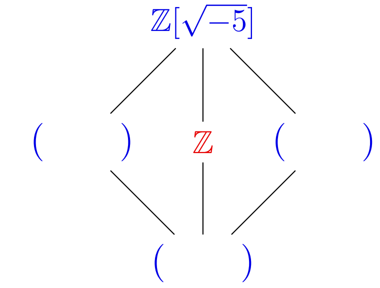
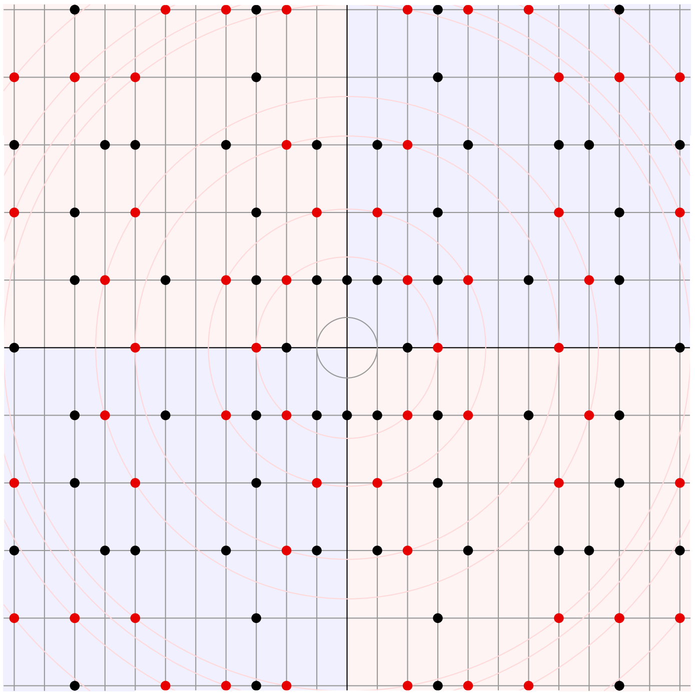
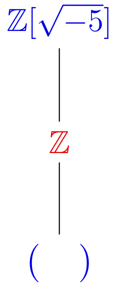
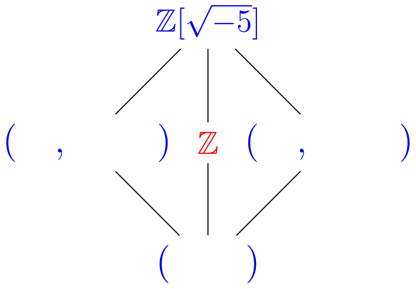
Math 4130, Final Exam. May 5, 2023

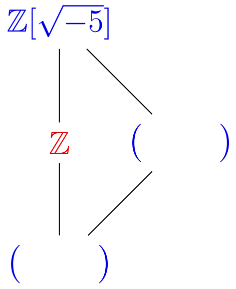
1. (20 points) A portion of the quadratic integer ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is shown below, as a subset of the complex plane. Primes are **black**. Light red circles are drawn to highlight pairs $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$ of quadratic integers that have the same norm, which are in turn colored red.











(a) Write down the units of $\mathbb{Z}[\sqrt{-5}]$.

(b) Find an integer $n \in \mathbb{Z}$ that does *not* factor uniquely into irreducibles in $\mathbb{Z}[\sqrt{-5}]$, and exhibit two distinct factorizations: $n = p^2 = (a + b\sqrt{-5})(a - b\sqrt{-5})$.

(c) Find an element in $\mathbb{Z}[\sqrt{-5}]$ that is *irreducible* but not *prime*, and compute its norm, $N(a+b\sqrt{-5}) = a^2 + 5b^2$.

