Let e and e' be the identities of G and G', respectively. If $f : G \to G'$ is homomorphic, then $f(e) = e'$.

Proposition 11 If $f : G \to G'$ is homomorphic, then for all $x \in G$, it holds that $f(x^{-1}) = f(x)^{-1}$.

Proposition 12 If $f : G \to G'$ is homomorphic, then $\mathsf{Im}(f)$ is a subgroup of G'.

Proposition 13 A homomorphism map $f : G \to G'$ is isomorphic if $\mathsf{Im}(f) = G'$ and $\mathsf{Ker}(f) = \{e\}$.

Theorem 5 (Fundamental Homomorphism Theorem) Let $f : G \to G'$ be a homomorphism map from group G to group G'. Then, all the followings hold.

1. $\mathsf{Im}(f)$ is a subgroup of G'.
2. $\mathsf{Ker}(f)$ is a normal subgroup of G.
3. $\bar{f} : x \circ \mathsf{Ker}(f) \in G/\ker(f) \mapsto f(x) \in G'$ is homomorphic, and it holds that
$$G/\mathsf{Ker}(f) \cong \mathsf{Im}(f)$$
In particular, when $\mathsf{Im}(f) = G'$ (surjective), $G/\mathsf{Ker}(f) \cong G'$.

7 Ring

Proposition 14 $(R_1 \times \cdots \times R_n)^\times = R_1^\times \times \cdots \times R_n^\times$.

Generally, for monoid $G_1, \ldots, G_n$, $(G_1 \times \cdots \times G_n)^\times = G_1^\times \times \cdots \times G_n^\times$.

Proposition 15 If $R \cong R_1 \times \cdots \times R_n$, then $R^\times = R_1^\times \times \cdots \times R_n^\times$.

Proposition 16 $(0_{R_1}, \ldots, R_i, \ldots, 0_{R_n})$ is an ideal in product ring $(R_1 \times \cdots \times R_n)$.

Even for non-commutative $R_1, \cdots, R_n$, $(0_{R_1}, \ldots, R_i, \ldots, 0_{R_n})$ is a (two-sided) ideal.

8 Ideal and Residue Class Ring

Proposition 17

- If R is a commutative ring, left and right ideals of R are two-sided ideals.
- $n\mathbb{Z}$ is an ideal of ring $\mathbb{Z}$.
- $\{0\}$ and R are always ideals of any ring R.

Theorem 6 (Residue Class Ring) Let I be an ideal of ring R. Then, R/I is a ring, with appropriate additive and multiplicative operations. R/I is called a residue class ring.

9 Fundamental Ring Homormorphism Theorem

Theorem 7 (Fundamental Ring Homomorphism Theorem) * Let $f : R \to R'$ be ring homomorphic. Then,

1. $\mathsf{Im}(f) = \{f(x) \,|\, x \in R\}$ is a subring of R'.
2. $\mathsf{Ker}(f) = \{x \in R \,|\, f(x) = 0' \in R'\}$ is a (two-sided) ideal of R.
3. $\bar{f} : x + \mathsf{Ker}(f) \in R/\ker(f) \mapsto f(x) \in R'$ is ring homomorphic and it holds that
$$R/\mathsf{Ker}(f) \cong \mathsf{Im}(f).$$
   If $\mathsf{Im}(f) = R'$, then $G/\mathsf{Ker}(f) \cong R'$.

10 Fermat's Little Theorem

Theorem 8 (Fermat's Little Theorem) Let p be a prime. For $a \in \mathbb{N}$, the following holds.
$$a^{p-1} \equiv 1 \pmod{p}$$

11 Euler's Theorem

$\phi(n) \triangleq \{x \in \mathbb{N} \mid 1 \leq x \leq n \text{ and } (x,n) = 1\}$ is called *Euler's ϕ function* or *Euler's totient function.* Equivalently, Euler's totient function $\phi(n)$ is the number of positive integers up to n that are relatively prime to n.

Proposition 18 *

- For $(m,n) = 1$, it holds that $\phi(mn) = \phi(m)\phi(n)$.
- For prime p and positive integer e, it holds that $\phi(p^e) = p^{e-1}(p-1)$.
- Let $n = \prod_{i=1}^{s} p_i^{e_i}$. Then, it holds that

$$\phi(n) = n \prod_{i=1}^{s} (1 - \frac{1}{p_i}).$$

Theorem 9 (Euler's Theorem) For $a, n \in \mathbb{N}$,

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

12 Integral Domain and Finite Field

Proposition 19 * Let R be an integral domain. $a \in R$ is a prime element $\Longleftrightarrow$ (a) is a prime ideal in R.

Proposition 20 *

- Euclidean Domain (ユークリッド整域) $\subset$ Principal Ideal Domain (単項イデアル整域).
- In a PID, a prime element (素元) = an irreducible element.
  - In a PID R,
    $a \in R$: an irreducible element $\Leftrightarrow$ $a \in R$: a prime element $\Leftrightarrow$ $(a) \subset R$: a prime ideal.
- In $\mathbb{Z}$, any ideal is of the form $(n) = n\mathbb{Z}$; $p\mathbb{Z}$ is a prime ideal for any prime p; if I is a prime ideal, there is a prime p such that $I = p\mathbb{Z}$.

Theorem 10 * For an ideal I in R, it holds that

$$I \text{ is a maximal ideal.} \quad \Longleftrightarrow \quad R/I \text{ is a field.}$$

Theorem 11 * When R is a PID, I is a prime ideal $\Leftrightarrow$ I is a maximal ideal.

Proposition 21 * Let K be a field. Then the polynomial ring in X over K, denoted $K[X]$, is an Euclidean domain with $\lambda(f) = \deg(f)$.

Proposition 22 *

- $f(X)$ is an irreducible polynomial in $K[X]$.
- $f(X)$ is a prime element in $K[X]$.
- $(f(X))$ is a prime ideal.
- $(f(X))$ is a maximal ideal.
- $K[X]/(f(X))$ is a field.

Theorem 12 *

- When $q = p$ (prime), then $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.
- When $q = p^r$, for any monic irreducible $f(X) \in \mathbb{F}_p[X]$ of $\deg(f) = r$,

$$\mathbb{F}_q \cong \mathbb{F}_p[X]/f(X).$$

13 Calculation

Problem 1 Find $(X, Y) \in \mathbb{Z}^2$ such that $7X + 12Y = 1$.

Problem 2 Find the inverse of 7 (or more presicely $7 + 12\mathbb{Z}$) in $\mathbb{Z}/12\mathbb{Z}$.

Problem 3 Find $(X, Y) \in \mathbb{Z}^2$ such that $117X + 71Y = (117, 71)$.

Problem 4 Compute $3^{722} \bmod 1001$ (where $1001 = 7 \times 11 \times 13$).

Problem 5 Find integers X such that $X^5 \equiv 8 \pmod{21}$.

Problem 6 What are those integers when divided by 5 is remainder 1; divided by 7 is remainder 3; and divided by 11 is remainder 5.

$$\begin{aligned} x =& 1 \bmod 5 \\ x =& 3 \bmod 7 \\ x =& 5 \bmod 11 \end{aligned}$$