Abstract Algebra II

Midterm Exam 2

Doerd

Sp: Stanhope

① a) Claim: $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/49\mathbb{Z}$.

Proof: Assume for contradiction there is an isomorphism $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/49\mathbb{Z}$ and let G denote this isomorphism class $G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/49\mathbb{Z}$.

Next, swap to multiplicative notation for convenience, so

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

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 $\varphi : A \to 1 \times A$ is given by $\varphi : a \mapsto (1, a)$ which is a homomorphism by

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

and injective by $\varphi(a) = \varphi(b)$ 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 $\varphi(a) = (1, a)$.

using this, we can write

$\mathbb{Z}_7 \times \mathbb{Z}_7 \cong 1 \times \mathbb{Z}_7 \times \mathbb{Z}_7$ and $\mathbb{Z}_{49} \cong 1 \times \mathbb{Z}_{49}$. Proved

Further, by $\mathbb{Z}^0 \cong 1$, this gives

$6 \cong \mathbb{Z}^0 \times \mathbb{Z}_7 \times \mathbb{Z}_7$ and $6 \cong \mathbb{Z}^0 \times \mathbb{Z}_{49}$.

And, observe that both of these representations are in a form comparable with the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 5.2.3).

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

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

Thus, both forms

$$6 \cong \mathbb{Z}^0 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \text{ and } 6 \cong \mathbb{Z}^0 \times \mathbb{Z}_{49}$$

satisfies the uniqueness promised in Theorem 5.2.3.

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

$$\mathbb{Z}_{392},\ \mathbb{Z}_{196}\times\mathbb{Z}_2,\ \mathbb{Z}_{98}\times\mathbb{Z}_2\times\mathbb{Z}_2,$$

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

Proof: Each of the above isomorphism classes are written in the form such that the Fundamental Theorem of Finitely Generated Abelian Groups (Thm. 5.2.3) promises that each of the above are distinct. However, it remains to show that ~~this~~ the list is complete.

For this, apply Theorem 5.2.5 with the observation that $392 = 2^3\cdot 7^2$. This theorem promises a complete list.

~~This Theorem then~~ Theorem 5.2.5 then promises that by $|A| = 2^3\cdot 7^2$, $A \cong B\times C$ with $|B| = 2^3$ and $|C| = 7^2$.

Further, $B \cong \mathbb{Z}_{2^{\beta_1}}\times\cdots\times\mathbb{Z}_{2^{\beta_T}}$ with $\sum B_i = 3$

and $C \cong \mathbb{Z}_{7^{\alpha_1}}\times\cdots\times\mathbb{Z}_{7^{\alpha_S}}$ with $\sum \alpha_s = 2$.

Next, note that the partitions of 3 are:

$1+1+1 = 2+1 = 3$

and the partitions of 2 are:

$1+1 = 2$

Thus, B is isomorphic to one of the following:

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

And C is isomorphic to one of the following:

$C \cong \mathbb{Z}_{7^2}$ OR $C \cong \mathbb{Z}_{7^1} \times \mathbb{Z}_{7^1}$.

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

$$A \cong (\mathbb{Z}_{2^3}) \times (\mathbb{Z}_{7^2}) \cong \mathbb{Z}_{392}$$

OR $A \cong (\mathbb{Z}_{2^3}) \times (\mathbb{Z}_7 \times \mathbb{Z}_7) \cong \mathbb{Z}_{56} \times \mathbb{Z}_7$

OR $A \cong (\mathbb{Z}_{2^2} \times \mathbb{Z}_2) \times (\mathbb{Z}_{7^2}) \cong \mathbb{Z}_{196} \times \mathbb{Z}_2$

OR $A \cong (\mathbb{Z}_{2^2} \times \mathbb{Z}_2) \times (\mathbb{Z}_7 \times \mathbb{Z}_7) \cong \mathbb{Z}_{28} \times \mathbb{Z}_{14}$

OR $A \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_{7^2}) \cong \mathbb{Z}_{98} \times \mathbb{Z}_2 \times \mathbb{Z}_2$

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

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 392 and containing an element of order 196, then either $A \cong \mathbb{Z}_{392}$ or $A \cong \mathbb{Z}_{196} \times \mathbb{Z}_2$.

