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) Write down two "almost the same" definitions of how G acts on X as we discussed in class. Be sure to list all the detailed conditions.

(b) Define what it means for F to be a field.

(c) Formulate Division Algorithm for $\mathbb{Z}$ and $\mathbb{Z}[i]$.

(a) ① $\varphi: G \to Sym(X)$

② $\varphi: G \times X \to X$

① $e_G(x) = x \in G$.

② $g_1 * g_2(x) = g_1(g_2(x))$

(b) 1) $(F, +)$ is an abelian (① group (② ~ ④)

2) $(F, \times)$ is associative.

3) $(F, +, \times)$ distributivity

4) identity for F: 0_F.

units for F: 1_F

5) $(F, \times)$ is commutative

6) $F^* = F \setminus \{0\}$. i.e. $\forall a \in F.\ a \neq 0,\ \exists\, b \in F.$ s.t. $ab = 1_F$.

(c) For $\mathbb{Z}$: $\forall a, b \in \mathbb{Z}$, there exists a pair (q, r), $q, r \in \mathbb{Z}$, s.t. $a = bq + r$

where $0 \leq r < |b|$

For $\mathbb{Z}[i]$: $\forall x, y \in \mathbb{Z}[i]$, there exists

$q, r \in \mathbb{Z}[i]$, $x = yq + r$.

where $N(r) < N(y)$

(here $N(a+bi) = a^2 + b^2$

Problem: 1: Examples

(a) Provide an example of an element of $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_6$ which has order 10 and does not have a 0 in any component.

(b) Provide an example of a principal ideal of $\mathbb{Z}_3 \times \mathbb{Z}_4$ which is a prime ideal.

(c) Find an example of a field extension K/F such that $[K : F] = 3$.

(a) $10 = 2 \cdot 5$

: element $(2,1,3)$ has order 10 and does not have a 0 in any component

(b) $\langle (0,1) \rangle = \{(1,2),(1,4),(2,2),(2,4),(0,2),(0,4)\}$. $\{(0,1)\}$.

(c) $F = \mathbb{Q}$. $K = \mathbb{Q}(\sqrt[3]{2})$

$[K:F] = 3$

$ab \in \mathbb{Z}$

$\mathbb{Z}/42$.

$a \in \mathbb{Z}$ or $b \in \mathbb{Z}$.

$(0,1) * (a,b) = (0,b)$

$\{(0,1)\ (0,2)\ (0,3)\ (0,4)\}$.

$\forall (0,b) \in \mathbb{Z}$.

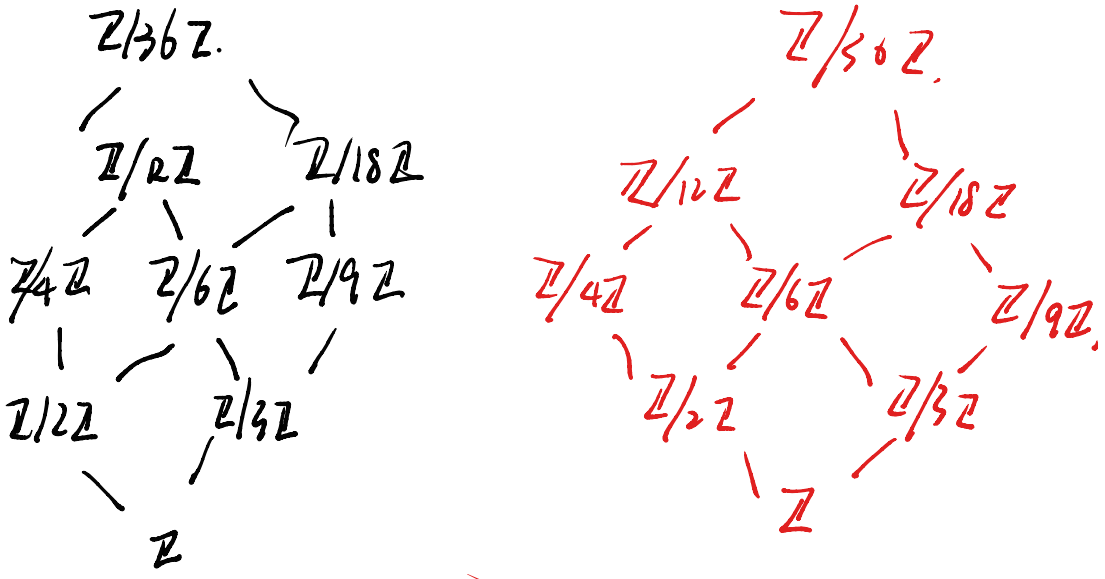
$(0,a) \in \mathbb{Z}$ or $(0,b) \in \mathbb{Z}$.

