

Please read these instructions carefully before you begin the exam.

You are taking this exam under the honor system. Your signature at the bottom of this page is your promise to abide by the conditions described below. Breaking this promise violates Lewis and Clark's academic integrity policy and will result (at minimum) in a score of zero on this exam.

1. Do not write your name anywhere on your exam. Instead, write a code name or number on the upper-right hand corner of each page. At the bottom of this page of instructions, under your name and signature, write your code. This is to guarantee that I grade your exam objectively. Include this cover sheet as you upload your exam papers when you turn it in.
2. To answer these questions, use only the knowledge in your head, notes from class, old homework assignments and their solution keys, and the course text by Dummit and Foote. You can also use old notes and assignments from Math 421 last semester. Do not use information from the internet to solve these problems. If you have questions about this rule please contact me.
3. The procedures you use to tackle the problems must be carefully stated. The clarity of your answers will be as important as their correctness. A carefully and clearly written partial solution can be worth more than a complete solution which is disorganized and confusing.
4. This exam is due in Moodle by midnight on Friday, April 17.
5. Do not talk to or collaborate in any way with any other student, whether enrolled in Math 422 or not, whether they have already taken the exam or not, about these problems until Saturday, April 18. That includes: their difficulty, how long you worked on them, as well as any other exam-related topic you might imagine. Please take care to keep your write-ups and scratch work private so that others in the course don't encounter them.
6. Finally, do your best to think logically and clearly, and then trust your judgment. There are no "trick" questions here. Be sure to read the questions carefully, and ask me for clarification if necessary.

Your name and signature: Sean Richardson

Your code: Doerd (code can be anything, maybe your favorite movie character)

Start date and time: 05/15 at 10:00am End date and time: 07/15 at 11:00pm

Abstract Algebra II

Liz Stanhope

Midterm Exam 2

PJ. 1

Doord

① a)

claim: $\mathbb{Z}_{72} \times \mathbb{Z}_{72}$ is not isomorphic to \mathbb{Z}_{492} .

Proof: Assume for contradiction there is an isomorphism

$\mathbb{Z}_{72} \times \mathbb{Z}_{72} \cong \mathbb{Z}_{492}$ and let ϕ denote this

isomorphism class $\phi \in \mathbb{Z}_{72} \times \mathbb{Z}_{72} \cong \mathbb{Z}_{492}$.

Next, swap to multiplicative notation for convenience, so

$$\phi \in \mathbb{Z}_7 \times \mathbb{Z}_7 \cong \mathbb{Z}_{49}.$$

Next, note that the direct product of any group A with the trivial group does not change the isomorphism class of A . That is, $1 \times A \cong A$.

Indeed, an isomorphism $\psi: A \rightarrow 1 \times A$ is given by $\psi: \psi(a) \mapsto (1, a)$ which is a homomorphism by

$$\psi(ab) = (1, ab) = (1, a) \cdot (1, b) = \psi(a) \psi(b),$$

and injective by $\psi(a) = \psi(b)$ gives $(1, a) = (1, b)$ and so $a = b$. And surjective by any $x \in 1 \times A$ has the form $x = (1, a)$ and thus $\psi(a) = (1, a)$.

using Th. 3, we can write

$$\mathbb{Z}_7 \times \mathbb{Z}_7 \cong \mathbb{Z}^0 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \text{ and } \mathbb{Z}_{49} \cong \mathbb{Z}^0 \times \mathbb{Z}_{49}. \quad \boxed{\text{P.S. 2) Poerel}}$$

Further, by $\mathbb{Z}^0 \cong \mathbb{Z}$, this gives

$$G \cong \mathbb{Z}^0 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \text{ and } G \cong \mathbb{Z}^0 \times \mathbb{Z}_{49}.$$

And, observe that both of these representations
are in a form comparable with
 the Fundamental Theorem of Finitely Generated Abelian
 Groups (Theorem S.2.3).

Indeed, for $\mathbb{Z}^0 \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $0 \geq 0$, ~~and~~ $7 \geq 2$,
 and $7 \geq 1$.

Additionally, for $\mathbb{Z}^0 \times \mathbb{Z}_{49}$, $0 \geq 0$, and $49 \geq 2$.

