GROUP

What is the condition that guarantees there is only one group of order n?

ALGEBRA PRELIM

GROUPS

Let H be a subgroup of G with index equal to the smallest prime dividing the order of G (specifically 2). What can be said about the relationship between H and G?

ALGEBRA PRELIM

GROUPS

Name two methods for detecting isomorphisms among semidirect products by a cyclic group.

ALGEBRA PRELIM

GROUPS

What special property does a group G of order p^2 have? Give a proof.

ALGEBRA PRELIM

GROUPS

Let $\mathrm{Inn}(G)$ be the group of inner homomorphisms of a group G. Is $\mathrm{Inn}(G)$ a normal subgroup of $\mathrm{Aut}(G)$?

ALGEBRA PRELIM

GROUPS

What is the automorphism group of V_4, the Klein four-group?

ALGEBRA PRELIM

GROUPS

State the <u>Orbit-Stabilizer Theorem</u>

ALGEBRA PRELIM

GROUPS

What does it mean for a group action to be <u>faithful</u>? <u>transitive</u>? What is the <u>kernel</u> of a group action?

ALGEBRA PRELIM

GROUPS

Let G be an abelian group acting transitively on set A. Prove that for $a, b \in A$, $\mathrm{Stab}_G(a) = \mathrm{Stab}_g(b)$.

ALGEBRA PRELIM

GROUPS

What is the definition of a <u>group homomorphism</u>?

ALGEBRA PRELIM

H is a normal subgroup of G.

There is only 1 group of order n if and only if n and $\varphi(n)$ are relatively prime. Note that φ is the totient function.

The group is abelian.

Pf: Center of p-group is nontrivial, so suppose $|Z(G)| = p$. $Z(G)$ normal, so quotient $G/Z(G)$ has order p and is cyclic. Quotient is generated by element $a + Z(G)$ so all cosets are $na + Z(G)$ for integer n. For $x, y \in G$, $x = na + z_1$ and $y = ma+z_2$. Then $x+y = na+z_1+ma+z_2 = na+ma+z_1+z_2 = (n+m)a+z_2+z_2 = z_2+ma+na+z_1 = ma+z_2+na+z_1 = y+x$. Thus G was abelian.f

Method One: Let K be a cyclic group, H an arbitrary normal group, and φ_1, φ_2 both homomorphisms $K \to \mathrm{Aut}(H)$. If $\mathrm{im}\,\varphi_1 = \mathrm{im}\,\varphi_2$, then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$

Method Two: Let K be an arbitrary group, H an arbitrary normal group, and φ_1, φ_2 both homomorphisms $K \to \mathrm{Aut}(H)$. If $\mathrm{im}\,\varphi_1$ and $\mathrm{im}\,\varphi_2$ are conjugate subgroups of $\mathrm{Aut}(H)$, then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$

It is S_3 because the three non-identity elements are all equivalent and can be shuffled freely while still preserving the group structure.

Yes, this is called Goursat's lemma.

Let G be a group acting on a set A. If distinct elements of G induce distinct permutations of the elements of A, then the action is *faithful*.

If for every $a, b \in A$, there exists some $g \in G$ such that $g \cdot a = b$, then the action is *transitive*.

The *kernel* of a group action is $\{g \in G \mid g \cdot a = a \ \forall a \in A\}$.

Let G be a group acting on set A. Then for $a \in A$,

$$|G|/|\mathrm{stab(x)}| = |\mathrm{orb}(x) = [G : \mathrm{stab(x)}]$$

For groups $(G, \times)$ and $(H, \cdot)$, the map $\varphi : G \to H$ is a homomorphism if for all $x, y \in G$, $\varphi(x \times y) = \varphi(x) \cdot \varphi(y)$.

Let $g \in \mathrm{Stab}_G(a)$. Since G acts transitively, there exists $h \in G$ such that $ha = b$. Then $gb = gha = hga = ha = b$ and so $g \in \mathrm{Stab}_G(b)$ as well. By symmetry, the two groups are equal.

GROUPS

What is the subgroup criterion?

ALGEBRA PRELIM

GROUPS

What are the normalizer and centralizer of a subset S of group G? What is the relationship between the normalizer and the centralizer?

ALGEBRA PRELIM

GROUPS

State several equivalent characterizations of normality of a subgroup

ALGEBRA PRELIM

GROUPS

State and prove Lagrange's Theorem

ALGEBRA PRELIM

GROUPS

State Cauchy's Theorem

ALGEBRA PRELIM

GROUPS

Let G be a group with subgroups H, K. What is the order of HK?

ALGEBRA PRELIM

GROUPS

If H, K are subgroups of G, when is HK also a subgroup of G? Can you think of a sufficient (and easier to check) condition that makes HK a subgroup?

ALGEBRA PRELIM

GROUPS

State the First Isomorphism Theorem for groups

ALGEBRA PRELIM

GROUPS

State the Second (Diamond) Isomorphism Theorem for groups

ALGEBRA PRELIM

GROUPS

State the Third Isomorphism Theorem for groups

ALGEBRA PRELIM

normalizer: $N_G(S) = \{g \in G \mid g^{-1}Sg = S\}$
The normalizer fixes the subset under conjugation.

centralizer: $C_G(S) = \{g \in G \mid g^{-1}sg = s, s \in S\}$
The centralizer fixes each element under conjugation.

The centralizer is a normal subgroup of the normalizer.

For a group G and subset H, H is a subgroup of G if and only if

1. H is nonempty and
2. for all $x, y \in H$, $xy^{-1} \in H$.

If H is finite, it suffices to check that H is nonempty and closed under multiplication.

Let G be a finite group and H a subgroup. Then $|H|$ divides $|G|$ and the number of left cosets of H in G is $|G|/|H|$.

Pf: Let $|H| = n$ and let the number of left cosets of H be k. Consider a map from H to a coset, $\varphi : H \to gH$ by $h \mapsto gh$ for some particular $g \in G$. This map is surjective by definition of left coset and injective by cancellation law. So every coset has size n. Since these left cosets partition G and there are k of them, $|G| = kn$.

Let N be a subgroup of G. Then TFAE:

- $N \trianglelefteq G$
- $N_G(N) = G$
- $gN = Ng$ for all $g \in G$
- The cosets of N form a group
- $gNg^{-1} \subseteq N$ for all $g \in G$
- N is the kernel of some homomorphism of G

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}$$

If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

If $\varphi : G \to H$ is an isomorphism of groups, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.

