21-373 Final exam theorem list

- Two out of eight questions on the final exam will ask you to prove results that we proved in class. This document is about them.
- In proving the results you can use only results that precede it in the book/lectures. [For example, you cannot use the classification of finite abelian groups to prove Application 1 on page 61.]
- You must clearly state all the results that you use in your proof
- You can give any valid proof. You do not have to give the same proof as in the book or lectures.
- The proofs must contain all the details, including those that were left as exercises in the book or lecture.
- Below is a complete list of possible results that might appear on the final

1. (Lemma 2.3.1) Let G be a group. Then
   (a) The identity element of G is unique.
   (b) Every $a \in G$ has a unique inverse in G.
   (c) For every $a \in G$, we have $(a^{-1})^{-1} = a$.
   (d) For all $a, b \in G$, we have $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.
2. (Lemma 2.3.2) Let G be a group, and $a, b \in G$. Then the equation $a \cdot x = b$ has a unique solution in G.
3. (Lemma 2.4.1) A nonempty subset of the group G is a subgroup if and only if
   (a) $a, b \in H$ implies that $ab \in H$,
   (b) $a \in H$ implies that $a^{-1} \in H$.
4. (Lemma 2.4.2) If H is a nonempty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.
5. (Lemma 2.4.5 and Theorem 2.4.1) Let H be a subgroup of a group G.
   (a) There is a bijection between any two right cosets of H in G.
   (b) If G is a finite, then $o(H)$ divides $o(G)$.
6. (Corollary 1 on page 43) If G is a finite group and $a \in G$, then $o(a) \mid o(G)$.

7. (Corollary 5 on page 44) If G is a finite group whose order is a prime number p, then G is a cyclic group.

8. (Lemma 2.5.1) Let H, K be subgroups of a group G. Then HK is a subgroup G if and only if $HK = KH$.

9. (Theorem 2.5.1) Let H, K be fintie subgroups of a group G of orders $o(H)$ and $o(K)$. Then $o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$.

10. (Lemma 2.6.2) The subgroup N of G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

11. (Lemma 2.7.3) Let $G, \overline{G}$ be groups. If ϕ is a homomorphism of G into $\overline{G}$ with kernel K, then K is a normal subgroup of G.

12. (Theorem 2.7.1) Let $G, \overline{G}$ be groups. Let ϕ be a surjective homomorphism from G to $\overline{G}$ with kernel K. Then $G/K \approx \overline{G}$.

13. (Application 1 on page 61) Suppose G is a finite abelian group and $p \mid o(G)$, where p is a prime number. Then there is an element $a \neq e$ such that $a^p = e$.

14. (Lemma 2.8.2) $\mathcal{I}(G) \approx G/Z$, where $\mathcal{I}$ is the group of inner automorphisms of G, and Z is the center of G

15. (Theorem 2.9.1) Every group is isomorphic to a subgroup of $A(S)$ for some appropriate S.

16. (Pages 78-80)

    (a) Give a definition of an *even permutation*

    (b) Prove that the set of even permutations in S_n is an index-2 subgroup.

17. (Theorem 2.11.2) If G is a group, and $o(G) = p^n$ where p is a prime number, then $Z(G) \neq (e)$.

18. (Page 86) If $o(G) = p^2$ where p is a prime number, then G is abelian.

19. (Slightly easier form of Theorem 2.12.1) If G is a group, p is a prime number and $p^\alpha \mid o(G)$ and $p^{\alpha+1} \nmid o(G)$, then G has a subgroup of order p^α.

20. (The "only if" direction of Theorem 2.14.2) Let p be a prime number. Let G, G' be abelian groups of order p^n and $G = A_1 \times \cdots \times A_k$ and $G' = B_1 \times \cdots \times B_S$, where each A_i and B_i are cyclic of orders $o(A_i) = p^{n_i}$ and $o(B_i) = p^{H_i}$ satisfying $n_1 \geq \cdots \geq n_k > 0$ and $h_1 \geq \cdots \geq h_s > 0$. Then G and G' are isomorphic only if $k = s$ and for each i, $n_i = h_i$.

21. (Lemma 3.2.1 for rings with 1) If R is a ring with 1, then for all $a, b \in R$

    (a) $a0 = 0a = 0$

    (b) $a(-b) = (-a)b = -(ab)$

    (c) $(-a)(-b) = ab$

    (d) $(-1)a = -a$

22. (Fixed Lemma 3.2.2) Let R be a finite integral domain with at least two elements. Then R is a field.

23. (Part of Theorem 3.4.1) Let R and R' be rings and $\phi\colon R \to R'$ be a surjective ring homomorphism with kernel U. Then R' is isomorphic to R/U.

24. Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a field.

25. (Theorem 3.7.1 + its corollary on page 144) Prove that every Euclidean ring is a principal ideal domain.

26. (Theorem 3.8.1) $J[i]$ is a Euclidean ring.

27. (Lemma 3.8.1.) Let p be a prime integer and suppose that for some integer c relatively prime to p we can find integers x and y such that $x^2 + y^2 = cp$. Then there exist integers a and b such that $p = a^2 + b^2$.

28. (Lemma 3.9.2) Let F be a field. Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

29. (Lemma 3.10.1) If $f, g \in J[x]$ are both primitive polynomials, then fg is a primitive polynomial too.

30. (Lemma 3.11.4) Let R be a unique factorization domain, let F be its field of quotients. If $f \in R[x]$ is both primitive and irreducible as an element of $R[x]$, then it is irreducible as an element of $F[x]$. Conversely, if the primitive element of $f \in R[x]$ is irreducible as an element of $F[x]$, it is also irreducible as an element of $R[x]$.

31. (Theorem 5.1.1) Let K, L, F be fields. If L is a finite extension of K and if K is a finite extension of F, then $[L : F] = [L : K][K : F]$.

32. (Theorem 5.1.2) Let F be a subfield of K. Then $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F.

33. (Special case of Theorem 5.1.4) Let F be a subfield of K. If $a, b \in K$ are algebraic over F, then $a + b$ is algebraic over F.

34. (Theorem 5.1.5) If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.

35. (Problem 1 on page 219) Prove that e (the base of the natural logarithms) is irrational.

36. (Lemma 5.3.2) Let F be a field. A nonzero polynomial $f \in F[x]$ of degree n can have at most n roots in any extension of F.

37. (Simplified Theorem 5.3.1) Let F be a field. If $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$ and is irreducible over F, then there exists an extension E of F in which $p(x)$ has a root.

38. (Theorem 5.3.2) Let F be a field, and $f(x) \in F[x]$ be of degree $n \geq 1$. Then there is an extension E of F of degree at most $n!$ in which $f(x)$ splits into linear factors.

39. (Lemma 5.5.2) Let F be a field. The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree.

40. (Theorem 5.5.1) If F is a field of characteristic 0 and if a, b are algebraic over F, then there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.

373 theorems

1. (a) $e, f \in G$, s.t. $\forall a \in G$, $a \cdot e = e \cdot a = a \cdot f = f \cdot a \Rightarrow e = f$ (identity is unique)

then $e \cdot a = a \ \forall a \in G \Rightarrow e \cdot f = f$. similarly, $e \cdot f = e \Rightarrow e = f$

(b) $x \cdot a = a \cdot x = e$, $y \cdot a = a \cdot y = e \Rightarrow x = y$ (inverses are unique)

$a \cdot x = e = a \cdot y$, $\exists b \in G$ s.t. $b \cdot a = e$, then $b \cdot (a \cdot x) = b \cdot (a \cdot y)$ ← stronger: cancellation applies.

$\Rightarrow$ by associativity, $x = e \cdot x = (b \cdot a) \cdot x = b \cdot (a \cdot x) = b \cdot (a \cdot y) = (b \cdot a) \cdot y = e \cdot y = y$

(c) note that $a^{-1}(a^{-1})^{-1} = e = a^{-1} \cdot a \Rightarrow (a^{-1})^{-1} = a$ $\quad ((a^{-1})^{-1} = a)$

(d) $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1}) = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e$ $\quad ((a \cdot b)^{-1} = b^{-1} \cdot a^{-1})$

3. H is a subgroup of $G \Rightarrow (a, b \in H \Rightarrow ab \in H,\ a \in H \Rightarrow a^{-1} \in H)$ ← if finite, 2nd condition not necessary

($\Leftarrow$) $e \in H$ since $a \cdot a^{-1} \in H$, and associative law holds for H since it held in G.

4. suppose H finite, $a \in H$, then $a^2, a^3, \dots a^m, \dots \in H$. then for some $r, s \in \mathbb{Z}$, $r > s > 0$, $a^r = a^s$.

by cancellation, $a^{r-s} = e \in H$. since $r - s - 1 \geq 0$, $a^{r-s-1} \in H$ and $a^{r-s-1} = a^{-1}$, so $a^{-1} \in H$ follows.

