Test
Final Exam: Groups, Rings, and Fields

- You should provide clear and complete reasoning for every solved problem.

  REMEMBER THIS EXAM IS GRADED BY A HUMAN BEING. WRITE YOUR SOLUTIONS NEATLY AND COHERENTLY, OR THEY RISK NOT RECEIVING FULL CREDIT

- This is a closed-book examination. You can use results proved in lectures and HWs, provided you include appropriate references. Other results should be proved for receiving full credit.
- Turn off all cell phones, smartphones, and other electronic devices, and remove all headphones, earbuds, and smartwatches. Put all of these items away. The use of any networked devices while working on this exam is not permitted.
- You have 120 minutes for this exam.
- There are 7 problems in this exam, all of them are mandatory.

I have read and agreed to the rules above: _____
Print Your Full Name

DO NOT WRITE BELOW THIS LINE. FOR GRADING PURPOSES ONLY.

Problem 0	Problem 1	Problem 2	Problem 3	Problem 4	Problem 5	Problem 6	Sum

Problem 0: Theory

Every definition/axiom/proposition/theorem should be written clearly and without additional definitions or undefined notions.

(a) Let G be a group and H be its subgroup. Give a definition of an H-coset in G.

(b) Formulate Division Algorithm for $\mathbb{Z}[i]$, where $i^2 = -1$, and $\mathbb{Q}[x]$, where x is a free variable.

(a) $H \leq G$, $\forall g \in G$. $gH = g * H = \{g * h \mid h \in H\}$ is an H-coset in G.

(b) for $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$.

$\mathbb{Z}[i]$ $\forall x, y \in \mathbb{Z}[i]$, there exists $q, r \in \mathbb{Z}[i]$. $x = yq + r$. where $N(r) < N(y)$

$Q[x]$ $\forall f(x), g(x) \in Q[x]$. there exists $(q(x), r(x))$. $q(x), r(x) \in Q[x]$.

$f(x) = g(x)q(x) + r(x)$. where

$0 \leq \deg(r) < \deg(g)$

PLEASE TURN OVER

Problem 1: Examples

(a) Give an example of a field extension K/F such that $[K : F] \geqslant 5$. No proofs needed here.

(b) Prove that $\mathbb{Z}[\sqrt{-5}]$ contains no elements whose norm is 2 or 3.

(a) $K = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$

$F = Q$

where $[K:F] = 8$

(b) $\forall a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. $(a, b \in \mathbb{Z})$.

$N(a+b\sqrt{-5}) = a^2+5b^2$

assume there exists $a+bi$, wher $N(a+b\sqrt{-5}) = 2$ or 3

if $|b| \geq 1$. $N(a+b\sqrt{-5}) \geq 5+a^2 \geq 5 > 2$ or 3

$\therefore b=0 \Rightarrow N(a+b\sqrt{-5}) = a^2$

However, there are no such integer a s.t. $a^2 = 2$ or 3

$\therefore \mathbb{Z}[\sqrt{-5}]$ contains no element whose norm is 2 or 3

Problem 2: Group Theory

(a) Let G be a group, and H a subgroup of G with finite index $[G : H] = n$. Prove that there exists a normal subgroup K of G such that $K \leqslant H$ and $[G : K] \leqslant n!$.

(b) What is the largest possible order of an element in S_8? Describe all elements of this order. Prove all claims.

(a) Let $\varphi: G \times G/H \to G/H$

According to Cayley's Thm. every group is isomorphic to a group of permutation.

Here, G is a group action.

$\because [G:H]=n$

$\therefore G \cong S_n$ Let $f: G \to S_n$

Claim: $\ker(f)$ is a normal subgroup of G.

proof of claim: $\because \ker(f)$

$\therefore \forall k \in \ker(f).\ f(k) = e$

$\therefore \forall g \in G, \forall k \in \ker(f)$

$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(g^{-1}) = e$

$\therefore gkg^{-1} \in \ker(f)$ ∎

let $K=\ker(f)$. we have $K \trianglelefteq H$. (according to the claim).

Then $[G:K] = |G/K|$

According to First Isomorphism Thm.

$\mathrm{Im}(f) \cong G/\ker(f) \Rightarrow S_n \cong G/K \Rightarrow |G/K| = S_n = n!$

$\therefore [G:K] \leq n!$ ∎.