Thus, both forms

$$G \cong \mathbb{Z}^0 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \text{ and } G \cong \mathbb{Z}^0 \times \mathbb{Z}_{49}$$

reinforce the uniqueness of promised in ~~the~~

Theorem S.2.3.

b) claim: Let A be an abelian group of order 392. Then A belongs to one of the following distinct isomorphism classes:

$$\mathbb{Z}_{392}, \mathbb{Z}_{196} \times \mathbb{Z}_2, \mathbb{Z}_{18} \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

$$\mathbb{Z}_{56} \times \mathbb{Z}_7, \mathbb{Z}_{28} \times \mathbb{Z}_{14}, \mathbb{Z}_{14} \times \mathbb{Z}_{14} \times \mathbb{Z}_2.$$

Proof: Each of the above isomorphism classes are written in the form such that the Fundamental Theorem of Finitely Generated Abelian Groups (Thm. S.2.3) promises that each of the above are distinct. However, it remains to show that ~~this~~ the list is complete.

For this, apply Theorem S.2.5 with the observation that $392 = 2^3 \cdot 7^2$. This theorem promises a complete list.

Theorem S.2.5 then promises that by $|A| = 2^3 \cdot 7^2$, $A \cong B \times C$ with $|B| = 2^3$ and $|C| = 7^2$.

Further, $B \cong \mathbb{Z}_{2^{P_1}} \times \dots \times \mathbb{Z}_{2^{P_r}}$ with $\sum P_i = 3$

and $C \cong \mathbb{Z}_{7^{N_1}} \times \dots \times \mathbb{Z}_{7^{N_s}}$ with $\sum N_j = 2$.

Next, note that the partitions of 3 are:

Pj. 4
Doord

$$\text{Thus } 1+1+1 = 2+1 = 3$$

and the partitions of 2 are:

$$1+1 = 2$$

Thus, B is isomorphic to one of the following:

$$B \cong \mathbb{Z}_2^3 \quad \text{OR} \quad B \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{OR} \quad B \cong \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1}$$

And C is isomorphic to one of the following:

$$C \cong \mathbb{Z}_7^2 \quad \text{OR} \quad C \cong \mathbb{Z}_{7^1} \times \mathbb{Z}_{7^1}$$

Then, recalling $A \cong B \times C$, A is isomorphic to one of the 6 classes:

$$A \cong (\mathbb{Z}_2^3) \times (\mathbb{Z}_7^2) \cong \mathbb{Z}_{392}$$

$$\text{OR } A \cong (\mathbb{Z}_2^3) \times (\mathbb{Z}_7 \times \mathbb{Z}_7) \cong \mathbb{Z}_{56} \times \mathbb{Z}_7$$

$$\text{OR } A \cong (\mathbb{Z}_2^2 \times \mathbb{Z}_2) \times (\mathbb{Z}_7^2) \cong \mathbb{Z}_{112} \times \mathbb{Z}_2$$

$$\text{OR } A \cong (\mathbb{Z}_2^2 \times \mathbb{Z}_2) \times (\mathbb{Z}_7 \times \mathbb{Z}_7) \cong \mathbb{Z}_{20} \times \mathbb{Z}_{14}$$

$$\text{OR } A \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_7^2) \cong \mathbb{Z}_{16} \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\text{OR } A \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_7 \times \mathbb{Z}_7) \cong \mathbb{Z}_{14} \times \mathbb{Z}_{14} \times \mathbb{Z}_2$$

where the second isomorphism in each line is given by Proposition 5.2.6, that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if $\gcd(m, n) = 1$.

c) Claim: If A is an abelian group of order 3^{12} and containing an element of order 196 ,
 then either $A \cong \mathbb{Z}_{3^{12}}$ or $A \cong \mathbb{Z}_{192} \times \mathbb{Z}_2$. Pj. \$
Doerfl

Proof: First, consider an arbitrary product $A_1 \times \dots \times A_n$ of groups, and take (x_1, \dots, x_n) .
~~Suppose~~ Then, let $L = \text{lcm}(|A_1|, \dots, |A_n|)$.
 I now show that $(x_1, \dots, x_n)^L = (1, \dots, 1)$.