Problem: 2: Groups

(a) Draw the subgroup diagram for the cyclic group $(\mathbb{Z}/36\mathbb{Z}, +)$. Make sure to explain/prove your conclusions.

(b) Prove the isomorphism $\mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ using the theorem about the isomorphism for external/internal products of groups. All groups are additive(i.e., operation is "+").

(a)



(b) let $G = \mathbb{Z}/21\mathbb{Z}$, $H = \{[0], [7], [14]\}$

$K = \{[0], [3], [6], [9], [12], [15], [18]\}$,

we want to prove $\mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

$\Leftrightarrow$ prove G is an internal direct product of H, K.

① $H \cdot K = \{hk \mid h \in H, k \in K\} = \mathbb{Z}/21\mathbb{Z}$.

② $H \cap K = \mathbb{Z}/3\mathbb{Z} \cap \mathbb{Z}/7\mathbb{Z} = [0] = e$

③ $\forall h \in H, k \in K, h \cdot k = k \cdot h$

$\therefore HK$ is an internal product of G. ∎

$\therefore \mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

Problem: 3: Groups

Let $G = S_4$, the symmetric group on 4 elements, and let $X = \mathcal{P}_2(\{1,2,3,4\})$, the set of all unordered 2-element subsets of $\{1,2,3,4\}$. G acts on X by permuting the elements of $\{1,2,3,4\}$, i.e., for $\sigma \in G$ and $A = \{a,b\} \in X$, the action is defined as:

$$\sigma \cdot A = \{\sigma(a), \sigma(b)\}.$$

(a) Compute the orbit of $\{1,2\}$ and the stabilizer subgroup $G_{\{1,2\}}$ under the action of G. Verify the Orbit-Stabilizer Theorem.

(b) Compute the number of distinct orbits of G on X.

(c) Let G act on the set $Y = \mathcal{P}_3(\{1,2,3,4\})$, the set of all unordered 3-element subsets of $\{1,2,3,4\}$, by the same rule. Compute the number of distinct orbits of G on Y. Then, generalize the result to $\mathcal{P}_k(\{1,2,\ldots,n\})$, the set of all unordered k-element subsets of $\{1,2,\ldots,n\}$, where $G = S_n$.

(a) orbit of $\{1,2\}$: $\{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$.

stabilizer of $\{1,2\}$: $\{e, (34), (12), (12)(34)\}$

$\therefore |Orb_G\{1,2\}| = 6 \quad |Stab_G\{1,2\}| = 4 \quad |G| = |S_4| = 24$

$\therefore |G| = |Orb_G\{1,2\}||Stab_G\{1,2\}| = 24$, which exactly matches the orbit-stabilizer theorem.

(b) Number of orbits in G: $\frac{1}{|G|}\sum_{g\in G}|X_g|$ according to Burnside's Lemma

$\therefore \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{24}\cdot(\ )$

① $g = e \quad |X_g| = 6$

② g = 2-cycle if $g = (12), (34) \quad |X_g| = 6$

else $|X_g| = 0$

③ g = 3-cycle. $|X_g| = 0$

④ g = 2-2-cycle. if $g = (12)(34)$, $|X_g| = 6$

else $|X_g| = 0$

⑤ g = 4-cycle $|X_g| = 0$

$\therefore \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{24}(6+2\times 6+6) = 1$

(C) $Y = \{\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}\}$,

① $g = e$. $|X_g| = 4$

② g = 2-cycle. $|X_g| = 2$

③ g = 3-cycle. $|X_g| = 1$

④ else. $|X_g| = 0$

$\therefore \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{24}(1\times 4+6\times 2+8\times 1) = 1$

when it comes to $G = S_n$ acts on $D_k\{1,2,\cdots n\}$.