(b) $\sum x_i = 8$ $x_i > 0$. $\max \prod x_i$

let $i = 1 \cdots n \Rightarrow \sum_{i=1}^{n} x_i \geq n\sqrt[n]{\prod_{i=1}^{n} x_i} \Rightarrow 8 \geq n\sqrt[n]{\prod_{i=1}^{n} x_i}$

$\therefore \prod_{i=1}^{n} x_i \leq \left(\frac{8}{n}\right)^n$

PLEASE TURN OVER

$\because n \in \mathbb{Z}$.

$\therefore$ when $n=4$. $\left(\frac{8}{\pi}\right)^n$ get its maximum $\left(\frac{8}{2}\right)^3 = \frac{512}{27} = 18\frac{26}{27}$

$\because \prod_{i=1}^{n} x_i \in \mathbb{Z} \Rightarrow \prod_{i=1}^{n} x_i \leq 18$

when $3+3+2=8$. $\prod_{i=1}^{n} x_i = 18$

$\therefore$ largest possible order is 18

elements:

$$\left\{ \sigma_i \circ \sigma_j \circ \sigma_k \,\middle|\, \sigma_i \cap \sigma_j \cap \sigma_k = \phi,\ |\sigma_i| = 2,\ |\sigma_j| = |\sigma_k| = 3,\ \sigma_i, \sigma_j, \sigma_k \in S_8 \right\}.$$

eg. $(123)(456)(78)\cdots$

Problem 3: Group Theory

All groups are additive in this problem, i.e., the operation is addition $+$ of real numbers. As $\mathbb{Z} \leqslant \mathbb{Q}$ is a normal subgroup, we can consider the quotient group $\mathbb{Q}/\mathbb{Z}$.

(a) Is $\mathbb{Q}/\mathbb{Z}$ finite? Prove or disprove.

(b) Prove that every element of $\mathbb{Q}/\mathbb{Z}$ has a finite order.

(c) What are the possible orders (as elements of $\mathbb{N}$) can elements of $\mathbb{Q}/\mathbb{Z}$ have? Your answer should explicitly indicate a subset of $\mathbb{N}$.

(d) Prove that $\mathbb{Q}/\mathbb{Z}$ cannot be generated by two elements: there are no $[x_1], [x_2] \in \mathbb{Q}/\mathbb{Z}$ such that every $[b] \in \mathbb{Q}/\mathbb{Z}$ can be written as

$$[b] = a_1 \cdot [x_1] + a_2 \cdot [x_2] \text{ for some integers } a_1, a_2 \in \mathbb{Z}.$$

(a) $\mathbb{Q}/\mathbb{Z}$ is infinite

$\forall\, a, b \in \mathbb{Q}/\mathbb{Z}$. $a = a_z + a_d$ $\quad b = b_z + b_d$

where a_z, b_z are the integer parts of a, b

a_d, b_d are the decimal parts of a, b $\quad (0 \le a_d, b_d < 1)$

we say $a \sim b$ iff $a - b \mid 1 \Rightarrow (a_z + a_d) - (b_z + b_d) \mid 1$

$\therefore\ a_d = b_d \quad (a_d, b_d \in [0,1),\ a_d, b_d \in \mathbb{Q})$

$\therefore\ \mathbb{Q}/\mathbb{Z} = \{[r] \mid r \in [0,1),\ r \in \mathbb{Q}\}$ it is infinite.

(b) $\because\ \mathbb{Q}/\mathbb{Z} = \{[r] \mid r \in [0,1), r \in \mathbb{Q}\} = \{[\frac{p}{q}] \mid p, q \in \mathbb{Z},\ 0 \le p < q,\ q \ne 0\}$.

$\therefore\ |r| = |\frac{p}{q}| = q \Rightarrow$ it has finite order

(c) possible orders: $\mathbb{N}$.

(order of $|\frac{1}{q}| = q$ $\forall\, q \in \mathbb{N}$. $\Rightarrow$ orders might be $\mathbb{N}$)

(d) let $|x_1| = n_1$, $|x_2| = n_2$

$\therefore\ |b| = \operatorname{lcm}(|x_1|, |x_2|) \le n_1 n_2$

However, $\forall [b] \in \mathbb{Q}/\mathbb{Z}$. order can be $\mathbb{N} = \{1, 2 \cdots\}$,

$\therefore\ x_1$ and x_2 can only generate finite order.