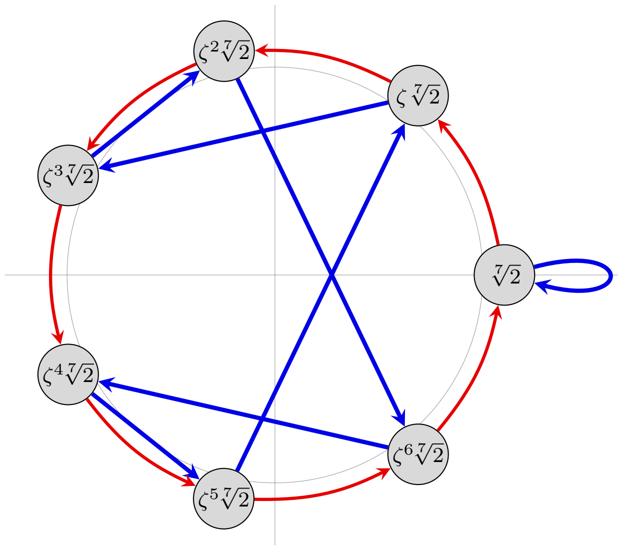
(d) Find an *inert prime*, i.e, some $p \in \mathbb{Z}$ such that (p) remains a prime ideal in $\mathbb{Z}[\sqrt{-5}]$.

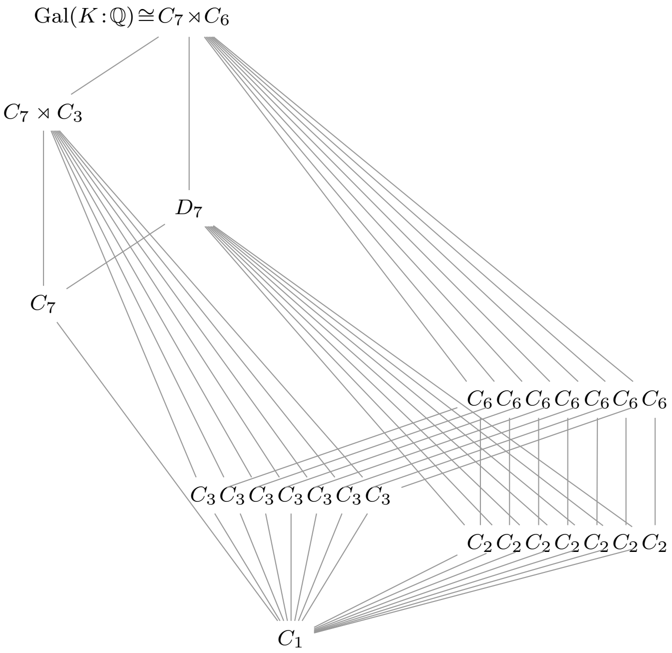
(e) The prime $29 \in \mathbb{Z}$ *splits*, because $29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$. Show that (29) is not a prime ideal of $\mathbb{Z}[\sqrt{-5}]$ by explictly demonstrating how the definition of a prime ideal fails.

(f) Show that the prime $5 \in \mathbb{Z}$ *ramifies* by finding a prime ideal P of $\mathbb{Z}[\sqrt{-5}]$ for which $(5) = P^2$.

(g) Fill in the missing portions of the subring lattices shown above with actual ideals of $\mathbb{Z}[\sqrt{-5}]$.

2. (50 points) Let $f(x) = x^7 - 2 \in \mathbb{Q}[x]$, and $K = \mathbb{Q}(\sqrt[7]{2}, \zeta)$ be its splitting field, where $\zeta = e^{2\pi i/7}$, a primitive 7th root of unity. Its Galois group is $G = \mathrm{Gal}(f(x)) \cong C_7 \rtimes C_6$. The action of $G = \langle \rho, \sigma \rangle$ on the roots of $f(x)$ is shown below on the left, and on the right is its subgroup lattice.




$\mathrm{Gal}(K:\mathbb{Q}) \cong C_7 \rtimes C_6$
$C_7 \rtimes C_3$
D_7
C_7
C_6 C_6 C_6 C_6 C_6 C_6 C_6
C_3 C_3 C_3 C_3 C_3 C_3 C_3
C_2 C_2 C_2 C_2 C_2 C_2 C_2
C_1

(a) Circle every normal subgroup on the subgroup lattice.