5. (a) to show bijection between Ha & Hb, $\forall f: Ha \to Hb$, find $g: Hb \to Ha$ s.t. $f \circ g = id_{Hb}$, $g \circ f = id_{Ha}$

define $f(x) = xa^{-1}b$, then for $ha \in Ha$ arbitrary, $f(ha) = hb \in Hb$.

now, $g(y) = yb^{-1}a$, then $(f \circ g)(y) = f(yb^{-1}a) = (yb^{-1}a)(a^{-1}b) = y$

(b) being congruent mod H is an equivalence relation (reflexive, symmetric, transitive)

by (a), each equivalence group has same # of elements by (a)

↳ this # is equal to $|Ha|$ for any $a \in G$, in particular, $|He| = |H| = o(G)$, so $o(H) \mid o(G)$

6. if $o(a) = o(ca)$, then $o(a) \mid o(G)$, so need to show $\langle a \rangle = \{a^0, a^1, \dots, a^{n-1}\}$, $a^i \neq a^j$ for $i \neq j$

- $S \subseteq \langle a \rangle$ since $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$.
- let a^i be arbitrary, $a^n = e \Rightarrow a^{kn} = (a^n)^k = e \Rightarrow a^i = a^{i-kn}$ for any $k \in \mathbb{Z}$, then $\langle a \rangle \subseteq S$
- if $a^i = a^j$, $0 \leq i < j < n$, then $a^{j-i} = e$ and $j - i \leq n \Rightarrow$ contradict minimality ← $o(a)$ is smallest $n \in \mathbb{N}^+$ s.t. $a^n = e$

7. since $o(H) \mid o(G) = p$, $o(H) = 1$ ($H = \{e\}$) or $o(H) = p$ ($H = G$), so G has no nontrivial subgroups

now let $H = \langle a \rangle$ for some $a \neq e$, then $H = G$ and G is cyclic.

8. (a) if $HK = KH$, by subgroup criterion, enough to check closure

- $hk \in HK$ arbitrary, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$

- $(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$, since $k_1h_2 \in KH = HK$, $\exists k_3 \in K$, $h_3 \in H$, $k_1h_2 = h_3k_3$, $(h_1h_3)(k_3k_2) \in HK$.

if HK a subgroup, then $(hk)^{-1} = k^{-1}h^{-1} \in HK$, $k^{-1}h^{-1} \in KH$ since $k \in K$, $h \in H$.

9. $HK = \bigcup_{k \in K} Hk$ (right cosets either equal or disjoint)

since each Hk has exactly $o(H)$ elements, $|HK| = o(H) \cdot$ (# of diff. cosets of the form Hk for $k \in K$) $= o(H) \cdot m$

now, $Hk_1 = Hk_2 \Leftrightarrow k_1 \equiv k_2 \pmod H \Leftrightarrow k_1k_2^{-1} \in H$.

since $k_1, k_2 \in K$, $k_1k_2^{-1} \in K \Rightarrow k_1k_2^{-1} \in H \cap K$ ($H \cap K$ a subgroup of G) $\Rightarrow (H \cap K)k_1 = (H \cap K)k_2$

so, m = # right cosets of $H \cap K$ in $K = \frac{o(K)}{o(H \cap K)}$

10. if $gN = Ng$, then $gNg^{-1} = Ngg^{-1} = N$

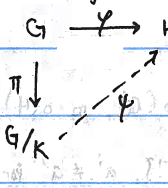
if N normal, then $gNg^{-1} \subseteq N$. since $g^{-1} \in G$, $g^{-1}Ng \subseteq N$.

for any f, $f(g^{-1}Ng) \subseteq f(N)$. let $f(x) = gxg^{-1}$, then $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$

then $gNg^{-1} = N \Rightarrow (gNg^{-1})g = Ng \Rightarrow gN = Ng$

11. let $K = \ker\varphi$, for $a, b \in K$, $\varphi(ab) = \varphi(a)\varphi(b) = ee = e \Rightarrow ab \in K$, $\varphi(a^{-1}) = \varphi(a)^{-1} = e^{-1} = e \Rightarrow a^{-1} \in K$

normality: $a \in K$, $b \in G$, then $\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = e \Rightarrow bab^{-1} \in K$.

12. 

$\pi(g) = Kg$ is the natural projection, φ surjective, define $\psi: G/K \to H$, $\psi(Kg) = \varphi(g)$

- well-defined as: $Kg_1 = Kg_2 \Rightarrow g_1 \equiv g_2 \pmod K \Rightarrow g_1g_2^{-1} \in K$

$\Rightarrow \varphi(g_1g_2^{-1}) = e \Rightarrow \varphi(g_1)\varphi(g_2)^{-1} = e \Rightarrow \varphi(g_1) = \varphi(g_2)$

- ψ is homomorphism: $\psi((Kg_1)(Kg_2)) = \psi(Kg_1g_2) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(Kg_1)\psi(Kg_2)$

- injectivity: $h \in H$, $\psi^{-1}(h) = \{Kg \mid \varphi(Kg) = h\} = \{Kg \mid \varphi(g) = h\} = \{Kg \mid g \in \varphi^{-1}(h)\}$

$= \{Kg \mid g \in Kg'\}$ where $g' \in \varphi^{-1}(h)$ $= \{Kg \mid Kg = Kg'\} = \{Kg'\}$ a 1-element set in G/K.