$\therefore$ there are no such x_1, x_2 that ···

PLEASE TURN OVER

Problem 4: Rings

(a) Prove that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

(b) Consider the ring $\mathbb{Z}[\sqrt{-7}]$ and the principal ideal $\langle\sqrt{-7}\rangle \trianglelefteq \mathbb{Z}[\sqrt{-7}]$. Find the quotient

$$\mathbb{Z}[\sqrt{-7}]/\langle\sqrt{-7}\rangle$$

and, using this, prove that $\langle\sqrt{-7}\rangle$ is maximal.

(a) $\forall\, a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

$$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

$\because$ there are infinite pairs such that $a^2-2b^2=1$ $(a,b\in\mathbb{Z})$.

$\therefore \frac{a}{a^2-2b^2} = a \in \mathbb{Z},\ \frac{b}{a^2-2b^2} \in \mathbb{Z}. \Rightarrow (a+b\sqrt{2})^{-1} \in \mathbb{Z}[\sqrt{2}]$.

$\therefore \mathbb{Z}[\sqrt{2}]$ has infinitely many units

(b) $\forall\, a+b\sqrt{-7} \in \mathbb{Z}[\sqrt{-7}]$.

According to division algorithm

$a = (-7)\cdot q + r \quad 0 \le r < 7,\ q, r \in \mathbb{Z}$.

$$\therefore a+b\sqrt{-7}+\langle\sqrt{-7}\rangle = (-7)\cdot q + r + b\sqrt{-7} + \langle\sqrt{-7}\rangle$$
$$= r + (b+q\sqrt{-7})\sqrt{-7} + \langle\sqrt{-7}\rangle$$
$$= r + \langle\sqrt{-7}\rangle \quad (0\le r<7,\ r\in\mathbb{Z}).$$

$\therefore \mathbb{Z}[\sqrt{-7}]/\langle\sqrt{-7}\rangle = \{[0],[1],[2],[3],[4],[5],[6]\}$.

Obviously, $\mathbb{Z}[\sqrt{-7}]/\langle\sqrt{-7}\rangle$ is a commutative ring with 1

And $\because [1]\times[1]=[1],\ [2]\times[4]=[4]\times[2]=[1]$.

$[3]\times[5]=[5]\times[3]=[1],\ [6]\times[6]=[1]$

$\therefore \forall [a] \in \mathbb{Z}[\sqrt{-7}]/\langle\sqrt{-7}\rangle,\ [a]\neq 0,\ \exists [b] \in \mathbb{Z}[\sqrt{-7}]/\langle\sqrt{-7}\rangle,\ \text{s.t. } [a][b]=1$

$\therefore \mathbb{Z}[\sqrt{-7}]/\langle\sqrt{-7}\rangle$ is a field

$\therefore \langle\sqrt{-7}\rangle$ is maximal

PLEASE TURN OVER

Problem 5: Ideals

(a) Let S be a commutative ring with 1_S and z be an element in S. Prove that $\langle z\rangle$ coincides with S if and only if z is a unit in S.

(b) Consider the polynomial ring $\mathbb{Z}[x]$ and let

$$I = \{p(x) \in \mathbb{Z}[x] : p(x-1) \text{ has constant term equal to } 0\}.$$

Prove that I is a principal ideal (in particular, prove that it is an ideal).

(c) Consider the ring $\mathbb{Z}[\sqrt{-3}]$. Prove that

$$\langle 2, 1+\sqrt{-3}\rangle^2 = \langle 2\rangle \cdot \langle 2, 1+\sqrt{-3}\rangle.$$

(a) "$\Leftarrow$"

$\because z$ is a unit in S

$\therefore \exists x \in S$. s.t. $x \cdot z = z \cdot x = 1_S$

$\because \langle z\rangle$ is an ideal

$\therefore x \cdot z = 1_S \in \langle z\rangle \Rightarrow \langle z\rangle = S$

"$\Rightarrow$" $\because \langle z\rangle$ coincides with S

$\therefore 1_S \in \langle z\rangle$

$\because \langle z\rangle = \{z^k \mid k \in \mathbb{Z}\}$.