# of distinct orbits is 1

Problem: 4: Rings

Let R be a ring, I is a subset of R,i.e. $I \subset R$.

(a) let R be a commutative ring with 1_R, and a, b, $1-ab$ are units of R. Show that $a-b^{-1}$, $(a-b^{-1})^{-1}-a^{-1}$ are also units.

(b) Let $R = \mathbb{Z}[x]$, $I = \langle 1+x \rangle$, determine whether I is a prime ideal in $\mathbb{Z}[i]$. Prove all claims.

(c) Prove that $R^* = R$ implies that $|R| = 1$.

(a) $\because a, b, 1-ab$ are units

$\therefore a^{-1}, b^{-1}, (1-ab)^{-1} = \frac{1}{1-ab} \in R$

$\therefore (a-b^{-1})^{-1} = \frac{1}{a-b^{-1}} = \frac{b}{ab-1} = \frac{-b}{1-ab} \in R.$

$(a-b^{-1})^{-1} - a^{-1} = \frac{1}{a-b^{-1}} - \frac{1}{a} = \frac{1}{ab-1} - \frac{1}{a} = -\frac{1}{1-ab} - \frac{1}{a} \in R$

$\therefore (a-b^{-1})^{-1}$ and $(a-b^{-1})^{-1} - a^{-1}$ are also units.

(b) consider $\mathbb{Z}[x]/\langle 1+x \rangle$

$\forall a+bx+\langle 1+x \rangle \in \mathbb{Z}[x]/\langle 1+x \rangle$

$a+bx = (1+x)b + (a-b)$

$\therefore a+bx+\langle 1+x \rangle = (1+x)b + (a-b) + \langle 1+x \rangle$

$= (a-b) + \langle 1+x \rangle$

$\therefore \forall xy + \langle 1+x \rangle \in \mathbb{Z}[x]/\langle 1+x \rangle.$

$x = a+bx+\langle 1+x \rangle$

$y = c+dx+\langle 1+x \rangle$

$xy = 0 \Rightarrow (a+b+\langle 1+x \rangle)(c+di+\langle 1+x \rangle)$

$= (ac+bd) + (ad+bc)x + \langle 1+x \rangle$

$= (ac+bd) + (ad+bc)x - (ad+bc)(1+x) + \langle 1+x \rangle$

$= (ac+bd-ad-bc)+\langle 1+x\rangle$

$\therefore \quad a(c-b)-b(c-d)=0$ identi

$\therefore (a-b)(c-d)=0$

$\therefore a=b$ or $c=d$.

$\therefore x=0$ or $y=0 \Rightarrow \langle 1+x\rangle$ is a prime ideal.

$R^\times = R$

R^*

$\mathbb{Z}/9\mathbb{Z} = \{[0]$ (*) $[1]$ $[2]$ $[3]$ $[4]$ $[5]$ $[6]$ $[7]$ $[8]\}$

$[2]*[5]=[0]=[1]$

(c) claim : $0_R = 0_R \cdot a \quad \forall a \in R$.

$\because 0_R \cdot a = (0_R + 0_R)\cdot a$

$\therefore 0_R \cdot a + 0_R = 0_R \cdot a + 0_R \cdot a \Rightarrow 0_R = 0_R \cdot a$

claim proved.

$\mathbb{Z}/9\mathbb{Z}^* = \{[1][2][4][5][7][8]\}$

identity $\in R$

unit $\in R$.

$\because R^\times = R$

$\therefore \exists\, b \in R$ s.t. $0_R = 0_R \cdot b = 1_R$.