For this, fix ~~an x_k and~~ an x_k and note
 $|x_k| \mid |A_k|$ by Corollary 3.2.9 and ~~hence~~
 $|A_k| \mid \text{lcm}(|A_1|, \dots, |A_n|)$ by definition of the least
 common multiple, thus $|x_k| \mid L$, which implies $x_k^L = 1$.

Then,
 $(x_1, \dots, x_n)^L = (x_1^L, \dots, x_n^L) = (1, \dots, 1)$ confirming
 claim.

In particular, note that for my (x_1, \dots, x_n) ,
 $|x_1, \dots, x_n| \leq L$.

Now, I compare L for the isomorphism classes
 listed in Part (b).

~~Part~~

GROUP(A_1, \dots, A_n)

$\lim(A_1, \dots, A_n)$

Pg. 6
Doord

$$\mathbb{Z}_{18} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \quad 98$$

$$\mathbb{Z}_{56} \times \mathbb{Z}_7 \quad 56$$

$$\mathbb{Z}_{28} \times \mathbb{Z}_{14} \quad 28$$

$$\mathbb{Z}_{14} \times \mathbb{Z}_{14} \times \mathbb{Z}_2 \quad 14$$

For each of the four groups listed above, the quantity L is strictly less than 112 and by $|(\chi_1, \dots, \chi_n)| \leq L$ for any element, none of the above classes ~~can~~ contain an element of degree 196.

This only leaves \mathbb{Z}_{392} and $\mathbb{Z}_{192} \times \mathbb{Z}_2$ from part (b) and I complete this proof with the observation that $x^2 \in \mathbb{Z}_{392}$ has order 196 and $(y, 1) \in \mathbb{Z}_{192} \times \mathbb{Z}_2$ (has order 196).
 x denotes the generator of \mathbb{Z}_{392} and y is the generator of \mathbb{Z}_{192} .

d) claim: Let $G = \mathbb{Z}_{492} \times \mathbb{Z}_{42} \times \mathbb{Z}_{22}$. Then pg. 7
Doerfl

$H = \{(0, 0, 0), (0, 7, 0)\}$ and $K = \{(0, 0, 0), (0, 0, 1)\}$
 are subgroups of G such that G/H and G/K
 are not isomorphic.

Proof: First, note that $K = \{(0, 0, n) \mid n \in \mathbb{Z}_{22}\}$
 and so Proposition S.1.2 promises that
 $K \cong \mathbb{Z}_{22}$ and thus is a subgroup of G . The
 same proposition gives that

$$G/K \cong \mathbb{Z}_{492} \times \mathbb{Z}_{42}.$$

Next, I first show H is indeed a subgroup by
 the two step subgroup criterion. First, $H \neq \emptyset$
 and next, take $h_1, h_2 \in H$ and consider $h_1 - h_2$.

~~If h_2 is odd, then $h_1 - h_2$ is even.~~

~~if h_1~~
 note h_1 and h_2 have the form $(0, 2n, 0)$ and
 everything of this form in H .

Then, for $h_1 - h_2 = (0, 2n, 0) - (0, 2m, 0) = (0, 2(n-m), 0)$
 which is in H , giving H a subgroup. Also, by
 #6 abelian, $H \trianglelefteq G$.

Now, assume for contradiction there is an isomorphism $\frac{G}{H} \cong \mathbb{Z}/k$. This implies there is

an isomorphism $\phi: \frac{G}{H} \rightarrow \frac{\mathbb{Z}}{492} \times \frac{\mathbb{Z}}{42}$.

Further, by H normal G/H forms a well-defined group with ~~addition~~ the operation defined by the

surjective homomorphism from representatives to equivalence classes $p: G \rightarrow \frac{G}{H}$. But then, the composition

$\phi \circ p: G \rightarrow \frac{\mathbb{Z}}{492} \times \frac{\mathbb{Z}}{42}$ is a surjective homomorphism.