$\therefore \exists k \in \mathbb{Z}$. s.t. $z^k = 1_S$

$\therefore z \cdot z^{k-1} = 1_S$ where $z^{k-1} \in S$.

$\therefore z$ is a unit

(b) $\because p(x) \in \mathbb{Z}[x]$. $p(x-1)$ has constant term equal to 0

$\therefore p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$p(x-1) = a_n (x-1)^n + a_{n-1}(x-1)^{n-1} + \cdots + a_1(x-1) + a_0$

$\therefore \sum_{i=0}^{n} (-1)^i a_i = 0$

① $\forall p(x), q(x) \in I$, $\sum_{i=0}^{n} (-1)^i p_i = \sum_{i=0}^{n} (-1)^i q_i = 0$ $(n \geq \deg(p(x)), \deg(q(x)))$

$p(x) + q(x) = (p_n + q_n)x^n + (p_{n-1} + q_{n-1})x^{n-1} + \cdots + (p_1 + q_1)x + p_0 + q_0$

$\therefore$ constant of $p(x-1) + q(x-1)$:

$$\sum_{i=1}^{n} (-1)^i (p_i + q_i) = \sum_{i=1}^{n} (-1)^i p_i + \sum_{i=1}^{n} (-1)^i q_i = 0 + 0 = 0$$

$\therefore p(x) + q(x) \in I$

② $\forall p(x) \in I$, $r(x) \in \mathbb{Z}[x]$.

let $p(x) = p_n x^n + p_{n-1}x^{n-1} + \cdots + p_1 x_1 + p_0$

$r(x) = r_n x^n + r_{n-1} x^{n-1} + \cdots + r_1 x_1 + r_0$

$\because p(x) \in I \quad \therefore \sum_{i=0}^{n} (-1)^i p_i = 0$

$$p \cdot r(x) = \sum_{k=0}^{2n} \sum_{i+j=k} p_i r_j x^k$$

$$\therefore (p \cdot r)(x-1) = \sum_{k=0}^{2n} \sum_{i+j=k} p_i r_j (x+1)^k$$

$$\therefore \text{constant of } (p \cdot r)(x-1) = \sum_{k=0}^{2n} \sum_{i+j=k} (-1)^k p_i r_j$$

$$= \sum_{k=0}^{2n} \sum_{i=0}^{n} \sum_{j=0}^{n} (-1)^{i+j} p_i r_j \, \delta(i+j-k) = \sum_{i=0}^{n} \sum_{j=0}^{n} (-1)^{i+j} p_i r_j$$

$$= \left(\sum_{i=0}^{n} (-1)^i p_i \right) \left(\sum_{j=0}^{n} (-1)^j r_j \right) = 0$$

$\therefore p(x) \cdot r(x) \in I.$

$\therefore I$ is an ideal

$\because \forall p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x_1 + p_0. \ \sum_{i=0}^{n} (-1)^i a_i = 0$

$\therefore x = -1$ is a root for $p(x)$

$\therefore p(x) = (x+1)(p'_{n-1} x^{n-1} + p'_{n-2} x^{n-2} + \cdots + p'_1 x + p'_0)$

$\overset{\text{def}}{=} (x+1) q(x)$, where $q(x) \in \mathbb{Z}[x]$.

$\therefore I$ can be generated by $x+1$, i.e. $I = \langle (x+1) \rangle$

$\therefore I$ is a principal ideal

(c) $\langle 2, 1+\sqrt{-3} \rangle^2 = \langle 4, 2+2\sqrt{-3}, -2+2\sqrt{-3} \rangle \quad \langle 2 \rangle \cdot \langle 2, 1+\sqrt{-3} \rangle = \langle 4, 2+2\sqrt{-3} \rangle$

$\therefore \langle 2 \rangle \cdot \langle 2, 1+\sqrt{-3} \rangle \subseteq \langle 2, 1+\sqrt{-3} \rangle^2$

$\because 2+2\sqrt{-3} - 4 = -2+2\sqrt{-3}$

$\therefore -2+2\sqrt{-3} \in \langle 4, 2+2\sqrt{-3} \rangle = \langle 2 \rangle \cdot \langle 2, 1+\sqrt{-3} \rangle$