HK is a subgroup if and only if $HK = KH$. Note that this does *not* mean that the elements of H and K commute.

If $H \leq N_G(K)$ then HK is a subgroup. In particular if K is normal, then HK is a subgroup.

Let G be a group and let H, K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.

Let G be a group with subgroups A, B and $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.

$$\begin{tikzcd}[column sep=small] & AB \arrow[dl, dash] \arrow[dr, dash] & \\ A \arrow[dr, dash] & & B \arrow[dl, dash] \\ & A \cap B & \end{tikzcd}$$

Groups

State the Fourth (Lattice) Isomorphism Theorem for groups

Algebra Prelim

Groups

State the definition of a composition series.

Algebra Prelim

Groups

What does it mean for a group to be solvable?

Algebra Prelim

Groups

Prove that p-groups are solvable.

Algebra Prelim

Groups

G is a group, $H \leq G$. Let G act by left multiplication on the set A of left cosets of H. Let π_H be the permutation representation.
(1) True or False: G acts transitively on A.
(2) What is the stabilizer of the point $1H \in A$?
(3) What is the kernel of the action of π_H?

Algebra Prelim

Groups

State Cayley's Theorem.

Algebra Prelim

Groups

If G is a finite group of order n and p is the smallest prime dividing $|G|$, then what can we say about a subgroup H whose index is p?

Algebra Prelim

Groups

For some subset S of a group G, how many conjugates of S are there? Use the normalizer $N_G(S)$ in your answer.

Algebra Prelim

Groups

State and explain the class equation.

Algebra Prelim

Groups

How many conjugacy classes of S_n are there?

Algebra Prelim

Let G be a group. Then a composition series is a sequence of subgroups $$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$ such that $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group. The quotients N_{i+1}/N_i are called *composition factors* of G.	Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N.
A p-group has a normal subgroup for every divisor of its order, so we can form a chain of normal subgroups each of index p relative to the group above it. Then each quotient is of order p and thus abelian. This mean the p-group is solvable.	A group G is solvable if there is a chain of subgroups $$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$ such that G_{i+1}/G_i is abelian.
Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup os S_n.	1. True 2. H is the stabilizer in G of the point $1H$ 3. The kernel of π_H is $\bigcap_{x \in G} xHx^{-1}$. This kernel is the largest normal subgroup of G contained in H.
The number of conjugates of a subset S is the index of the normalizer of S, $\lvert G : N_G(S)\rvert$. In particular, the number of conjugates of an element S of G is the index of the centralizer of s, $\lvert G : C_G(s)\rvert$.	H is normal in G.
The number of conjugacy classes of S_n is equal to the number of partitions of n. Also note that two elements of S_n are conjugate if and only if they have the same cycle type.	Let G be a finite group. Then $$\lvert G\rvert = \lvert Z(G)\rvert + \sum_{i=1}^{r} \lvert G : C_G(g_i)\rvert$$ where $Z(G)$ is the center of G and each g_i is a representative from a conjugacy class of G not contained in $Z(G)$.

Groups

Complete this sentence:

Group H is isomorphic to a subgroup of group G if and only if there exists a ____________ homomorphism from H to G.

Algebra Prelim

Groups

Name two different methods for writing $(1\ 2\ 3\ 4)$ as a product of transpositions.

Algebra Prelim

Groups

State the definition of a characteristic subgroup.

Algebra Prelim

Groups

Let G be a group and H be a subgroup. What is the relationship between H and gHg^{-1} for any element $g \in G$? What is the relationship if H is normal?

Algebra Prelim

Groups

Let G be a group and H be a subgroup. Let G act on H by conjugation. What is the kernel of the permutation representation of G afforded by this group action?

Algebra Prelim

Groups

If K is a characteristic subgroup of H and H is a normal subgroup of G. What can we say about K relative to G?

Algebra Prelim

Groups

What is the isomorphism type of $\mathrm{Aut}(G)$ if G is cyclic of order n? What is the order of $\mathrm{Aut}(G)$?

Algebra Prelim

Groups

What is the order of the automorphism group of $\mathbb{Z}/n\mathbb{Z}$ when n is a prime? What if n is not prime?

Algebra Prelim

Groups

What is isomorphism type of the automorphism group of $(\mathbb{Z}/p\mathbb{Z})^n$?

Algebra Prelim

Groups

What is the isomorphism type of $\mathrm{Aut}(D_8)$?

Algebra Prelim

Head-to-Tail method: (1 4) (1 3) (1 2) *Swap-the-Last-to-First method:* (1 2) (2 3) (3 4)	injective
H is always isomorphic to gHg^{-1}. If H is normal, then conjugation by g is an automorphism of H.	A subgroup H of a group G is *characteristic* if every automorphism of G maps H to itself.
K is normal in G.	The permutation representation afforded by this action of g on H is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$.
In both cases, the order of the automorphism group if $\varphi(n)$ where φ is the totient function. If $n = p$ is a prime, then $\mathrm{Aut}(\mathbb{Z}/p/Z) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. If $n = p_1^{e_1} \cdots p_k^{e_k}$, then $\mathbb{Z}/n\mathbb{Z}^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})^\times$ by Chinese Remainder Theorem or structure theorem for modules over PIDs.	$\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, which is of order $\varphi(n)$ where φ is the totient function. $\mathrm{Aut}(G)$ is isomorphic to the units of $\mathbb{Z}/n\mathbb{Z}$ because an automorphism of G is uniquely determined by mapping any generator to any other generator.
$\mathrm{Aut}(D_8) \cong D_8$	$\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = GL_n(\mathbb{Z}/p\mathbb{Z})$ $\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ is a basis for $(\mathbb{Z}/p\mathbb{Z})^n$ as a vector space. Take any $\{v_1, \ldots, v_n\}$. By Linear algebra we have that the mapping $T(e_i) = v_i$ extends uniquely to a linear transformation of V. Each such T is a group endomorphism from V to V and likewise any endomorphism of V is a linear map of V as a vector space. If we restrict our attention to automorphisms of V we have $\mathrm{Aut}(V) = \{T : V \to V \mid \ker T = 0\} = GL_n(\mathbb{Z}/p\mathbb{Z})$.

Groups

What is the isomorphism type of $\mathrm{Aut}(Q8)$*?*

Algebra Prelim

Groups

Suppose n *is a positive integer but* $n \neq 6$*.*
What is the isomorphism type of $\mathrm{Aut}(S_n)$*?*
What is the index of $\mathrm{Inn}(S_n)$ *in* $\mathrm{Aut}(S_n)$*?*

Algebra Prelim

Groups

State Sylow's Theorem.