Now, observe that $(0, 1) \in \frac{\mathbb{Z}}{492} \times \frac{\mathbb{Z}}{42}$ ~~is not~~

~~Since $\phi(p(g)) = \phi(g)$ is of order 4.~~

By $\phi \circ p$ surjective, there is an element $g \in G$ such that $(\phi \circ p)(g) = (0, 1)$. But then, $4g = 0$, so letting $g = (x, y, z)$, $4 \cdot (x, y, z) = (0, 0, 0)$. But, by $|x| \leq 49$ by ~~the~~ Corollary 3.2.9, $x=0$. ~~Additionally,~~ ~~g~~ This leaves $g = (0, y, z)$, but then $2 \cdot g = (0, 2y, 2z) = (0, 2y, 0)$, so $2 \cdot g \in H$. But then, $P(2g) = \text{Id}$, so $(\phi \circ p)(2g) = (0, 0)$. But recalling definition of g gives $2 \cdot (0, 1) = (0, 0)$, a contradiction.

$$\begin{array}{ccc} G & \xrightarrow{\phi \circ p} & \frac{\mathbb{Z}}{492} \times \frac{\mathbb{Z}}{42} \\ p \downarrow & & \swarrow \phi \\ G/H & & \end{array}$$

83.8

Doord

② Problems

Claim: If a group of prime order P acts on a finite set then the orbits of the action are either all of size 1 or P . $(P \text{ prime})$

Proof: Let G be a group of order P and let S be a finite set. Take my action $G \times S \rightarrow S$, let $a \in S$ and consider the orbit $O(a)$.

Recall that the stabilizer of a , G_a , forms a subgroup and the orbit-stabilizer theorem gives

$$|O(a)| = |G : G_a|. \text{ But, by Lagrange's Theorem, } |G_a| \mid |G|, \text{ and by } |G| = P \text{ for prime } P,$$

$$|G_a| = 1 \text{ or } |G_a| = P.$$

$$\text{Then, } |G : G_a| = \frac{|G|}{|G_a|} \text{ is either 1 or } P.$$

So, $|O(a)| = |G : G_a|$ is either 1 or P , confirming claim.

③ ~~Claim~~

Let G be a finite group and let p be a prime dividing $|G|$.

a) Claim: For $S = \{(x_1, \dots, x_p) : x_i \in G, \prod x_i = 1\}$.

Then S contains $|G|^{p-1}$ elements.

Proof: I claim the mapping $\varphi: G \times \dots \times G \rightarrow G$ given by $\varphi: (x_1, \dots, x_p) \mapsto \prod x_i$ is a surjective homomorphism. The homomorphism property follows from the following chain of equalities:

$$\begin{aligned} \varphi((x_1, \dots, x_p) \cdot (y_1, \dots, y_p)) &= \varphi((x_1 y_1, \dots, x_p y_p)) \\ &= \prod (x_i y_i) = (\prod x_i)(\prod y_i) = \varphi((x_1, \dots, x_p)) \cdot \varphi((y_1, \dots, y_p)). \end{aligned}$$

Surjective follows from

$$\varphi((g, 1, 1, \dots, 1)) = g \text{ for any } g \in G.$$

Note that $\ker \varphi = S$ by definition, and so by $\frac{G \times \dots \times G}{\ker \varphi} \cong G$, $\frac{G \times \dots \times G}{S} \cong G$. Then, note

$$\left| \frac{G \times \dots \times G}{S} \right| = \frac{|G \times \dots \times G|}{|S|} \text{ gives that}$$

$$|S| = \frac{|G \times \dots \times G|}{|G|} = \frac{|G|^p}{|G|} = |G|^{p-1}.$$

b) Claim: Take the cyclic group of order P , (B.11)
 $C_P = \langle g \rangle$ and let $\sigma \in S_P$ be the
Permutation $\sigma = (1 \ 2 \ \dots \ P-1 \ P)$. Then define
The map $C_P \times S \rightarrow S$ by
 $g^n \cdot (x_1, \dots, x_p) = (x_{\sigma^n(1)}, \dots, x_{\sigma^n(p)})$.

This map, as the notation suggests, is a group action.

Proof:

First note that by σ^n a permutation, and commutativity
of multiplication, the elements of the tank will still
multiply to 1.

Next, because an g^n is an element of the cyclic
group ~~can~~ must have multiple representations, well-defined
must be addressed.
So, assume $g^n = g^m$ and consider

$$g^n \cdot (x_1, \dots, x_p) = (x_{\sigma^n(1)}, \dots, x_{\sigma^n(p)})$$

$$\text{and } g^m \cdot (x_1, \dots, x_p) = (x_{\sigma^m(1)}, \dots, x_{\sigma^m(p)})$$

Then, note $(g^n(g^m)^{-1})^{-1} = 1 \Rightarrow g^{n-m} = 1$, so $n-m|P$.