(b) The *commutator subgroup* is $G' \cong$______________, and the *abelianization* is $G/G' \cong$______________.

(c) The *derived series* $G = G^{(0)} \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots$ is ____.

(d) The *center* is $Z(G) \cong$________. (This can be deduced from the subgroup lattice and action graph.)

(e) The *ascending central series* $\langle 1 \rangle = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots$ is ______________________________________.

(f) The *descending central series* $G = L_0 \trianglerighteq L_1 \trianglerighteq L_2 \trianglerighteq \cdots$ is ______________________________________.

(g) Find all *composition series* $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = G$, and list the composition factors of each.

(h) The group G (is) (is not) [$\longleftarrow$ *circle one of these*] solvable, and (is) (is not) nilpotent.

(i) Find all (nontrivial) ways that G can be written as an extension of Q by N. For each one, determine whether it is a central, abelian, or split extension (it can be more than one of these).

(j) Other than $C_7 \rtimes C_6$, find all way(s) that G can be decomposed as a (nontrivial) direct or semidirect product of its subgroups.

For some of the remaining parts, the following maps are referred to:

$$\begin{aligned}\mathcal{F}\colon \big\{\text{subgroups of } G\big\} &\longrightarrow \big\{\text{subfields of } K\big\}\\ \mathcal{G}\colon \big\{\text{subfields of } K\big\} &\longrightarrow \big\{\text{subgroups of } G\big\},\end{aligned}$$

where $\mathcal{F}(H) =$ "*the (subfield of) elements of K fixed by every $\phi \in H$,*"
$\mathcal{G}(E) =$ "*the (subgroup of) automorphisms of G that fix every $e \in E$.*"

(k) Show that $f(x) = x^7 - 2$ is irreducible.

(l) Write the explicit automorphisms that generate $\mathrm{Gal}(x^7 - 2) = \langle \rho, \sigma \rangle$, where $\langle \rho \rangle \cong C_7$ and $\langle \sigma \rangle \cong C_6$:

$$\begin{cases} \rho\colon \sqrt[7]{2} \longmapsto \\ \rho\colon \quad \zeta \longmapsto \end{cases} \qquad \begin{cases} \sigma\colon \sqrt[7]{2} \longmapsto \\ \sigma\colon \quad \zeta \longmapsto \end{cases}$$

(m) The field $K = \mathbb{Q}(\sqrt[7]{2}, \zeta)$ is a vector space over $\mathbb{Q}$ of dimension ______________________.

(n) The splitting field $K = \mathbb{Q}(\sqrt[7]{2}, \zeta)$ has degree ______________________ over $\mathbb{Q}$.

(o) The field $E = \mathbb{Q}(\sqrt[7]{2})$ has degree 7 over $\mathbb{Q}$. By the tower law, $K = \mathbb{Q}(\sqrt[7]{2}, \zeta)$ has degree ___ over E.

(p) There are exactly ______________ intermediate subfields E for which $\mathbb{Q} \subsetneq E \subsetneq \mathbb{Q}(\sqrt[7]{2}, \zeta)$.

(q) How many intermediate subfields E, where $\mathbb{Q} \subsetneq E \subsetneq \mathbb{Q}(\sqrt[7]{2}, \zeta)$, are *normal* (or equivalently, *Galois*) extensions of $\mathbb{Q}$? Justify your answer.

(r) By the fundamental theorem of Galois theory, $\mathcal{G}\mathbb{Q} =$__________ and $\mathcal{G}K =$__________.

(s) By the fundamental theorem of Galois theory, $\mathcal{F}G =$__________ and $\mathcal{F}\langle 1 \rangle =$__________.

(t) Write down an intermediate field L, for which $\mathbb{Q} \subsetneq L \subsetneq \mathbb{Q}(\sqrt[7]{2}, \zeta)$, that has *degree* 6 over $\mathbb{Q}$, and then determine what familiar groups $\mathcal{G}L$ and $\mathrm{Gal}(L : \mathbb{Q}) \cong G/\mathcal{G}L$ are isomorphic to.