- surjectivity follows from surjectivity of $\varphi: G \to H \Rightarrow \psi$ is surjective isomorphism $\Rightarrow G/K \cong H$

↑ 23 uses the same proof (but for rings)

13. induction on $o(G)$: BC, if $o(G)=p$, then G is cyclic and any $a\neq e$ has order p

I.S.) pick $a\in G\setminus\{e\}$ arbitrarily, $H \overset{\text{def}}{=} \langle a\rangle$, $o(a)=o(H) \mid o(G)$

- if $H=G$, G is cyclic, $b=a^{o(G)/p} \Rightarrow b^p = a^{o(G)} = e$

since $o(a)=o(G)$, $a^i\neq e$ for $i<o(G)$, so $b\neq e$, then $o(b)=p$.

- if $o(H)<o(G)$ and $p\mid o(H)$, then apply induction to H.

- $1<o(H)<o(G)$, $p\nmid o(H)$, then $o(G/H)=i_G(H)=\frac{o(G)}{o(H)}$ (H normal since G abelian)

then $p\mid \frac{o(G)}{o(H)}$, so by induction, $\exists Hg\in G/H$ s.t. $o(Hg)=p$.

$\Rightarrow (Hg)^p = H \Leftrightarrow Hg^p = H \Leftrightarrow g^p\in H$ (since $Hg\neq H \Leftrightarrow g\notin H$)

let $g' = g^{o(H)}$, if $g'=e$, then $g^{o(H)}=e \Rightarrow g\in H \Rightarrow Hg=H \Rightarrow o(H)=p$

if $g'\neq e$, then $(g')^p = g^{p\cdot o(H)} = e$ (since $g^p\in H$), then $o(g')=p$

14. define $\psi: G\to I(G)$ via $\psi(g)=\varphi_g \rightsquigarrow \varphi_g(h)=ghg^{-1}$, $I(G)=\{\varphi_g : g\in G\}$ is a group under composition

(*) : $\varphi_{g_1}\varphi_{g_2}=\varphi_{g_1g_2}$

by (*), ψ is a homomorphism, and by definition of $I(G)$, ψ is surjective $\rightarrow I(G)=\psi(G)\approx G/Z(G)$

↑ $\ker\psi = \{g\in G \mid \psi(g)=id_G=\varphi_e\} = \{g\mid \varphi_g=id_G\} = \{g\mid \forall h\in G,\ \varphi_g(h)=h\}$

$= \{g\mid \forall h,\ ghg^{-1}=h\} = \{g\mid gh=hg\} = \{g\mid h,g \text{ commute}\} \overset{\text{def}}{=} Z(G)$.

15. define $\psi: G\to A(G)$ via $\psi(g)=\varphi_g$, where $\varphi_g: G\to G$ is given by $\varphi_g(h)=gh$

*$A(S)$ = set of all bijections from $S\to S$ with composition.
↳ a permutation group.

then $\varphi_g\in A(G)$ since $\varphi_{g^{-1}}$ is the inverse of φ_g

further, ψ is a homomorphism since $(\varphi_{g_1}\circ\varphi_{g_2})(h)=\varphi_{g_1}(\varphi_{g_2}(h))=g_1(g_2(h))=\varphi_{g_1g_2}(h)$

ψ is injective since $\ker\psi=\{g\in G\mid \psi(g)=id_G\}=\{g\mid \forall h, \varphi_g(h)=h\}=\{e\}$ is trivial

then $\psi(G)\approx G$ (from injectivity) and $\psi(G)$ is a subgroup of $A(G)$ (since ψ homomorphism)

16. (a) $\pi\in S_n$ is even if $\operatorname{sgn}(\pi)=1$, i.e., a product of an even number of transpositions

(b) $\{\pm 1\} = \operatorname{sgn}(S_n) \approx \frac{S_n}{\ker\operatorname{sgn}} = \frac{S_n}{A_n} \Rightarrow i_{S_n}(A_n)=o(\{\pm1\})=2$

↳ alternatively, $\exists$ bijection $A_n\to S_n\setminus A_n$ via $\sigma\in A_n \mapsto (1,2)\sigma$ (inverse exists since $id=(1,2)(1,2)$)

17. if $a\notin Z(G) \Rightarrow N(a)\neq G \Rightarrow$ by Lagrange, $o(N(a))=p^m$ s.t. $m<n$

$\Rightarrow p\mid \frac{o(G)}{o(N(a))} \Rightarrow o(Z(G)) = o(G) - \sum_a \frac{o(G)}{o(N(a))}$ is divisible by $p \Rightarrow Z(G)\neq\{e\}$.