Algebra Prelim

Groups

Let P *be a normal Sylow* p*-subgroup of* G*. What is the image of* P *under any element of* $\mathrm{Aut}(G)$*? How many other Sylow* p*-subgroups besides* P *are there?*

Algebra Prelim

Groups

For what values of n *is* A_n *a simple group?*

Algebra Prelim

Groups

State the Fundamental Theorem of Finitely Generated Abelian Groups.

Algebra Prelim

Groups

Determine all possible abelian groups of order 180 by using invariant factors

Algebra Prelim

Groups

Describe the process of obtaining elementary divisors from invariant factors.

Then describe the process of obtaining invariant factors from elementary divisors.

Algebra Prelim

Groups

Table of Groups of Small Order: List all groups of order n *for* $n \in \{1, 2, 3, 4, 5\}$

Algebra Prelim

Groups

Table of Groups of Small Order: List all groups of order n *for* $n \in \{6, 7, 8, 9, 10\}$

Algebra Prelim

For all $n \neq 6$, $\mathrm{Aut}(S_n) \cong S_n$.

Symmetric groups aside from S_6 have only inner automorphisms, so $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ and the index of $\mathrm{Inn}(S_n)$ in $\mathrm{Aut}(S_n)$ is 1.

$\mathrm{Aut}(Q_8) \cong S_4$

The image of P under an automorphism of G is just P itself. This is because normal Sylow p-subgroups are characteristic.

There are no other Sylow p-subgroups besides P. Conjugation by elements of G induces a transitive action on the set of Sylow p-subgroups, so if P is normal, there are no other Sylow p-subgroups.

Let G be a group of order $p^\alpha m$, $p \nmid m$. Let $n_p = |Syl_p(G)|$.

1. If $P \in Syl_p(G)$ and Q is any p-subgroup, then Q is a subgroup of some conjugate of P.
2. $n_p \equiv 1 \mod p$.
3. $n_p \mid m$. This is because $n_p = [G : N_G(P)]$

Let G be a finitely generated abelian group. Then

1. $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ for integers $r, n_1, \ldots, n_s$ such that $r \geq 0$, $n_j \geq 2$ for all j, and $n_{i+1} \mid n_i$ for all $1 \leq i \leq s-1$ and
2. the expression in (1) is unique

For $n \neq 4$.

Invariant factors to elementary divisors: Factor each invariant factor into prime powers. This list of prime powers are the elementary divisors.

Elementary divisors to invariant factors: Group together the elementary divisors that are powers of the same prime. The largest invariant factor is the product of highest power primes in each group. The second invariant factor is the product of second-highest power primes in each group, and so on.

$180 = 2^2 \cdot 3^2 \cdot 5$, so the possible invariant factors (and the corresponding abelian groups) are listed below:

Invariant factors	Abelian Groups
$2^2 \cdot 3^2 \cdot 5$	$\mathbb{Z}_{180}$
$2 \cdot 3^2 \cdot 5, 2$	$\mathbb{Z}_{90} \times \mathbb{Z}_2$
$2^2 \cdot 3 \cdot 5, 3$	$\mathbb{Z}_{60} \times \mathbb{Z}_3$
$2 \cdot 3 \cdot 5, 2 \cdot 3$	$\mathbb{Z}_{30} \times \mathbb{Z}_6$

Order	Group
6	$\mathbb{Z}_6, S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^2, D_8, Q_8$
9	$\mathbb{Z}_9, \mathbb{Z}_3^2$
10	$\mathbb{Z}_{10}, D_{10}$

All of these groups are cyclic.

Order	Group
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$

Groups

Table of Groups of Small Order: List all groups of order n for $n \in \{11, 12, 13, 14, 15\}$

Algebra Prelim

Groups

Table of Groups of Small Order: List all abelian groups of order 16. List 3 non-abelian groups of order 16.

Algebra Prelim

Groups

Table of Groups of Small Order: List all groups of order n for $n \in \{17, 18, 19, 20\}$

Algebra Prelim

Groups

Classify all groups of order pq when p, q are distinct primes.

Algebra Prelim

Groups

Let G be a group and let $x, y \in G$. What is $[x, y]$, the commutator of x and y? Why is it called a commutator?

Algebra Prelim

Groups

What is a commutator subgroup of a group G? Is it a normal subgroup? If so, what can we say about the quotient of G by the commutator subgroup?

Algebra Prelim

Groups

What factoring property does the map $G \to G/[G, G]$ have?

Algebra Prelim

Groups

What is the universal property of the abelianization?

Algebra Prelim

Groups

Prove that $[G, G] \trianglelefteq G$

Algebra Prelim

Groups

State the recognition theorem for the direct and semidirect product of groups.

Algebra Prelim

Abelian groups: $\mathbb{Z}_{16}, \mathbb{Z}_8 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_4, \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2^4$

Non-abelian groups: $D_{16}, D_8 \times \mathbb{Z}_2, Q_8 \times \mathbb{Z}_2$

Order	Group
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2, A_4, D_{12}, \mathbb{Z}_3 \rtimes \mathbb{Z}_4$
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}, D_{14}$
15	$\mathbb{Z}_{15}$

Assume $p > q$.

If $p \nmid q - 1$, the only possible group is the cyclic group of order pq.

If $p \mid q - 1$, then there are two possible groups: the cyclic group of order pq and the semidirect product $\mathbb{Z}_q \rtimes \mathbb{Z}_p$.

Order	Group
17	$\mathbb{Z}_{17}$
18	$\mathbb{Z}_{18}, \mathbb{Z}_6 \times \mathbb{Z}_3, D_{18}, S_3 \times \mathbb{Z}_3, \mathbb{Z}_3^2 \rtimes \mathbb{Z}_2$
19	$\mathbb{Z}_{19}$
20	$\mathbb{Z}_{20}, \mathbb{Z}_{10} \times \mathbb{Z}_2, D_{20}, \mathbb{Z}_5 \rtimes \mathbb{Z}_4, F_{20}$

Note: $F_{20} = \langle x, y \mid x^4 = y^5 = 1, xyx^{-1} = y^2 \rangle$

The commutator subgroup $[G, G]$ of group G is defined as $\langle [x, y] = x^{-1}y^{-1}xy \mid x, y \in G \rangle$. It is a normal subgroup of G and quotienting by it gives an abelian group. In fact, $G/[G, G]$ is the largest abelian quotient in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $[G, G] \leq H$.