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

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

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

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

Now, I compute L for the isomorphism classes listed in part (b).

GROUP $(A_1 \times \cdots \times A_n)$	$lcm(\lvert A_1 \rvert, \ldots, \lvert A_n \rvert)$
$\mathbb{Z}_{18} \times \mathbb{Z}_2 \times \mathbb{Z}_2$	98
$\mathbb{Z}_{56} \times \mathbb{Z}_7$	56
$\mathbb{Z}_{28} \times \mathbb{Z}_{14}$	28
$\mathbb{Z}_{14} \times \mathbb{Z}_{14} \times \mathbb{Z}_2$	14

For each of the four groups listed above, the quantity L is strictly less than 196 and by $|(x_1, \ldots, x_n)| \leq L$ for any element, none of the above classes can contain an element of degree 196.

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

d) Claim: Let $G = \mathbb{Z}/4\mathbb{Z} * \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then

* $H = \{(0,0,0), (0,2,0)\}$ 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 $K = \{(0,0,n) \mid n \in \mathbb{Z}/2\mathbb{Z}\}$ and so Proposition 5.1.2 promises that $K \cong \mathbb{Z}/2\mathbb{Z}$ and thus is a subgroup of G. The same proposition gives that

$$G/K \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

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 identity, we get $h_1 - h_2 = h_1$ trivially.~~

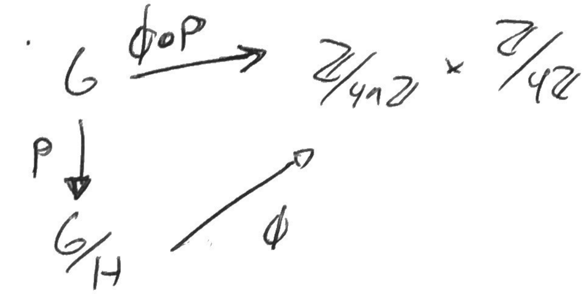
~~If h_1~~

Note h_1 and h_2 have the form $(0, 2n, 0)$ and everything of this form is in H.

Then, $h_1 - h_2 = (0, 2n_1, 0) - (0, 2n_2, 0) = (0, 2(n_1 - n_2), 0)$ which is in H, giving H a subgroup. Also, by G abelian, $H \trianglelefteq G$.

Now, assume for contradiction there is an isomorphism $G/H \cong G/K$. This implies there is an isomorphism $\phi : G/H \to \mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

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 $p: G \to G/H$. But then, the composition $\phi \circ p : G \to \mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is a surjective homomorphism.



Now, observe that $(0, 1) \in \mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ~~is of~~ ~~Satisfies $4 \cdot (0,1) = (0,0)$. By~~ 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, $4 \cdot g = 0$, so letting $g = (x, y, z)$, $4 \cdot (x, y, z) = (0, 0, 0)$. But, by $|x| \mid 49$ by ~~theorem~~ 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 $2g \in H$. But then, $p(2g) = Id$, so $(\phi \circ p)(2g) = (0,0)$ ~~so 2~~. But recalling definition of g gives $2 \cdot (0, 1) = (0, 0)$, a contradiction.

(2) Problem 2:

Claim: If a group of prime order p acts on a finite set the orbits of the action are either of size 1 or p. (prime)

Proof: Let G be a group of order p and let S be a finite set. Take any action $G \times S \to S$, let $a \in S$ and consider the orbit $\mathcal{O}(a)$. Recall that the stabilizer of a, G_a, forms a subgroup and the orbit-stabilizer Theorem gives $|\mathcal{O}(a)| = |G : G_a|$. But, by Lagranges Theorem, $|G_a| \mid |G|$, and by $|G| = p$ for prime p, $|G_a| = 1$ or $|G_a| = p$.