18. $Z(G) \neq (e) \Rightarrow o(Z(G)) = p$ or p^2, if p^2, then $Z(G) = G \Rightarrow G$ abelian

if $o(Z(G)) = p$, pick $a \notin Z(G)$, then $a \in N(a)$ and $Z(G) \leq N(a) \Rightarrow \{a\} \cup Z(G) \subseteq N(a)$

$\Rightarrow o(N(a)) \geq p+1 \Rightarrow o(N(a)) = p^2 \Rightarrow a \in Z(G)$ $\rightarrow \leftarrow$.

19. If a proper subgroup of G has order divisible by p^n, apply IH.

WLOG, $\forall H \neq G$, H subgroup of G, $p^n \nmid o(H)$. then by class equation, $o(Z(G)) = o(G) - \sum_{a} \frac{o(G)}{o(N(a))}$ is divisible by p.

by Cauchy's thm, $Z(G)$ contains a subgroup H of order p, H is normal.

let $G' = G/H$, $o(G') = \frac{o(G)}{o(H)} = \frac{p^n r}{p} = p^{n-1} r$, applying induction to G', $\exists$ subgroup L', $o(L') = p^{n-1}$

$L \overset{\text{def}}{=} \{g \in G \mid Hg \in L'\} = \bigcup_{Hg \in L'} Hg = \pi^{-1}(L')$, where $\pi : G \to G'$ is the natural projection (*)

$|L| = \sum_{Hg \in L'} |Hg| = \sum_{Hg \in L'} p = p \cdot o(L') = p \cdot p^{n-1} = p^n$, L is a subgroup: $x, y \in L \Leftrightarrow \pi(x), \pi(y) \in L'$

20. $G(s) = \{sx : x \in G\}$ is a subgroup of G, specifically, $G(p) \approx \mathbb{Z}/p^{n-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n-1}\mathbb{Z}$ (written additively, $x + \cdots + x$)

$o(G) = p^{\#\text{dots}}$, $o(G(p)) = p^{\#\text{dots above } y=1}$ and $o(G(p^t)) = p^{\#\text{dots above } y=t}$

let D_1, D_2 be the diagrams of G, G', we know that $G(p^m) \approx G'(p^m)$ $\forall m \geq 0$

$\#$ dots in t^{th} row $= (\#\text{dots above } y=t) - (\#\text{dots above } y=t+1) \Rightarrow$ rows in D_1 = rows in D_2

Rings & Fields!

21. (a) by right distributive law, $a0 = a(0+0) = a0 + a0 \Rightarrow a0 = 0$ since R is a group under addition.

(b) $ab + a(-b) = a(b + (-b)) = a0 = 0 \Rightarrow a(-b) = -(ab)$

(c) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, $(u^{-1})^{-1} = u \Rightarrow -(-x) = x$

(d) $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0 \Rightarrow (-1)a = -a$.

22. let $a \in R \setminus \{0\}$, $R = \{0, r_1, \ldots, r_n\}$ and consider $0a, r_1 a, \ldots, r_n a$, (*) note that $r_i a = r_j a \Leftrightarrow r_i = r_j$

since R finite and (*) contains as many elements as R, for some i, $r_i a = a$, say $r_i a = a$.

claim r_i is a unity. say $b \in R \setminus \{0\}$, since b appears in (*), $\exists r_j$ s.t. $r_j a = b$.

$\Rightarrow r_i b = r_i(r_j a) = r_j(r_i a) = r_j a$ (commutative since integral domain) $= b$

$r_k a = 1$ for one r_k $\Rightarrow r_k = a^{-1}$.

24. let $a \in R \setminus \{0\}$, ideal $aR = \{ar : r \in R\}$ is nonzero bc. $a \in aR$, so $aR = R$

since $1 \in R$, $\exists b \in R$ s.t. $ab = 1$

25. Let U be an ideal in R, $h = \min\{d(r) : r \in U\}$, let c be any element of U s.t. $d(c) = h$.

claim that $U = \{cr : r \in R\} = (c)$. RHS $\subseteq U$ since $c \in U$ and U is ideal.

conversely, if $u \in U$, divide u by c, then $u = tc + r$, either $r = 0$ or $d(r) < d(c)$.

if $d(r) < d(c)$, then $r = u - tc \in U$, contradict minimality of c, then $r = 0$, $u = tc \in (c)$.