$[x, y] = x^{-1}y^{-1}xy$

This is called a commutator because $xy = yx[x, y]$

Note: This is the same answer as "What factoring property does the map $G \to G/[G, G]$ have?"

If A is an abelian group and $\varphi : G \to A$ is a homomorphism, then φ factors through $[G, G]$ and the following diagram commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\varphi"'] & G/[G,G] \arrow[d] \\ & A \end{tikzcd}$$

If A is an abelian group and $\varphi : G \to A$ is a homomorphism, then φ factors through $[G, G]$ and the following diagram commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\varphi"'] & G/[G,G] \arrow[d] \\ & A \end{tikzcd}$$

Direct Product: If group G contains normal subgroups H and K, $H \cap K = 1$, and $G = HK$, then $G \cong H \times K$.

Semidirect Product: The conditions are the same as above, but only one subgroup needs to be normal.

Let $g \in G$. Then $g[G, G]g^{-1} = g\langle [x, y] \mid x, y \in G \rangle g^{-1} = \langle g[x, y]g^{-1} \mid x, y \in G \rangle = \langle [gxg^{-1}, gyg^{-1}] \mid x, y \in G \rangle = \langle [x, y] \mid x, y \in G \rangle$, with the last equality holding since conjugation is an automorphism on G.

GROUPS

True or False: Every group can be written as a semidirect product. Give a proof or counterexample.

ALGEBRA PRELIM

GROUPS

List all groups of order p^3.

ALGEBRA PRELIM

GROUPS

If every group of order n (for some particular n) can be expressed as a semidirect product, what steps do you take to classify all groups of order n?

ALGEBRA PRELIM

GROUPS

Suppose group G can be expressed as a semidirect product $H \rtimes K$. If $(h_1, k_1), (h_2, k_2) \in G$, what is $(h_1, k_1)(h_2, k_2)$? (That is, how is the group operation defined in a semidirect product?)

ALGEBRA PRELIM

GROUPS

List the properties of p-groups.

ALGEBRA PRELIM

GROUPS

What is an upper central series?

ALGEBRA PRELIM

GROUPS

What does it mean for a group to be nilpotent? What is the nilpotence class of a nilpotent group?

ALGEBRA PRELIM

GROUPS

What is the nilpotence class of an abelian group?

ALGEBRA PRELIM

GROUPS

Arrange the following types of groups in a chain of inclusions: cyclic groups, nilpotent groups, solvable groups, abelian groups, all groups

ALGEBRA PRELIM

GROUPS

Let G be a finite group, let $p_1, \ldots, p_2$ be the distinct primes dividing its order, and let $P_i \in Syl_{p_i}(G)$, $1 \leq i \leq s$. State 5 conditions that are equivalent to the nilpotence of G.

ALGEBRA PRELIM

The three abelian groups are $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, and $\mathbb{Z}_p^3$. $$\mathrm{Heis}(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\}.$$ If $p = 2$, this last group is Q_8. If $p \neq 2$, the last group is some group of exponent p.	False. Q_8 is not a semidirect product because no two subgroups have trivial intersection. Every subgroup contains the subgroup $\{1, -1\}$.
$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2)$ where $k_1 \cdot h_2$ is the action of k_1 on h_2 as defined by φ, some automorphism of H.	1. Show every group G of order n has proper subgroups H, K such that $H \trianglelefteq G$, $H \cap K = 1$ and $HK = G$ 2. Find all possible isomorphism types for H and K 3. For each pair H, K found in (2), find all possible homomorphisms $\varphi : K \to \mathrm{Aut}(H)$ 4. For each triple H, K, φ found in (3), form the semidirect product $H \rtimes_\varphi K$ and determine which ones are isomorphic
The *upper central series* for a group G is the chain of subgroups $$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$ where the subgroups are inductively defined as $Z_0(G) = 1$, $Z_1(G) = Z(G)$, and $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$	Let P be a group whose order is p^a for prime p. 1. The center of P is nontrivial. 2. If H is a nontrivial normal subgp, then it intersects the center nontrivially. 3. P has a normal subgp of any order dividing p^a. 4. Every proper subgp of P is a proper subgp of its normalizer in P. (i.e. nilpotent) 5. Every maximal subgp has index p and is normal in P. 6. P is nilpotent of nilpotence class at most $a - 1$.
It is 1, since $Z_1(G) = Z(G) = G$.	A group G is called *nilpotent* if $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest such c is the *nilpotence class* of G.
1. If $H < G$, then $H < N_G(H)$ ("normalizer grows") 2. $P_i \trianglelefteq G$ for $1 \leq i \leq s$ (every Sylow subgroup is normal) 3. $G \cong P_1 \times P_2 \times \cdots \times P_s$ 4. Every maximal subgroup of G is normal 5. Its central series (or lower/upper central series) terminates after finitely many steps.	cyclic groups $\subseteq$ abelian groups $\subseteq$ nilpotent groups $\subseteq$ solvable groups $\subseteq$ all groups

Groups

What is a lower central series?

Algebra Prelim

Groups

What is the derived series or commutator series of a group G?

Algebra Prelim

Groups

For a group G, what condition on the groups in the derived series of G is necessary and sufficient for G to be solvable?

Algebra Prelim

Groups

State Burnside's theorem on groups of order $p^a q^b$.

Algebra Prelim

Groups

(Techniques for producing normal subgroups in groups of order n)

Describe the technique known as "counting elements."

Algebra Prelim

Groups

(Techniques for producing normal subgroups in groups of order n)

Describe the technique known as "exploiting subgroups of small index."

Algebra Prelim

Groups

(Techniques for producing normal subgroups in groups of order n)

Describe the technique known as "permutation representations."

Algebra Prelim

Groups

(Techniques for producing normal subgroups in groups of order n)

Describe the technique known as "playing p-subgroups against each other for different primes p."

Algebra Prelim

Groups

(Techniques for producing normal subgroups in groups of order n)

Describe the technique known as "studying normalizers of intersections of Sylow p-subgroups."

Algebra Prelim

Groups

What is the universal property of the free group $F(S)$ on a set S?

Algebra Prelim

The *derived* or *commutator series* of a group G is the following sequence of groups, defined inductively $\forall i \geq 1$.

$$G^{(0)} = G \qquad G^{(1)} = [G, G] \qquad G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

For a group G, the *lower central series* is the chain of subgroups

$$G^0 \geq G^1 \geq G^2 \geq \cdots$$

where the subgroups are defined inductively as $G^0 = G$, $G^1 = [G, G]$, and $G^{i+1} = [G, G^i]$.