$\therefore 0_R = 1_R$

$0_R \in R$

$1_R \in R$

$\therefore \forall a \in R$

$0_R = 0_R \cdot a = 1_R \cdot a = a$

$\therefore \forall a \in R,\ a = 0_R \Rightarrow |R| = 1$

$0_R \cdot b = 0_R = 1_R \cdot 0_R$

$\exists\, c$ s.t. $0_R \cdot c = 1_R$

Problem: 5: Ideals

(a) Is the ideal $(x^4-1, x^5-x^3) \subset \mathbb{Q}[x]$ maximal? Be sure to carefully justify your answer.

(b) Let I be an ideal of R, which is a commutative ring with 1_R.
Prove that $\sqrt{I} = \{r \in R | \exists n \geq 1, \text{s.t.} \quad r^n \in I\}$ is also an ideal of R.

(c) Consider $\mathbb{Z}[x]$ and $I = \langle x^2-1 \rangle$. Prove that $\mathbb{Z}[x]/I \cong \mathbb{Z} \times \mathbb{Z}$.

(d) Consider the ring $\mathbb{Z}[\sqrt{-5}]$. Show that $\langle 3 \rangle = \langle 3, 1+n\sqrt{-5} \rangle \langle 3, 1-n\sqrt{-5} \rangle$ if and only if n is not a multiple of 3.

(a) it is not maximal

$(x^4-1, x^5-x^3) = ((x^2-1)(x^2+1), (x^2-1)x^3)$

$= (x^2-1) \subsetneq (x-1) \lhd \mathbb{Q}[x]$

∴ not maximal

(b) ① $\forall r_1 \in \sqrt{I}, r_2 \in \sqrt{I}$.

$\exists n_1, n_2 \geq 1$. $r_1^{n_1} \in I$. $r_2^{n_2} \in I$

$\therefore (r_1+r_2)^{n_1+n_2} = \sum_{i=0}^{n_1+n_2} \binom{n_1+n_2}{i} r_1^i r_2^{n_1+n_2-i}$

$r_1 + r_2 = r \in \sqrt{I}$

$\exists n \; r^n \in I$

$i \leq n_1$

∴ whether $i \geq n_1$ or $n_1+n_2-i \geq n_2$

$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$

1° $i \geq n_1$

$r_1^i = r_1^{n_1+(i-n_1)} \in \sqrt{I}$

$\therefore r_1^i r_2^{n_1+n_2-i} = r_1^{n_1} \cdot (r_1^{i-n_1} r_2^{n_1+n_2-i}) \in \sqrt{I}$.

$\in R$

2° $n_1+n_2-i \geq n_2$

$\therefore r_2^{n_1+n_2-i} = r_2^{n_2} r_2^{n_1-i}$

$\in R$

$\therefore r_1^i r_2^{n_1+n_2-i} = r_2^{n_2}(r_1^i \cdot r_2^{n_1-i}) \in \sqrt{I}$

$\therefore r_1 + r_2 \in I$.

② $\forall r \in \sqrt{I}$. i.e. $\exists n$. s.t. $r^n \in I$.

$\forall x \in R, \quad (r \cdot x)^n = r^n x^n \in I \Rightarrow r \cdot x \in \sqrt{I}$

(c) $\mathbb{Z}[x]/I = \mathbb{Z}[x]/\langle x^2-1\rangle$

$\forall [f_1(x)], [f_2(x)] \in \mathbb{Z}[x]/\langle x^2-1\rangle$

$f_1(x) \equiv f_2(x) \pmod{x^2-1}$

$\because x^2-1 \equiv 0 \pmod{x^2-1}$

$\therefore x^2 \equiv 1 \pmod{x^2-1} \Rightarrow \mathbb{Z}[x]/I \cong \{ax+b \mid a,b \in \mathbb{Z}\} \cong \mathbb{Z}\times\mathbb{Z}$

$ax+b$

$\mathbb{Z} \times \mathbb{Z}$

(d) we want to prove $\langle 3\rangle = \langle 3, 1+n\sqrt{-5}\rangle \langle 3, 1-n\sqrt{-5}\rangle$