But then, $\sigma^{n-m} = 1$ by $\sigma^P = 1$, so $\sigma^n = \sigma^m$,
confirming well-defined.

(B.12)
Doerfl

Next, note that

$$1. (x_1, \dots, x_p) = \underbrace{y^0(x_1, \dots, x_p)}_{=} = (x_{\sigma^0(1)}, \dots, x_{\sigma^0(p)}) =$$

$$= (x_1, \dots, x_p)$$

Additionally, for ~~$y^n, x^m \in C_p$~~ , $y^n, y^m \in C_p$,

~~$(y^n y^m) \cdot (x_1, \dots, x_p) =$~~

$$= y^{n+m} \cdot (x_1, \dots, x_p) = (x_{\sigma^{n+m}(1)}, \dots, x_{\sigma^{n+m}(p)})$$

$$= (x_{\sigma^{n+m}(1)}, \dots, x_{\sigma^{n+m}(p)})$$

$$= y^n \circ (x_{\sigma^m(1)}, \dots, x_{\sigma^m(p)}) = y^n \circ (y^m \cdot (x_1, \dots, x_p))$$

and thus we have a well-defined group struct.

c) Claim: There is an element in G of order p . B.13
Dated

Proof: Take the action $(P \curvearrowright S)$ as described in (b). Next, consider the orbit of $(1, 1, \dots, 1) \in S$.

Permuting the elements of $(1, 1, \dots, 1)$ will bring it back to itself as all the elements are the same. Thus, the orbit of $(1, \dots, 1)$ is of size 1.

Next, note that the sum of orbit sizes is the cardinality of S , for the orbits partition S .

That is, $\sum |\mathcal{O}_i| = |S|$.

Then, by problem 2, each orbit is of cardinality 1 or p (by $|C_G| = p$). So,

~~Also~~ $n \cdot 1 + m \cdot p = |S| = |G|^{p-1}$, where n is the number of orbits of cardinality 1 and m is the number of orbits of cardinality p .

Note that by $n = |G|^{p-1} - m \cdot p$ and

$p \mid |G|$ gives $p \mid (|G|^{p-1} - m \cdot p)$, thus $p \mid n$.

Additionally, $n \geq 1$ by the orbit of $(1, 1, \dots, 1)$.

But $P \neq 1$ for any prime P , thus Pg. 14
Doerfl
 $n \geq n+1$.

Thus, There exists one other non-identity element $(x_1, x_2, \dots, x_p) \in S$ that has order 1.

However, taking $C_P = \langle y \rangle$, in order for

$y \cdot (x_1, \dots, x_p) = (x_2, x_3, \dots, x_p, x_1)$ to be equal to (x_1, x_2, \dots, x_p) , we must have $x_{1k} = x_{k+1}$ for each k and thus all the elements are equal.

But then, we get there is an element

$(x, x, \dots, x) \in S$, meaning $\prod_i^P x = 1$, or $x^P = 1$.

Finally, ~~Assume~~ assume for contradiction ~~that~~ ~~for~~ ~~by the~~ ~~order~~ ~~of~~ ~~the~~ ~~Theorem~~ that x has order $n < P$. Then,

$P = nr + r$ for $r < n$. And, $n \neq 1$ by (x, x, \dots, x) non-identity, so $n \neq P$, meaning $0 < r < n$. But then $x^r = x^{P-n} = 1$, contradicting definition of order and confirming x has order P .

15
Doord

④ Claim: The lists $3+2+5, 1+2+3+4,$
 and $2+2+2+2+2$ could NOT appear on the
 right hand side of the class equation, while
 $1+2+2+2+5$ could.

Proof:

Recall the class equation:

$$|G| = |\mathcal{C}(G)| + \sum_{i=1}^n |G : C_G(g_i)|$$

for j_1, j_2, \dots, j_n distinct non-central representatives of
 conjugacy classes.