Such groups are solvable.

G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

Let $|G| = n$, $H \leq G$, $[G : H] = k$. G acting on cosets of H by left multiplication induces a map from G to S_k. Suppose G is simple so that the kernel is trivial. Then G is isomorphic to a subgroup of S_k so $n \mid k!$. Because of this argument, if k is the smallest integer such that $n \mid k!$, then $\nexists\, H < G$ with index less than k.

ex) Suppose $n = 3993 = 3^2 \cdot 13 \cdot 29$. The possible indices of a subgroup are $3, 9, 13, \ldots$. Of these, only $29!$ is divisible by 3993.

Use this technique when for $P \in Syl_p(G)$, $|P| = p$.

Suppose by contradiction the group is simple so that the number of Sylow p-subgroups is greater than 1 (i.e. $n_p > 1$). Since each Sylow p-subgroup intersects only at the identity, count the number of elements in each subgroup. If the total elements counted is greater than n, then at least one n_p must be 1 and the unique Sylow p-subgroup is normal.

This technique is for primes p, q such that $p < q$ and $p \nmid q - 1$ (this makes groups of order pq cyclic).

If G has a Sylow q-subgroup Q of order q and $p \mid |N_G(Q)|$, then Cauchy's Theorem says $P = \langle p \rangle$ is a group of order p that normalizes Q. Then PQ is cyclic and thus abelian, so $PQ \leq N_G(P)$ and $q \mid |N_G(P)|$. This may force $N_G(P) = G$ or may force the index of $N_G(P)$ to be lower than that which is allowable by the "exploiting subgroups of small index" technique.

Let $|G| = n$ and H a subgroup of index k. Let $\varphi : G \to S_k$ be the permutation representation of G by action on cosets of H. Suppose that G is simple. Then the kernel is trivial and G is isomorphic to a subgroup of S_k. We can attempt to show that S_k contains no simple subgroup of order n.

We can use facts such as (1) if G contains an element/subgp of some order, so must S_k and (2) if $P \in Syl_p(G)$ and $P \in Syl_p(S_k)$, then $|N_G(P)|$ divides $|N_{S_k}(P)|$.

Any map from set S to a group G extends uniquely to a homomorphism φ from $F(S)$ to G.

$$\begin{tikzcd} S \arrow[r] \arrow[dr] & F(S) \arrow[d, dashed, "\varphi"] \\ & G \end{tikzcd}$$

Suppose $R, P \in Syl_p(G)$ are distinct subgroups and $R \cap P \neq 1$. Then by property 4 in the list of properties of p-groups, $P_0 = R \cap P$ satisfies $P_0 < N_P(P_0)$ and $P_0 < N_R(P_0)$. This may cause the normalizer in G of P_0 to have too small an index to satisfy the bound provided by the "exploiting subgroups of small index" technique.

Groups

What is a free group?

Algebra Prelim

Groups

The derived series of a group terminates (every group in the chain is eventually trivial group 1) if and only if the group is ____________

Algebra Prelim

Groups

If G, H are solvable groups, which of the following are also solvable? The direct product $H \times G$? The semidirect product $H \rtimes G$? Any subgroup K of G? The quotient G/N for some normal subgroup N of G?

Algebra Prelim

Groups

Let a be an element of order n and b be an element of order m. Is it true that $\langle a, b\rangle$ has order $\operatorname{lcm}(a, b)$?

Algebra Prelim

Groups

State and prove Frattini's Argument.

Algebra Prelim

Groups

Prove that if G is solvable, then G/N is solvable.

Algebra Prelim

Groups

Prove that if $N \trianglelefteq G$, N is solvable, and G/N is solvable, then G is solvable.

Algebra Prelim

Rings

What is a ring?

Algebra Prelim

Rings

What is a division ring? What is another name for a commutative division ring?

Algebra Prelim

Rings

What is an integral domain? What desirable property do integral domains possess? What desirable property do finite integral domains possess?

Algebra Prelim

solvable

A free group is a group with no relations. Its elements are just the *words* made by the generators in some set S.

No, this is not generally true. If the permutation representations of a and b are disjoint, then it is true.

These are all solvable. Ha!

G is a composition series such that each successive quotient is abelian. Quotienting every group in the series produces a composition series for G/N such that each successive quotient is abelian. Thus G/N is solvable.

If $H \trianglelefteq G$ and $P \in Syl_p(H)$, then $G = N_G(P)H$

Proof: Let $g \in G$. Then $g^{-1}Pg \in H$ since $H \trianglelefteq G$. Thus $g^{-1}Pg$ is also a Sylow p-subgroup of H. Since all Sylow p-subgroups of H must be conjugate by some element of H, there exists $h \in H$ such that

$$h(g^{-1}Pg)h^{-1} = P.$$

So $gh^{-1} \in N_G(P)$ and $g \in N_G(P)H$. Since g was arbitrary, $G \subseteq N_G(P)H$ which implies $G = N_G(P)H$.

A *ring* R is a set together with two binary operations + and × such that

1. (R, +) is an abelian group
2. × is associative
3. The distributive property holds

N is solvable so there is composition series $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_n = N$ so that N_{i+1}/N_i is abelian. Likewise there is a series for $\overline{G} = G/N$ composed of subgroups $\overline{G_i}$. By the Lattice isomorphism theorem, there are subgroups G_i of G containing N such that $G_i/N = \overline{G_i}$. Thus we can form the following composition series for G, each successive quotient is abelian, and G is solvable:

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_n = N = G_0 \trianglelefteq \cdots \trianglelefteq G_m = G$$

An *integral domain* is a ring with no zero divisors.

Integral domains possess the cancellation property.

Finite integral domains are fields.

A ring with identity ($1 \neq 0$) is a *division ring* if every nonzero element has a multiplicative inverse.

A commutative division ring is a *field*.

RINGS

What is a left ideal?

ALGEBRA PRELIM

RINGS

What is the subring criterion?

ALGEBRA PRELIM

RINGS

What is a ring homomorphism?

ALGEBRA PRELIM

RINGS

Is the kernel of a ring homomorphism an ideal of the domain?

ALGEBRA PRELIM

RINGS

Let I, J be ideals of ring R.
What is $I + J$? Is it an ideal of R?
What is IJ? Is it an ideal of R?

ALGEBRA PRELIM

RINGS

Let I, J be ideals of ring R. Is it true that $I \cap J \subseteq IJ$?