Then, $|G : G_a| = \dfrac{|G|}{|G_a|}$ is either 1 or p.

So, $|\mathcal{O}(a)| = |G : G_a|$ is either 1 or p, confirming claim.

(3) ~~a) Claim~~

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

a) Claim: Let $S = \{(x_1, \ldots, x_p) : x_i \in G, \prod x_k = 1\}$. Then S contains $|G|^{p-1}$ elements.

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

$$\varphi((x_1, \ldots, x_p) \cdot (y_1, \ldots, y_p)) = \varphi((x_1 y_1, \ldots, x_p y_p))$$

$$= \prod (x_k y_k) = \left(\prod x_k\right)\left(\prod y_k\right) = \varphi((x_1, \ldots, x_p)) \cdot \varphi((y_1, \ldots, y_p)).$$

Surjective follows from

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

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

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

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

b) Claim: Take the cyclic group of order p, $C_p = \langle g \rangle$ and let $\sigma \in S_p$ be the permutation $\sigma = (1\ 2\ \dots\ p-1\ p)$. Then define the map $C_p \times S \to S$ 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 tuple will still multiply to 1.

Next, because an element of the cyclic group can have multiple representations, well-definedness must be addressed.

So, assume $g^n = g^m$ and consider

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

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

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

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

Next, note that

1. $(x_1,\dots,x_p) = \mathrm{id}^\circ(x_1,\dots,x_p) = (x_{\sigma^\circ(1)},\dots,x_{\sigma^\circ(p)}) =$ Done!

$= (x_1,\dots,x_p)$

Additionally, for ~~$\mathrm{id}^n, \mathrm{id}^m \in C_p$~~, $\mathrm{id}^n, \mathrm{id}^m \in C_p$,

~~$(\mathrm{id}^n \mathrm{id}^m).(x_1,\dots,x_p)$~~ $(\mathrm{id}^n \mathrm{id}^m).(x_1,\dots,x_p) =$

$= \mathrm{id}^{n+m}.(x_1,\dots,x_p) = (x_{\sigma^{n+m}(1)},\dots,\sigma^{n+m}(p))$

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

$= \mathrm{id}^m.(x_{\sigma^m(1)},\dots,x_{\sigma^m(1)}) = \mathrm{id}^n.(\mathrm{id}^m.(x_1,\dots,x_n))$

and thus we have a well-defined group action.

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

Proof: Take the action $C_p \curvearrowright S$ as described in (b). Next, consider the orbit of $(1,1,\ldots,1) \in S$. Permuting the elements of $(1,1,\ldots,1)$ will bring it back to itself as all the elements are the same. Thus, the orbit of $(1,\ldots,1)$ is of size 1.

Next, note that the sum of orbit sizes is the cardinality of S, for the orbits partition S. That is, $\sum_i |O_i| = |S|$.

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

$n \cdot 1 + m \cdot p = |S| = |G|^{p-1}$, 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 $(1,1,\ldots 1)$

But $p \neq 1$ for any prime p, thus n is at least 2.

Thus, there exists one other ~~element~~ non-identity element $(x_1, x_2, \ldots, x_p) \in S$ that has orbit 1.

However, taking $C_p = \langle g \rangle$, in order for $g \cdot (x_1, \ldots, x_p) = (x_2, x_3, \ldots, x_p, x_1)$ to be equal to $(x_1, x_2, \ldots, x_p)$, we must have $x_k = x_{k+1}$ for each k and thus all the elements are equal.

But then, we get there is an element $(x, x, \ldots, x) \in S$, meaning $\prod_i^p x = 1$, or $x^p = 1$.