26. let $d(x) = N(x) = x\varphi(x) = a^2 + b^2$, $a, b \in \mathbb{Z}[i]$, $b \neq 0$, think of a, b as elements of $\mathbb{Q}[i]$ & divide there

$c = \frac{a}{b} \in \mathbb{Q}[i]$, $c = \alpha + \beta i$, $\alpha + \beta \in \mathbb{Q}$

round α, β to nearest integers: $\alpha = a_0 + \alpha_1$, $\beta = \beta_0 + \beta_1$, $\alpha_0, \beta_0 \in \mathbb{Z}$, $|\alpha_1|, |\beta_1| \leq \frac{1}{2}$

then $c_0 = \alpha_0 + \beta_0 i \in \mathbb{Z}[i]$, $c_1 = \alpha_1 + \beta_1 i$, $\frac{a}{b} = c = c_0 + c_1 \Rightarrow a = c_0 b + \underbrace{c_1 b}_{\text{remainder}}$, $a, c_0 b, c_1 b \in \mathbb{Z}[i]$.

claim that either $c_1 b = 0$ or $d(c_1, b) < d(b)$:

$$N(c_1 b) = c_1 b\, \varphi(c_1 b) = c_1 b\, \varphi(c_1)\varphi(b) = c_1 \varphi(c_1)\, b\, \varphi(b) = N(c_1) N(b)$$

note that $N(c_1) = N(\alpha_1 + \beta_1 i) = \alpha_1^2 + \beta_1^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 \leq \frac{1}{2} \Rightarrow N(c_1 b) \leq \frac{1}{2} N(b) < N(b)$.

27. suppose p is not prime in $\mathbb{Z}[i]$. then $p = (d + ei)(f + gi)$, both non-units

$p^2 = p\varphi(p) = (d^2 + e^2)(f^2 + g^2)$, both $d^2 + e^2 \neq 1$ & $f^2 + g^2 \neq 1$, then $d^2 + e^2 = p = f^2 + g^2$ (since p prime)

AFSOC p is prime in $\mathbb{Z}[i]$. then $p \mid a^2 + b^2 = (a + bi)(a - bi) \Rightarrow p \mid (a + bi)$ or $p \mid (a - bi)$ in $\mathbb{Z}[i]$

if $p \mid (a + bi)$ in $\mathbb{Z}[i]$, then since φ is automorphism, $\varphi(p) \mid \varphi(a + bi) \Rightarrow p \nmid (a - bi)$, similarly for $p \mid (a - bi)$.

then $p^2 \mid (a + bi)(a - bi) = a^2 + b^2 = cp$ in $\mathbb{Z}[i]$, i.e., $\frac{cp}{p^2} \in \mathbb{Z}[i] \Rightarrow \frac{cp}{p^2} \in \mathbb{Z} \Rightarrow p^2 \mid cp$ in $\mathbb{Z}$ $\rightarrow\leftarrow$

28. WLOG, $f(x) = a_0 + a_1 x + \ldots + a_m x^m$, $g(x) = b_0 + b_1 x + \ldots + b_n x^n$, $a_m, a_n \neq 0$, $m \geq n$

let $f_1(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x)$, then $\deg(f_1) \leq m - 1$, then inducting on the degree of $f(x)$,

IH $\Rightarrow f_1(x) = t_1(x) g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$, $r(x), t_1(x) \in F[x]$.

$\Rightarrow f(x) = \left(\left(\frac{a_n}{b_n}\right) x^{n-m} + t_1(x)\right) g(x) + r(x) = t(x) g(x) + r(x)$ where $t(x) = \left(\frac{a_n}{b_n}\right) x^{n-m} + t_1(x) \in F[x]$

29. let $f = a_0 + a_1 x + \ldots + a_n x^n$, $g = b_0 + b_1 x + \ldots + b_m x^m$, $fg = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$

AFSOC $\exists$ prime p s.t. $p \mid c_0, c_1, \ldots, c_{m+n}$. since f primitive, $\exists i$ s.t. $p \nmid a_i$, WLOG, $p \mid a_0, a_1, \ldots, a_{i-1}$

similarly, let j be the least $p \nmid b_j$, $p \mid b_0, \ldots, b_{j-1}$.

consider $c_{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \ldots + a_{i+j-1} b_1 + a_{i+j} b_0$

$\Rightarrow$ all terms except possibly $a_i b_j$ divisible by p, then $p \mid c_{i+j} \Rightarrow p \mid a_i b_j \Rightarrow p \mid a_i$ or $p \mid b_j$ $\rightarrow\leftarrow$.