ALGEBRA PRELIM

RINGS

Given a ring R and some subset A, what is the ideal generated by A?

ALGEBRA PRELIM

RINGS

Given a ring R and ideal I, what is the condition that guarantees $I = R$?

ALGEBRA PRELIM

RINGS

If R is a field, then what can we say about a nonzero ring homomorphism from R to another ring?

ALGEBRA PRELIM

RINGS

What is a maximal ideal? Does every ring have maximal ideals? Which rings always have maximal ideals?

ALGEBRA PRELIM

Given any subset S of a ring R, we know that S is a subring if S is nonempty and closed under subtraction and multiplication.

Let R be a ring, I a subset of R, and $r \in R$. I is an *ideal* of R if

1. I is a subring of R and
2. I is closed under left multiplication by elements from R.

Yes indeedy.

Let R, S be rings and $\varphi : R \to S$. Then φ is a *ring homomorphism* if $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$.

No. $IJ \subseteq I \cap J$. Sometimes IJ may even be strictly smaller.

$I + J = \{a + b \mid a \in I, b \in J\}$
This is an ideal of R.

$IJ = \{a_1 b_1 + \cdots a_n b_n \mid a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in J, n \in \mathbb{Z}^+\}$
This is an ideal of R.

Note: $S = \{ij \mid i \in I, j \in J\}$ is not necessarily an ideal.

$I = R$ if and only if I contains a unit

Proof: ($\to$) If $I = R$, then I contains 1, which is a unit.

($\leftarrow$) If $a \in I$ is a unit, then $a^{-1} \in I$ as well. By the multiplicative sucking property, $a^{-1}a \in I$ and so $1 \in I$. Then every element of R is in I and $R = I$.

The left ideal generated by A is

$$RA = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}.$$

An ideal M in a ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.

No, not every ring has maximal ideals. For example, $\mathbb{Q}$ equipped with standard addition and trivial multiplication ($ab = 0\ \forall a, b \in \mathbb{Q}$) has no maximal ideals. We can perform this construction for any abelian group that has no maximal subgroups.

In a ring with identity, every proper ideal is contained in a maximal ideal.

That homomorphism is injective. The kernel of the homomorphism would need to be an ideal, and the only ideals in a field are 0 and R. Since the homomorphism is nonzero, the kernel is not all of R. Thus the kernel is 0 and the map is injective.

Let R be a ring and I. What can be said about R/I when I is maximal? What can be said about R/I when I is prime?

What is a prime ideal?

In a commutative ring with unity, is every prime ideal a maximal ideal or is every maximal ideal a prime ideal? Give an example. In what kind of ring do prime and maximal ideals coincide?

Given a ring R, what is its ring of fractions? Under what condition is the ring of fractions a field?

Let A, B be ideals in ring R. What does it mean for A and B to be comaximal?

State the Chinese Remainder Theorem. Give an example.

What is a Euclidean domain?

What is a norm on an integral domain R? What is a positive norm?

What is the greatest common divisor of a, b?

Let R be a commutative ring and $a, b \in R$. If $(a, b) = (d)$ for some element d, what do we know about d?

Assume R is a commutative ring. The ideal P is a *prime ideal* if $P \neq R$ and whenever $ab \in P$, at least one of a or $b \in P$.

R/I is a field if and only if I is a maximal ideal.

R/I is an integral domain if and only if I is a prime ideal.

Let R be a commutative ring and D a nonempty subset of R that does not contain 0 or zero divisors and is closed under multiplication. Then the *ring of fractions* is $Q = \left\{ \dfrac{r}{d} \mid r \in R, d \in D \right\}$.

If $D = R - \{0\}$ (i.e. R is an integral domain) then Q is a field.

Every maximal ideal is a prime ideal. The converse is not always true: in any nonfield integral domain, the zero ideal is a prime ideal which is not maximal.

In a PID, every nonzero prime ideal is maximal.

Let $A_1, \dots, A_k$ be ideals in ring R. The map $R \to R/A_1 \times \cdots \times R/A_k$ defined by $r \mapsto (r + A_1, \dots, r + A_k)$ is a ring homomorphism with kernel $A_1 \cap \cdots \cap A_k$.

If each pair of ideals in the list is comaximal, then this map is surjective and $A_1 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$ so that $R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \cdots \times R/A_k$.

ex.) If integer n has prime factorization $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$ and $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$.

Ideals A and B are *comaximal* if $A + B = R$.

A *norm* on integral domain R is a function $N : R \to \mathbb{Z}_{\geq 0}$ such that $N(0) = 0$. If in addition, $N(a) \neq 0$ for $a \neq 0$, then N is a *positive norm*.

An integral domain R is a *Euclidean domain* if there exists a norm N on R such that for $a, b \in R$, there exist $q, r \in R$ such that

$$a = qb + r \qquad \text{with } r = 0 \text{ or } N(r) < N(b)$$

d is the greatest common divisor of a, b.

Warning: This is *not* saying that $(a, b) = (gcd(a, b))$ (which is true in a Euclidean domain). This is saying that *if* $(a, b) = (d)$, then d is the GCD.

In general, it is possible that $(a, b) \neq (gcd(a, b))$. In $\mathbb{Z}[x]$, the ideal $(2, x)$ is not the whole ring. However, their GCD is 1 and the ideal (1) is indeed the whole ring

A *greatest common divisor* of a, b is a nonzero element d such that

1. $d \mid a$
2. $d \mid b$
3. if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Rings

In what kind of ring is it true that any two elements from the ring are guaranteed to have a greatest common divisor?

Algebra Prelim

Rings

Let R be an integral domain. If $(d) = (d')$, prove that $d = ud'$ for some unit u.

Algebra Prelim

Rings

In what kind of ring is it true that if $(a, b) = (d)$, then $d = gcd(a, b)$?

Algebra Prelim

Rings

Let I be an ideal and suppose $ab \in I$ but $a, b \notin I$. Why is it the case that a, b are not units?

Algebra Prelim

Rings

What is a <u>principal ideal domain</u>?

Algebra Prelim

Rings

If R is a commutative ring such that $R[x]$ is a PID, prove that R is a field.

Algebra Prelim

Rings

Let R be an integral domain. What does it mean for $r \in R$ to be <u>irreducible</u>? What does it mean for r to be be <u>prime</u>? What is the relationship between these two terms?