(u) An example of a subfield $E \subseteq K$ with $\mathcal{G}E \cong C_6$ is $E =$______________________.

(v) Is E, in the previous part, the splitting field of a polynomial over $\mathbb{Q}$? Why or why not?

(w) The subfields ____________ $\neq$ ____________ both have the same minimal polynomial.

(x) Find a primitive element for $K = \mathbb{Q}(\sqrt[7]{2}, \zeta)$. That is, some $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.

(y) Is K an extension of $\mathbb{Q}$ by radicals? Why or why not?

3. (25 points) Consider the polynomial $f(x) = x^4 - 4x^2 - 5 = (x^2 + 1)(x^2 - 5)$.

   (i) Sketch the four roots of $f(x)$ in the complex plane. Label the real and imaginary axis with a few "integer hash marks," to depict it approximately to scale.

   (ii) Find the splitting field K of $f(x)$ over $\mathbb{Q}$, and construct its subfield lattice, with K at the bottom. Label each edge by the *degree* of the corresponding extension.

   (iii) Write down a *basis* for K over $\mathbb{Q}$ (no proof needed), and use this to write a formula for a generic element of K (as a linear combination of the basis elements). What is the *degree* of the field extension, $[K : \mathbb{Q}]$?

   (iv) Compute the Galois group $G = \mathrm{Gal}(f(x))$. Explicitly describe *all* automorphisms of K (either by the image of the generators, or of a generic element).

   (v) The Galois group $G = \mathrm{Gal}(f(x))$ acts on the four roots of $f(x)$. Draw the action diagram, by adding arrows to your sketch from Part (a). Distinguish the generators by labels, or solid/dahsed lines.

(vi) Construct two copies of the subgroup lattice of G, side-by-side, with each edge labeled by the corresponding index. In one, use the actual groups by generators (e.g., $\langle \phi \rangle$), and in the other, write the isomorphism type (e.g., C_2).

(vii) Decide whether each subfield E of K ($\mathbb{Q}$ and K included) is a *normal* extension of $\mathbb{Q}$. How do you know this?

(viii) For each subfield E of K (including $\mathbb{Q}$ and K), write down the automorphisms $\mathcal{G}E \leq G$ that fix it.

(ix) Find an element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.

4. (20 points) Let I be an ideal of a commutative ring R with 1.

(a) The quotient ring consists of the set $R/I := \{ \qquad\qquad\qquad\qquad\qquad\qquad \}$.

(b) The additive identity is the coset ________, and the muliplicative identity is the coset ________.

(c) Write down how addition and multiplication (of cosets) are defined in the quotient ring.

(d) Carefully define what it means for an element (coset) of R/I to be a *zero divisor*.

(e) Define what it means for I to be a *prime ideal* of R.

(f) Prove that R is an integral domain if and only if the zero ideal $\{0\}$ is prime.

(g) Prove that I is prime if and only if R/I is an integral domain.

5. (25 points) Fill in the following blanks.

1. Every group is a quotient of a ____________________ group.

2. In the ring $R = \mathbb{Z}[x]$, the substructure $S = \mathbb{Z}$ is a(n) __________ but not a(n) __________.

3. The ideal $I =$__________ of $\mathbb{Z}[x]$ is non-principal because it cannot be generated by a single element.

4. An example of a quadratic integer ring $\mathbb{Z}[\sqrt{m}]$ that is Euclidean arises for $m =$__________.

5. An example of a quadratic integer ring $\mathbb{Z}[\sqrt{m}]$ that is not a UFD arises for $m =$__________.

6. An ideal $M \subsetneq R$ is *maximal* if R/M is ____________________.

7. An ideal $P \subsetneq R$ is *prime* if R/P is ____________________.

8. Hilbert's basis theorem says that every ideal of $F[x_1, \dots, x_n]$ is ____________________.

9. The commutator subgroup G' of any abelian group G is ____________________.

10. The commutator subgroup G' of any nonabelian simple group G is ____________________.

11. A group G is nilpotent iff all of its ____________________ are normal.

12. An example of a solvable group that is not nilpotent is ____________________.

13. Every alternating group A_n is simple, except the group(s) ____________________.

14. An example of a nontrivial group G with ascending central series $\langle 1 \rangle = Z_0 = Z_1 = Z_2 = \cdots$ is _____.