30. Suppose primitive element $f(x) \in R[x]$ is irreducible in $R[x]$ but reducible in $F[x]$.

then $f(x) = g(x)\,h(x)$, $g(x), h(x) \in F[x]$ are of positive degree

now, $g(x) = \frac{g_0(x)}{a}$, $h(x) = \frac{h_0(x)}{b}$, where $a, b \in R$, $g_0, h_0 \in R[x]$ * $\deg g = \deg g_0 = \deg g_1$, similarly for h.

also, $g_0(x) = \alpha g_1(x)$, $h_0(x) = \beta h_1(x)$, where $\alpha = c(g_0)$, $\beta = c(h_0)$, and $g_1(x), h_1(x)$ are primitive in $R[x]$.

then $f(x) = \frac{\alpha\beta}{ab} g_1(x) h_1(x) \Rightarrow \alpha\beta = ab$ by comparing contents $\Rightarrow f(x) = g_1(x) h_1(x)$ is nontrivial factorization in $R[x]$

31. let $v_1, \dots, v_n$ be a basis for L over K ($v_i \in L$), $w_1, \dots, w_m$ be a basis for K over F ($w_j \in K$)

L / K / F

claim that $\{v_i w_j : i \in [1, n],\ j \in [1, m]\}$ is a basis for L over F.

- spanning: suppose $r \in L$ arbitrary, since $v_1, \dots, v_n$ span L, we can find $\alpha_1, \dots, \alpha_n \in K$ s.t. $r = \alpha_1 v_1 + \dots + \alpha_n v_n$

since $w_1, \dots, w_m$ span K, we can find $\beta_{ij} \in F$ s.t. $\alpha_i = \beta_{i1} w_1 + \dots + \beta_{im} w_m \Rightarrow r = \sum_i \left(\sum_j \beta_{ij} w_j\right) v_i$

- linear independence: suppose $\beta_{ij} \in F$, $0 = \sum_{ij} \beta_{ij} v_i w_j = \sum_i \underbrace{\left(\sum_j \underbrace{\beta_{ij}}_{\in F} w_j\right)}_{\in K} v_i$

$\sum_j \beta_{ij} w_j$ is a lin. comb. of w_i with F-coeff. $\Rightarrow \beta_{ij} = 0$ $\in K$: since v_i's are LI over K, $\forall i$, $\sum_j \beta_{ij} w_j = 0$

32. if $[F(a) : F] = n < \infty$, then $(n+1)$-elements, $1, a, \dots, a^n$, are LI over F

then $\exists b_0, \dots, b_n \in F$, $b_0 + b_1 a + \dots + b_n a^n = 0 \Rightarrow a$ is algebraic over F

if $a \in K$ is algebraic over F, minimal polynomial $f = b_0 + \dots + b_n x^n$, $\deg f = n$, then

$F(a) = \{c_0 + \dots + c_{n-1} a^{n-1} : c_i \in F\}$ is of degree n over F $\Rightarrow [F(a) \cong \frac{F[x]}{(f)} : F] = \deg f$

K / E=L(b) / L=F(a) / F

33. since a is algebraic and satisfies a polynomial in F of degree $\le m$, $[F(a) : F] \le m$, similarly, $[L(b) : L] \le n$

then $[E : F] = [E : L][L : F] \le mn \Rightarrow [F(a+b) : F] \le mn$ since $F(a+b) \subseteq E$

34. let $r \in K$ be arbitrary. since r is algebraic over E, there is a polynomial $f = b_0 + b_1 x + \dots + b_n x^n \neq 0$ s.t. $f(r) = 0$

E' / F(b0)(b1) / F(b0) / F ; K / E / F

let $E' = F(b_0, b_1, \dots, b_n)$, then $[E' : F] = [F(b_0) : F][F(b_0, b_1) : F(b_0)] \cdots [F(b_0, \dots, b_n) : F(b_0, \dots, b_{n-1})]$

since each b_i is algebraic over $F(b_0, \dots, b_{i-1})$ since it is algebraic over F, all factors on RHS are finite.

so, $[E' : F] < \infty$, and $[E'(r) : E'] < \infty$ bc. r is a root of $f \in E'[x] \Rightarrow [F(r) : F] \le [E'(r) : F] < \infty$.

35. let $S_n = \sum_{k=0}^{n} \frac{1}{k!}$ be the partial sum, claim that $0 < e - S_n < \frac{1}{n!\cdot n}$

$e - S_n = \frac{1}{(n+1)!} + \frac{1}{(n+2)!} = \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \dots\right) < \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+1)^2} + \dots\right) = \frac{1}{n!\cdot n}$

AFSOC $e = \frac{p}{q} \in \mathbb{Q}$, then $0 < e - S_q < \frac{1}{q!\,q} \Rightarrow 0 < q!\left(\frac{p}{q} - S_q\right) < \frac{1}{q}$, but $q!\left(\frac{p}{q} - S_q\right) \in \mathbb{Z}$,

and there exist no integers between 0 and $\frac{1}{q}$ $\rightarrow\leftarrow$.