Finally, ~~[illegible]~~ assume for contradiction ~~[illegible]~~ that x has order $n < p$. Then, $p = nq + r$ for $r < n$. And, $n \neq 1$ by $(x, x, \ldots, x)$ non-identity, so $n \nmid p$, meaning $0 < r < n$. But then $x^r = x^{p-nq} = 1$, contradicting definition of order and confirming x has order p.

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 $1+2+3+5$ could.

Proof:

Recall the class equation:

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

for k distinct non-central representatives of conjug acy classes.

By $Z(G)$ a subgroup, Lagranges Theorem gives $|Z(G)| \mid |G|$. 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,

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

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

$\square$

Thus, every number in the class equation must divide $|G|$. But then, if $|G| = 3+2+5$ appears in the class equation, then $|G| = 10$, but $3 \nmid 10$, ruling out the sequence $3+2+5$.

Similarly, if $|G| = 1+2+3+4$, then $|G| = 10$ and again $3 \nmid 10$, 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 group D_{10} and note the following computation of conjugacy classes:

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

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,

03.17
Doerd

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

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

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

Thus, this gives the sequence

$$|Z(G)| + |G : C_G(r)| + |G : C_G(r^2)| + |G : C_G(s)|$$

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

~~[illegible]~~

It remains to show that the sequence $2+2+2+2+2$ is not possible. For this, note that $|Z(G)| = 2$ and there are four conjugacy classes, each of ~~[illegible]~~ order 2. These conjugacy classes partition G, so then these conjugacy classes belong to conjugacy classes of 8 elements 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

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

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

Further, by $x \cdot x = xxx^{-1} = x$, $x \in C_G(x)$

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, $|x| = 5$.

This holds for each non-central x, so

There are 8 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

8 elements are distinct. Thus, there are

at least 2 subgroups of order 5.

Next, I claim that these 2 subgroups

only have intersection of the identity.

For this, ~~note that~~ denote the two Doerd
subgroups of order 5 to be K and H.

By Corollary 3.2.10, both K and H are cyclic. Next, assume $x \in K \cap H$ for a non-identity element x_0. 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 $HK \leq G$ has cardinality

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{5 \cdot 5}{1} = 25,$$ contradicting $HK \leq G$ and thus we have our contradiction, so the sequence $2+2+2+2+2$ is impossible.

⑤ **Claim:** Take extension of fields 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 $d_F(x) \mid d_E(x)$ and $d_E(x) \mid d_F(x)$. First, note that $d_F(x) \mid f(x), g(x)$ and so ~~$f(x) \cdot a(x) =$~~ $d_F(x) \cdot a(x) = f(x)$ 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 $d_F(x) \mid f(x), g(x)$ from the perspective of $E[x]$ and by definition of gcd, we then get ~~$d_E(x)$~~ $d_F(x) \mid d_E(x)$.

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

definition of gcd and by viewing
our a, b, f, g as elements of $E[x]$, ~~we get~~ Doerd

it follows ~~from~~ That $d_F(x) \mid f(x)$ 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

$f(x), g(x) \in F[x]$. 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.

Doerd

(6) Claim: $\mathbb{A}$ is not a finite extension of $\mathbb{Q}$.

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

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

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

By $2 \mid 0$, $2 \nmid 1$, $2^2 \nmid 2$, & Eisenstein 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 $\{1, \sqrt[n+1]{2}, \sqrt[n+1]{2^2}, \ldots, \sqrt[n+1]{2^n}\}$ form a basis for $\mathbb{Q}(\sqrt[n+1]{2^n})$ as a vector space over $\mathbb{Q}$.

But this implies that

$\{1, \sqrt[n+1]{2}, \sqrt[n+1]{2^2}, \ldots, \sqrt[n+1]{2^n}\}$ are a linearly independent set. further, each $\sqrt[n+1]{2^k}$ is algebraic, for it is the root of the polynomial $x^{n+1} - 2^k$.

But then, this demonstrates $n+1$ linearly independent vectors over $\mathbb{Q}$ with each vector in A.

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