By $\mathcal{C}(G)$ a ~~subgroup~~, Lagrange's theorem
 gives $|\mathcal{C}(G)| \mid |G|$. Further, by $C_G(g_i)$ a
 subgroup, $|C_G(g_i)| \mid |G|$, thus $|C_G(g_i)| \cdot k = |G|$
 for some integer k . ~~But then~~ note $k \mid |G|$.

But then,

$$|G : C_G(g_i)| = \frac{|G|}{|C_G(g_i)|} = \frac{k \cdot \cancel{|C_G(g_i)|}}{\cancel{|C_G(g_i)|}} = k.$$

Thus, $|G : C_G(g_i)| \mid |G|$. to

Thus, every ~~number~~ number in the class equation must divide 16. But then,

if $|G| = 3+2+5$ appears in the class equation, then $|G|=10$, but 3×10 , ruling out the sequence $3+2+5$.

Similarly, if $|G|=1+2+3+4$, then $|G|=10$ and again 3×10 , ruling out the sequence $1+2+3+4$.

Next, I show that the sequence $1+2+2+5$ can appear on the right hand side of the class equation. To see this, consider the sequence ~~of~~ group D_{10} , and note the following composition of conjugacy classes:

$$\left\{ \{1\}, \{r, r^4\}, \{r^2, r^3\}, \{s, sr, sr^2, sr^3, sr^4\} \right\}.$$

Note that $Z(D_{10}) = \{1\}$, and take representatives of the non-central conjugacy classes to be $\{r, r^2, s\}$. Then, by the orbit-stabilizer theorem,

| 83. 17
Doord

$$2 = |\mathcal{O}(r)| = |G : C_G(r)|,$$

$$2 = |\mathcal{O}(r^2)| = |G : C_G(r^2)|, \text{ and}$$

$$5 = |\mathcal{O}(s)| = |G : C_G(s)|.$$

Thus, this gives the sequence

$$|\mathcal{Z}(G)| + |G : C_G(r)| + |G : C_G(r^2)| + |G : C_G(s)|$$

$$= 1 + 2 + 2 + 5.$$

~~2+2+2+2~~

It remains to show that the sequence
 $2+2+2+2+2$ is not possible. For this, note
that $|\mathcal{Z}(G)| = 2$ and there are four
conjugacy classes, each of ~~the~~ order 2.

These conjugacy classes partition G , so there
are 8 elements belonging to conjugacy classes of
order 2. But then, ~~by the orbit-stabilizer~~
theorem take $x \in G$ to be one of these 8
non-central elements.

It then follows that

$$2 = |\mathcal{O}(x)| = |G : C_G(x)| = \frac{|G|}{|C_G(x)|} = \frac{10}{|C_G(x)|},$$

and so $|C_G(x)| = 5$.

Further, by $x \cdot x = x x x^{-1} = x$, $x \in C_G(x)$
and so x is an element of an order 5 subgroup.

But, by Corollary 3.2.9, $|x| \mid |C_G(x)|$, so

$|x| \mid 5$, and so $|x|=1$ or $|x|=5$, but by

x non-central, $|x|=5$.

Then, this holds for each non-central x , so
there are 3 elements of G with order 5;

and each belongs to a subgroup of order 5.

However, not all of them can belong to
the same subgroup of order 5, for these

3 elements are distinct. Thus, there are

at least 2 subgroups of order 5.

Next, I claim that these 2 subgroups ~~to~~
only have intersection at the identity.

For this, ~~those~~ denote the two subgroups of order 5 to be K and H . P.D. 19
Done

By Corollary 3.2.10, both K and H are cyclic. Next, assume $x \in K \cap H$ for a non-identity element x . Then, take the subgroup $\langle x \rangle \leq K$ and note Corollary 2.2 gives $|x| = |\langle x \rangle|$, so $|\langle x \rangle| = |x| = 5 = |K|$, so $\langle x \rangle = K$ and similarly $\langle x \rangle = H$, but then $H = K$, contradicting H, K distinct and

thus $H \cap K = \{1\}$.

But then, by Proposition 3.2.13, the set $HK \subseteq G$ has cardinality

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{5 \cdot 5}{1} = 25, \text{ contradicting}$$

$|HK| \leq 6$ and thus we have our contradiction, so the sequence $2+2+2+2+2 \rightarrow$ impossible.