15. The smallest nonsolvable symmetric group S_n is ____________________.

16. By definition, the Galois group of $f(x)$ is the automorphism group of its ____________________.

17. An example of a non-normal extension field of $\mathbb{Q}$ is ____________________.

18. The polynomial $f(x) =$____________________ has Galois group $\mathrm{Gal}(f(x)) \cong D_4$.

19. Since $f(x) = x^5 - 10x + 2$ is irreducible, the action of $\mathrm{Gal}(f(x))$ on its five roots has _____ orbit(s).

20. The Galois group of $f(x) = (x^2 + 1)(x^2 - 2)(x^2 - 3)$ has order ____________________,

    and its action on the six roots of $f(x)$ has ____________________ orbit(s).

21. The free group F_S of rank 1 (i.e., on $S = \{a\}$) is the familiar group $F_S \cong$__________ from Math 4120.

22. A group presentation for the free product of $\mathbb{Z}_3 = \langle a \rangle$ and $V_4 = \langle h, v \rangle$ ____________________.

23. If $G_1 = \langle S \mid R_1 \rangle$ and $G_2 = \langle S \mid R_2 \rangle$ are groups with $R_1 \subseteq R_2$, then ____________________.

6. (10 points) Show that the quotient group G/G' is abelian. [*Hint: consider the commutator of any two elements (cosets).*]

7. (10 points) The *fundamental homomorphism theorem* (FHT) says that if $\phi\colon R \to S$ is a ring homomorphism, then $R/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$. The proof of this for groups involves constructing a map

$$\iota\colon R/I \longrightarrow \operatorname{Im}(\phi), \qquad \iota(r+I) = \phi(r),$$

where $I = \operatorname{Ker}(\phi)$, and showing that it is a well-defined group isomorphism. *You may assume this*, but carry out the remaining details (not many!) to prove the ring-theoretic version of the FHT.

8. (5 points) Thinking back to the entire year-long abstract algebra sequence (Math 4120 and 4130), what was your favorite topic? Specifically, what did you find the most interesting, and why?

9. (5 points) Describe (at least) one big "ah-ha" moment you had in either Math 4120 or 4130 – either where you saw the big picture of different concepts, or made a connection relating a topic from algebra to something from a different class.

10. (30 points) Mathematics graduate students who took my Math 8510 (Abstract Algebra 1) class last semester have seen all of the "ingredients" of Galois theory: group actions, solvable groups, the proof that A_n is simple for $n \geq 5$, fields, and automorphism groups. Additionally, they have the same "visual background" as you, and are well-versed with Cayley graphs and subgroup lattices.

    However, field and Galois theory is not covered until the following semetser, in Math 8520. For this essay, your target audience should be one of my Math 8510 students who has not yet taken Math 8520. Write a few paragraphs describing *what* Galois theory is all about, and a high-level overview of *how* Évariste Galois proved that there are degree-5 polynomials that are not solvable by radicals. Assume they have never heard Galois theory.

    Make sure you include the following: What is a splitting field? What is the Galois group of $f(x)$? What is the "Galois correspondence", and what is the significance of normal subgroups? (You may refer to $\mathcal{F}$ and $\mathcal{G}$ as defined earlier.) What is an extension by radicals, and what does it have to do with the Galois group, and solvability by radicals? Why was it important to find a polynomial with Galois group S_5, and *how* did we go about finding such a polynomial? Include at least one picture of subgroup and subfield lattices to aid your explanations.