$\Leftrightarrow$ prove $\langle 3\rangle = \langle 9, 1+5n^2, 3+3n\sqrt{-5}, 3-3n\sqrt{-5}\rangle$

1° $9-(3-3n\sqrt{-5})-(3+3n\sqrt{-5})=3$

$\therefore 3 \in \langle 9, 1+5n^2, 3+3n\sqrt{-5}, 3-3n\sqrt{-5}\rangle$

$\therefore \langle 3\rangle \subseteq \langle 9, 1+5n^2, 3+3n\sqrt{-5}, 3-3n\sqrt{-5}\rangle$

2° $9 = 3\cdot 3$

$3+3n\sqrt{-5} = 3\cdot(1+n\sqrt{-5})$

$3-3n\sqrt{-5} = 3\cdot(1-n\sqrt{-5})$

$\therefore \Leftrightarrow$ prove $3 \mid 1+5n^2$

when $n=3k$ (multiple of 3)

$1+5n^2 = 1+5\cdot(3k)^2 \Rightarrow 3 \nmid 1+5n^2$

when $n=3k+1$

$1+5n^2 = 1+5(3k+1)^2 = 6+45k^2+30k \Rightarrow 3 \mid 1+5n^2$

when $n=3k+2$

$1+5n^2 = 1+5(3k+2)^2 = 21+45k^2+60k \Rightarrow 3 \mid 1+5n^2$

$\therefore \langle 3\rangle = \langle 3, 1+n\sqrt{-5}\rangle\langle 3, 1-n\sqrt{-5}\rangle$ iff $3 \mid n$

Problem: 6:Fields

Let $F = \mathbb{Q}$, the field of rational numbers, and let $\alpha = \sqrt{2} + \sqrt{3}$.

(a) Find the minimal polynomial $f(x)$ of element α s.t. $f(\alpha) = 0$ over F. What if $F = \mathbb{Q}(\sqrt{2})$? What if $F = \mathbb{Q}(\sqrt{6})$?

(b) Prove that $\mathbb{Q}[x]/(f(x))$ is a field. Briefly explain why $(f(x))$ is a maximal ideal in $\mathbb{Q}[x]$.

(c) Briefly show that $Q[\alpha] \neq Q(\alpha)$. Based on this, prove that $\mathbb{Q}(\alpha)$ is a k-dimensional vector space over $\mathbb{Q}$. (You should write down the value of k)

(a) $x = \sqrt{2} + \sqrt{3}$ $\quad x^2 = 5 + 2\sqrt{6}$ $\quad [Q(\sqrt{2}+\sqrt{3}) : Q] = 4 : 1 = 4$.

$x^2 - 5 = 2\sqrt{6} \Rightarrow$ $\quad (x^2-5)^2 = 24$ $\quad \sqrt{2}\ \sqrt{3}\ \sqrt{6}$

$\therefore f(x) = x^4 - 10x^2 + 1$

if $F = Q(\sqrt{2})$ $\quad x = \sqrt{2} + \sqrt{5}$

$\therefore x - \sqrt{2} = \sqrt{3}$

$Q[\sqrt[3]{2}]$ $\quad a + b\sqrt[3]{2}$

$Q(\sqrt[3]{2}) = Q[\sqrt[3]{2}, \sqrt[3]{4}]$ $\quad a + b\sqrt[3]{2} + c\sqrt[3]{4}$

$\therefore (x - \sqrt{2})^2 = 3$

$\therefore f(x) = x^2 - 2\sqrt{2}x - 1$

if $F = Q(\sqrt{6})$ $\quad x = \sqrt{2} + \sqrt{3}$

$x^2 = 5 + 2\sqrt{6}$

$\therefore f(x) = x^2 - 5 - 2\sqrt{6}$

R/I is field

$\Leftrightarrow$ I is maximal

R/I is integral domain

$\Leftrightarrow$ I is prime.