36. say a_i has multiplicity m_i, then $(x-a_i)^{m_i} \mid f$, $i = 1, 2, \dots, k$.

since $F[x]$ is UFD, and $(x-a_i)$ & $(x-a_j)$ not associative, $(x-a_1)^{m_1} \cdots (x-a_k)^{m_k} \mid f \Rightarrow \deg f \geq m_1 + \dots + m_k$.

37. let $E = \frac{F[x]}{(f)}$, map $F \to E$ via $r \mapsto r + (f)$, mapping is a homomorphism

- kernel is (0) (only happens when $r = 0$) $\Rightarrow$ injective $\Rightarrow$ E contains a copy of F as a subfield

- claim $t = x + (f)$ is a root of f in E. say $f = b_0 + b_1 x + \dots + b_n x^n$

$\longleftarrow f \longrightarrow$

then $f(t) = b_0 + b_1 t + \dots + b_n t^n = (b_0 + b_1 x + \dots + b_n x^n) + (f) = (f) = 0$ in E $\Rightarrow$ roots go both ways.

38. induct on $\deg f = n$. if $n = 1$, then $E = F$

I.S.) let f_0 be an irreducible factor of f, $\deg(f_0) \geq 2$. if $\nexists f_0$, then f splits in F, $E = F$.

then $F' = \frac{F[x]}{(f_0)}$ is an extension of F containing a root of f_0, say $\alpha \in F'$, so $f_0(\alpha) = 0$

in $F'[x]$, $(x-\alpha) \mid f \Rightarrow f = (x-\alpha) f_1$

apply induction to F' & f_1, to get E s.t. f_1 splits in $E[x]$ and $[E : F'] \leq (\deg f_1)! = (n-1)!$.

$[F' : F] = \deg f_0 \leq \deg f = n \Rightarrow [E : F] = [E : F'][F' : F] \leq (n-1)! \cdot n = n!$

39. suppose f has multiple roots, say $f = (x-a)^2 g$. note that $F[x]$ is UFD since F is a field

then $f' = 2(x-\alpha) g + (x-\alpha)^2 g' = (x-\alpha)(2g + g') \Rightarrow (x-\alpha) \mid \gcd(f, f')$

conversely, $\gcd(f, f') \neq 1$, since f splits, $(x-\alpha) \mid f, f'$ for some $\alpha \in F$.

$f = (x-\alpha) g$ for some g, $f' = g + (x-\alpha) g' \Rightarrow g = f' - (x-\alpha) g' = (x-\alpha) h$ for some $h \in F[x] \Rightarrow f = (x-\alpha)^2 h$.

40. let f, g be the minimal polynomial of a, b over F. WLOG, both f, g splits over K (else, replace K by splitting field of fg)

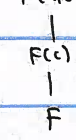
let $a_1, \dots, a_m$ be the roots of f, $b_1, \dots, b_n$ be the roots of g. $\lambda \in F$ is "good" if all mn elements $a_i + \lambda b_j$ distinct.

λ "bad" $\Leftrightarrow a_{i_1} + \lambda b_{i_1} = a_{i_2} + \lambda b_{i_2}$ with $(i_1, j_1) \neq (i_2, j_2)$

$\Leftrightarrow \lambda = \frac{a_{i_1} - a_{i_2}}{b_{j_2} - b_{j_1}}$ since if $j_1 = j_2$, then $i_1 = i_2$ since roots are unique

then # of bad λ's $\leq m^2 n (n-1)$, but since $\mathrm{char}(F) = 0$, F is infinite $\Rightarrow$ good λ's exist.

pick & fix such a $\lambda \in F$. let $c = a + \lambda b$. then $c \in F(a,b) \Rightarrow F(c) \subseteq F(a,b)$



let $h(x) = f(c - \lambda x) \in F(c)[x]$, $h(b) = f(c - \lambda b) = f(a) = 0 \Rightarrow (x-b) \mid h$ in $F[c][x]$

since $g(b) = 0 \Rightarrow (x-b) \mid g$ (bc. λ "good") $\Rightarrow (x-b) \mid \gcd(g, h)$, where $(x-b)^2 \nmid \gcd(g,h)$ bc. g has distinct roots bc. $\mathrm{char}(F) = 0$

if $b_j \neq b$ then $(x-b_j) \nmid h \Rightarrow \gcd(g, h) = (x-b) \in F(c)[x] \Rightarrow b \in F(c) \Rightarrow a \in F(c) \Rightarrow F(a,b) \subseteq F(c)$