Algebra Prelim

Rings

In what type of ring is a prime element the same as an irreducible element? In general, does prime imply irreducible or does irreducible imply prime? Give an example of an element that has one property but not the other.

Algebra Prelim

Rings

Prove that a prime element is always irreducible in an integral domain.

Algebra Prelim

Rings

What is a <u>unique factorization domain</u>?

Algebra Prelim

This is clear if d or d' is zero, so suppose both are nonzero. Since $d \in (d')$, there exists $x \in R$ such that $d = xd'$. Likewise there exists $y \in R$ so that $d' = yd$. Thus $d = xyd$ and $d(1 - xy) = 0$. Since $d \neq 0$, $xy = 1$.

UFDs.

The division algorithm in a Euclidean domain gives a convenient way to compute it, but the GCD is guaranteed to exist for any two ring elements in a GCD domain. A UFD is always a GCD domain.

Suppose by contradiction that b is a unit. Since $ab \in I$, by the multiplicative sucking property, $(ab)b^{-1} \in I$. But this implies that $a \in I$, contrary to our premise. Thus b is not a unit.

a and b need to be nonzero elements in a commutative ring.

R is a subring of $R[x]$, so R must also be an integral domain. Since $R[x]/(x)$ is isomorphic to R and R is an integral domain, we know that (x) is a prime ideal. In a PID, a prime ideal is also a maximal idea. Thus $R[x]/(x) \cong R$ is a quotient by a maximal ideal and hence is a field.

A *principal ideal domain* is an integral domain in which every ideal is principal.

In an integral domain, every prime element is irreducible.

Every irreducible element is also prime in a PID.

In $\mathbb{Z}[\sqrt{-5}]$, the number 3 is irreducible but not a prime because $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ and $3 \mid 9$ but 3 does not divide either of the two factors of 9.

Suppose $r \neq 0$ and r is not a unit. An element r is irreducible if whenever $r = ab$ for $a, b \in R$, one of a or b is a unit.

An element r is prime if the ideal (r) is a prime ideal. In a PID, an irreducible element is also prime.
In an integral domain, a prime element is always irreducible.

A *unique factorization domain* is an integral domain R in which every nonzero element r that is not a unit has a unique factorization into irreducible elements and that this factorization is unique up to multiplication by units.

Take prime element p such that $p = ab$. Then $ab = p \in (p)$ so either a or b is in (p). Assume WLOG $a \in (p)$. Then $a = pr$ for some $r \in R$. Thus $p = ab = prb$ and $rb = 1$ so b is a unit.

Rings

What are the primes in $\mathbb{Z}[i]$?

Algebra Prelim

Rings

Under what conditions is a prime p the sum of two integer squares? (i.e. State Fermat's Theorem of the sum of squares.)

Algebra Prelim

Rings

State the containment chain for different kinds of commutative rings. Give an example from each superset that is not contained in its subset.

Algebra Prelim

Rings

If F is a field, then $F[x]$ is what kind of ring? Be as specific as possible.

Algebra Prelim

Rings

State Gauss's Lemma for polynomials in a UFD.

Algebra Prelim

Rings

If ring R is a UFD, then what can we say about the polynomial ring formed from adjoining any number of variables to R?

Algebra Prelim

Rings

State the theorem for detecting irreducibility via quotient by an ideal.

Algebra Prelim

Rings

State Eisenstein's Criterion.

Algebra Prelim

Rings

How can we use Eisenstein's Criterion to indirectly show that $x^4 + 1$ is irreducible over $\mathbb{Q}$?

Algebra Prelim

Rings

Let F be a field so that $F[x]$ is a polynomial ring. What are the maximal ideals of $F[x]$? Give a proof.

Algebra Prelim

The prime p is the sum of two integer squares, $p = a^2 + b^2$, if and only if $p = 2$ or $p \equiv 1 \mod 4$. This representation of p is unique.

A Gaussian integer $a + bi$ is a Gaussian prime if and only if either

- one of a, b is zero and the other is a prime of the form $4n + 3$ or $-(4n + 3)$ or
- both $a, b \neq 0$ and $a^2 + b^2$ is a prime.

$F[x]$ is a Euclidean domain.

$E \subseteq P \subseteq U \subseteq I \subseteq C$

- $\mathbb{Z}/n\mathbb{Z}$, n not prime, $\in C$ but $\notin I$.
- $\mathbb{Z}[\sqrt{-5}] \in I$ but $\notin U$ because 6 factors as $2 \cdot 3$ and as $(1 + \sqrt{-5})(1 - \sqrt{-5})$.
- $\mathbb{Z}[x]$ is a UFD but not a PID
- The ring of integers in $\mathbb{Q}(\sqrt{-19})$, which is numbers of the form $(a + b\sqrt{-19})/2$ with a, b both even or both odd, is a PID but not Euclidean.

The polynomial ring is also a UFD.

Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible/irreducible in $F[x]$, then it is reducible/irreducible over $R[x]$

Let R be an integral domain with prime ideal P. Let $p(x)$ be a *monic* polynomial of degree ≥ 1 in $R[x]$. If every coefficient except the leading coefficient is in P and the constant term is not in P^2, then $p(x)$ is irreducible in $R[x]$.

Let R be an integral domain with ideal I. Let $p(x)$ be a nonconstant polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Note: The converse is not true. This theorem can fail to detect irreducibility. For example, $x^4 - 72x^2 + 4$ is irreducible, but is reducible modulo every integer.

The maximal ideals of $F[x]$ are those generated by irreducible elements.

Proof: Since $F[x]$ is Euclidean, irreducible elements are prime (in PIDs) and prime elements generate maximal ideals (in PIDs).

First we shift the polynomial. Let $f(x) = x^4 + 1$ and $g(x) = f(x + 1) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Now $g(x)$ is irreducible by Eisentein's, so $f(x)$ must also be irreducible since any factorization of g yields a factorization of f.

Rings

Let F be a field so that $F[x]$ is a polynomial ring. What kind of ring is $F[x]$?

Algebra Prelim

Rings

Let F be a field so that $R = F[x_1, \ldots, x_n]$ is a polynomial ring. What kind of ring is R?

Algebra Prelim

Rings

What is a Noetherian ring?

Algebra Prelim

Rings

Let R be a Noetherian Ring so that $R[x]$ is a polynomial ring. What kind of ring is $R[x]$?

Algebra Prelim

Rings

Prove that if F is a field, then $F[x_1, \ldots, x_n]$ is Noetherian.

Algebra Prelim

Rings

Let R be a ring and I its unique maximal ideal. Prove that I must contain every element of R that is not a unit.