$\because 4 \in \langle 2 \rangle \cdot \langle 2, 1+\sqrt{-3} \rangle. \ 2+2\sqrt{-3} \in \langle 2 \rangle \cdot \langle 2, 1+\sqrt{-3} \rangle$

$\therefore \langle 2, 1+\sqrt{-3} \rangle^2 \subseteq \langle 2 \rangle \cdot \langle 2, 1+\sqrt{-3} \rangle$

$\therefore \langle 2, 1+\sqrt{-3} \rangle^2 = \langle 2 \rangle \cdot \langle 2, 1+\sqrt{-3} \rangle$

Problem 6: Fields

(a) Determine all subfields of the field $\mathbb{Q}(\sqrt{3})$.

(b) Prove that $\mathbb{Q}(\sin(\frac{\pi}{12})) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

(c) Find a minimal field K such that $\mathbb{R} \leqslant K$ and $\mathbb{Q}[i] \leqslant K$. Prove all claims.

(a) $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})$ are subfields of $\mathbb{Q}(\sqrt{3})$

① there are no fields F between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})$

$\because [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3}):F][F:\mathbb{Q}] = 2$

$\therefore F = \mathbb{Q}$ or $F = \mathbb{Q}(\sqrt{3})$

② there are no subfields smaller than $\mathbb{Q}$

$\therefore \mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})$ are all subfields of $\mathbb{Q}(\sqrt{3})$

(b) $\sin\frac{\pi}{12} = \sin(\frac{\pi}{4} - \frac{\pi}{6}) = \frac{\sqrt{2}}{2}(\frac{\sqrt{3}}{2} - \frac{1}{2}) = \frac{\sqrt{6}-\sqrt{2}}{4}$

we want to prove $\mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\Longleftrightarrow$ prove ① $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$ ② $\frac{\sqrt{6}-\sqrt{2}}{4} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

① $\because \frac{\sqrt{6}-\sqrt{2}}{4} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$

$\therefore (\frac{\sqrt{6}-\sqrt{2}}{4})^{-1} = \frac{\sqrt{6}+\sqrt{2}}{4} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$

$\therefore \frac{\sqrt{6}+\sqrt{2}}{4}\cdot 2 + \frac{\sqrt{6}-\sqrt{2}}{4}\cdot 2 = \sqrt{6} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$

$\frac{\sqrt{6}+\sqrt{2}}{4}\cdot 2 - \frac{\sqrt{6}-\sqrt{2}}{4}\cdot 2 = \sqrt{2} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$

$\sqrt{6}\cdot\frac{\sqrt{6}-\sqrt{2}}{4} = \frac{3}{2} - \frac{1}{2}\sqrt{3} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$

$\therefore (-2)\cdot(\frac{3}{2} - \frac{1}{2}\sqrt{3}) + 3 = \sqrt{3} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$

$\therefore \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\frac{\sqrt{6}-\sqrt{2}}{4})$

② $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\therefore (\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \Rightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$(\sqrt{2}+\sqrt{3})^{-1} = \sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \Rightarrow (\sqrt{3}+\sqrt{2})-(\sqrt{3}-\sqrt{2}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\therefore \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

END OF EXAM

$\therefore \frac{\sqrt{6}-\sqrt{2}}{4} \in Q(\sqrt{2}+\sqrt{3})$ ∎.

(1) $R \subseteq k$. $Q[i] \subseteq k$

the minimal field k can be C

proof of $R \subseteq k = C$. (by setting $b=0$, $\{a+bi \mid a.b \in R\} = R$)

$\therefore k=C$ contains R

proof of $Q[i] \subseteq k=C$ (by setting $a.b \in Q$, $\{a+bi \mid a.b \in Q\} = Q[i]$)

$\therefore k=C$ contains $Q[i]$

proof of minimum: assume there exists a field F that sits between C and R, $Q[i]$ ($C = R[i] = \{a+bi \mid a.b \in R\}$)

$\therefore R \subseteq F \subseteq C$

$\therefore [C:R] = [C:F][F:R] = 2$

$\therefore [C:F]=1$ or $[F:R]=1$

$\therefore F = C$ or $F=R$

$\therefore$ that F doesn't exists.

$\therefore k=C$