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

$= Q(\sqrt{2}, \sqrt{3}, \sqrt{6})$

$= \{ a + b\sqrt{2} + (\sqrt{3} + d\sqrt{6}) \}$

$\sqrt{2}$ $\quad \sqrt{3}$ $\quad \sqrt{6}$

(b) prove $Q[x]/(f(x))$ is a field

$\Leftrightarrow$ prove that $(f(x))$ is a maximal ideal of $Q[x]$.

assume $f(x)$ is not maximal

$\therefore \exists\, q(x)$ s.t. $f(x) = q(x)p(x)$

where $p(\alpha) = 0$.

$f(\alpha) = 0$

however. $\deg(p(x)) = \deg(f(x)) - \deg(q(x))$

$< \deg(f(x))$

which caused a contradiction that $f(x)$ is not the minimal polynomial

$\therefore$ $f(x)$ is a maximal ideal

$\therefore$ $\mathbb{Q}[x]/(f(x))$ is a field.

(c) $\mathbb{Q}[\alpha] = \{a+b(\sqrt{2}+\sqrt{3}) \mid a, b \in \mathbb{Q}\}$

$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$ $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$

$= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$

$\neq \{a+b(\sqrt{2}+\sqrt{6}) \mid a, b \in \mathbb{Q}\}$

(that is. $\sqrt{6} \in \mathbb{Q}(\alpha)$ but $\sqrt{6} \notin \mathbb{Q}[\alpha]$) $\sqrt[3]{2}$

$\therefore \mathbb{Q}(\alpha) \neq \mathbb{Q}[\alpha]$.

proof of vector space: $k = 4$.

(1) $\forall a, b \in \mathbb{Q}(\alpha)$ $a \cdot b = b \cdot a$, $a + b = b + a$

and $\mathbb{Q}(\alpha)$ is obviously a group

$\therefore$ $\mathbb{Q}(\alpha)$ is an abelian group

(2) Scalar multiplication

$\forall \lambda \in \mathbb{Q}(\alpha)$ $\quad \mathbb{Q} \times \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$

$(k, a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) \to$

$ka + kb\sqrt{2} + kc\sqrt{3} + kd\sqrt{6}$

$\therefore$ proved.

$Q(\sqrt[3]{2})$ $a+b\sqrt[3]{2}$

$Q(\sqrt[3]{2}) = Q(\sqrt[3]{2}, \sqrt[3]{4})$ $(\sqrt{2}+\sqrt{3})^2 = \sqrt{6}$

$\sqrt[3]{2}$ $\sqrt[3]{4}$ $\sqrt{2}$ $\sqrt{3}$ $\sqrt{6}$

$[Q(\sqrt{2}, \sqrt{3}, \sqrt{6}) : Q] = 4$

$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ $a + b\sqrt[3]{2} + c\sqrt[3]{4}$

a a

$Q(\sqrt[3]{2}) = Q(\sqrt[3]{2}, \sqrt[3]{4})$

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

$\sqrt{2}$ $\sqrt{3}$ $\sqrt{7}$

$a\sqrt{2} + b\sqrt{3} + c\sqrt{7} + d\sqrt{14}$ $\sqrt{a_2}$

$a, b, c, d \in Q$

$Q(\sqrt{2}+\sqrt{3}) =$

$Q(\sqrt{2}+\sqrt{3}+\sqrt{7})^3 \supset Q(\sqrt{2}, \sqrt{3}, \sqrt{7}, \sqrt{14}\sqrt{2}, \sqrt{42})$

$2^3 \cdot 7$

$(\sqrt{2}+\sqrt{3}+\sqrt{7})(\sqrt{2}+\sqrt{3}-\sqrt{7})(\sqrt{2}-\sqrt{3}+\sqrt{7})(\sqrt{2}-\sqrt{3}-\sqrt{7})$

$\sqrt{8} = 2\sqrt{2}$

$e_1 = \sqrt{2}$

$e_2 = \sqrt{3}$ $e_4 = \sqrt{7}$

$e_3 = \sqrt{7}$ $e_5 = \sqrt{14}$ $\sqrt{21}$

$Q(\sqrt{3}, \sqrt{5}, \sqrt{11})$