⑤ Claim: Take extension of fields P. 20
Board

E/F . Then, suppose $f(x), g(x) \in F[x]$ are not both 0. Let $d_F(x)$ be the gcd of $f(x)$ and $g(x)$ in $F[x]$, and let $d_E(x)$ be the gcd of $f(x)$ and $g(x)$ in $E[x]$. Then, $d_F(x) = d_E(x)$.

Proof: The strategy will be to show $d_F(x) | d_E(x)$ and $d_E(x) | d_F(x)$. First, note that $d_F(x) | f(x), g(x)$ and so $\frac{f(x) \cdot a(x)}{d_F(x)} =$ $d_F(x) \cdot a(x) = f(x)$ and $d_F(x) \cdot b(x) = g(x)$ for $a(x), b(x) \in F[x]$. But by E/F , $a(x), b(x) \in E[x]$ and thus $d_F(x) | f(x), g(x)$ from the perspective of $E[x]$ and by definition of gcd, we then get ~~$d_F(x) | d_E(x)$~~ . $d_F(x) | d_E(x)$.

Next, for the other direction, apply the gcd theorem, which promises the existence of ~~$a(x), b(x)$~~ $a(x), b(x) \in F[x]$ such that $a(x)f(x) + b(x)g(x) = d_F(x)$. But then by

definition of \mathcal{J} and by viewing
 all a, b, f, g as elements of $E[x]$, the ~~get~~
 it follows ~~from~~ $d_F(x) \mid f(x)$ and $d_F(x) \mid g(x)$.

But this gives $d_F(x) \mid (a(x)f(x) + b(x)g(x))$ and
 Thus $d_F(x) \mid d_E(x)$.

So, we have $d_F(x) \mid d_E(x)$ and $d_E(x) \mid d_F(x)$,

so thus $d_F(x) = d_E(x) f(x)$ and
 $d_E(x) = d_F(x) g(x)$ for

$f(x), g(x) \in E[x]$. But then

$d_F(x) = f(x)g(x)d_F(x)$, so $f(x)g(x) = 1$, giving
 $f(x) \mid 1$ and $g(x) \mid 1$, thus

$d_F(x) = d_E(x) f(x)$ gives that $d_E(x)$ and
 $d_F(x)$ are equivalent up to associates.

⑥ Claim: A is not a finite extension of \mathbb{Q} . Pg. 22
Doord

Proof: Assume for the purpose of contradiction that A is a finite extension of \mathbb{Q} .

Then there is a basis $\{b_1, b_2, \dots, b_n\} \subseteq A$ over field \mathbb{Q} , so $[A : \mathbb{Q}] = n$

Next, consider the polynomial ~~$x^n - 2$~~ $x^{n+1} - 2$.

By 210, 2x1, 2x2, Eisenstein's irreducibility criterion applies and thus $x^{n+1} - 2$

is irreducible over \mathbb{Q} .

Next, consider the extension field $\mathbb{Q}(\sqrt[n+1]{2})$ and observe $\sqrt[n+1]{2}$ is a root of $x^{n+1} - 2$

over $\mathbb{Q}(\sqrt[n+1]{2})$: $(\sqrt[n+1]{2})^{n+1} - 2 = 2 - 2 = 0$.

Then, Corollary 4.15 in the Galois Notes gives

that $\{1, \sqrt[n+1]{2}, \sqrt[n+1]{2^2}, \dots, \sqrt[n+1]{2^n}\}$ form a basis

for $\mathbb{Q}(\sqrt[n+1]{2})$ as a vector space over \mathbb{Q} .

But this implies that

$\{1, \sqrt[^{n+1}]{2}, \sqrt[^{n+1}]{2^2}, \dots, \sqrt[^{n+1}]{2^n}\}$ are a linearly independent

Set. ~~and then~~ further, each $\sqrt[^{n+1}]{2^k}$ is algebraic, for it is the root of the polynomial $x - 2^k$.

But then, ~~we have in the basis~~ ^{This} demonstrates $n+1$ linearly independent vectors ~~in~~ over \mathbb{Q} with each vector in A .

This contradicts that A is dimension n over \mathbb{Q} .