Algebra Prelim

Modules

True or False: A submodule of a finitely-generated module is also finitely generated. Give a proof or counterexample

Algebra Prelim

Modules

True or False: If a module and its submodule are both finitely generated, then the minimal number of generators of the module is greater or equal to the minimal number of generators of the submodule.

Algebra Prelim

Modules

What is a (left) R−module?

Algebra Prelim

Modules

What is a submodule?

Algebra Prelim

R is a UFD. It is not a PID unless $n = 1$.	$F[x]$ is a Euclidean domain
$R[x]$ is Noetherian. This is known as *Hilbert's Basis Theorem.*	A commutative ring R with 1 is *Noetherian* if every ideal of R is finitely generated.
Let $r \in R$ be an element that is not a unit. Then the ideal (r) is contained in some maximal ideal. Since I is the unique maximal ideal, $r \in I$.	The only ideals of F are 0 and F, both of which are finitely generated by 0 and 1, respectively. Thus F is Noetherian. Since the polynomial ring formed by adjoining one indeterminate to a Noetherian ring is also Noetherian, we know $F[x_1]$ is Noetherian. By induction, $F[x_1, \ldots, x_n]$ is Noetherian.
False. Consider $\mathbb{Z}[x]$ as a $\mathbb{Z}$-module. $\mathbb{Z}[x]$ can be generated by 1, but the ideal/submodule $(2, x)$ cannot be generated by fewer than 2 generators. This is one of the reasons that modules suck.	False. Every ring with identity is finitely generated as an R-module over itself by the identity. But if its ideals are not finitely generated, then the submodules are non-finitely generated submodules. To be more specific, consider $\mathbb{R}[x_1, x_2, \ldots]$, the polynomial ring over the reals with countably many indeterminates. The ring is itself generated by 1, but the ideal $I = (x_1, x_2, \ldots)$ cannot be finitely generated.
Let R be a ring and M and R$-$*module*. An *R-submodule* of M is a subgroup N of M such that for all $r \in R, n \in N$, we have $rn \in N$ (i.e. closed under the action of ring elements).	Let R be a ring. A *left R-module* an abelian group (M, +) together with an action of R on M such that for all $r, s \in R$ and $m, n \in M$, • (r+s)m = rm + sm • (rs)m = r(sm) • r(m+n) = rm + rn If R has 1, we also require that $1m = m$. Then M will be a *unital* module.

MODULES *What is the <u>free module of rank n over R</u>?* ALGEBRA PRELIM	MODULES *What kind of module is the same as an abelian group?* ALGEBRA PRELIM
MODULES *If F is a field, what is an $F[x]$-module?* ALGEBRA PRELIM	MODULES *Let F be a field, V a vector space, and T a linear transformation from V to V. What are the submodules of the $F[x]$-module V?* ALGEBRA PRELIM
MODULES *State the submodule criterion.* ALGEBRA PRELIM	MODULES *Let R be a ring. What is an <u>$R-$module homomorphism</u>?* ALGEBRA PRELIM
MODULES *Let R be a ring and M, N be R-modules. What is $\mathrm{Hom}_R(M, N)$?* ALGEBRA PRELIM	MODULES *Let R be a ring and M, N be R-modules. Under what ring action is $\mathrm{Hom}_R(M, N)$ also an R-module?* ALGEBRA PRELIM
MODULES *True or False: Let R be a ring and M be an R-module. Then for any submodule N of M, we can form a quotient module M/N. Give a proof or counterexample.* ALGEBRA PRELIM	MODULES *Let A, B be submodules of the R-module M. What is the smallest module that contains both A and B?* ALGEBRA PRELIM

Any $\mathbb{Z}$-module is exactly an abelian group. $\mathbb{Z}$-submodules are subgroups.	Let R be a unital ring and let n be a positive integer. The *free module of rank n over R* is $$R^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R\}$$ as a module over R with componentwise addition and multiplication.
The submodules of V are subspaces U such that the action of T is contained in U. Thus subspaces of V that are T-stable are $F[x]$-submodules.	Let T be a linear transformation from vector space V to V. Then an $F[x]$-*module* is the vector space V under the action of polynomials from $F[x]$. The action is of a polynomial $p(x) \in F[x]$ is the linear transformation $p(T)$. There is a bijection between pairs V, T and $F[x]$-modules over V.
Let M, N be R-modules. A map $\varphi : M \to N$ is an R-*module homomorphism* if for all $x, y \in M, r \in R$ $$\varphi(x + ry) = \varphi(x) + r\varphi(y)$$	Let R be a ring and M an R$-$*module*. A subset N of M is submodule of$M$ if and only if 1. $N \neq \emptyset$, and 2. $x + ry \in N$ for all $r \in R, x, y \in N$
Let $r \in R$ and $\varphi \in \mathrm{Hom}_R(M, N)$. Let the action of r on φ be $(r\varphi)(m) = r(\varphi(m))$ for all $m \in M$. Under this action, $\mathrm{Hom}_R(M, N)$ is an R-module.	$\mathrm{Hom}_R(M, N)$ is the set of all R-module homomorphisms from M into N.
The smallest module that contains A and B is the sum, $A + B = \{a + b \mid a \in A, b \in B\}$. Note that we use the *sum* and not the product because we are combining groups, so we combine using the group operation.	True. Since M is an abelian group, N is normal so M/N is a group. Then define the action of R on M/N so that for $r \in R, x + N \in M/N$, $$r(x + N) = (rx) + N.$$ Then we can verify that this is a proper R-module.

Modules

Let M be an R-module and let A be a subset of M. What is the definition of RA, the submodule generated by A?

Algebra Prelim

Modules

Let M be an R-module and N a submodule of M. What does it mean for N to be cyclic?

Algebra Prelim

Modules

True or False: Let M be an R-module and N a submodule of M. Then N has a minimal generating set. Give a proof or counterexample.

Algebra Prelim

Modules

True or False: Let M be an R-module and N a submodule of M. If N has a minimal generating set, then that minimal generating set is unique. Give a proof or counterexample.

Algebra Prelim

Modules

True or False: A submodule of a finitely generated R-module is also finitely generated. Give a proof or counterexample.

Algebra Prelim

Modules

What is the direct product of a finite number of R-modules? What is the external direct sum of a finite number of R-modules?

Algebra Prelim

Modules

What is the direct product of an infinite number of R-modules? What is the direct sum of an infinite number of R-modules?

Algebra Prelim

Modules

Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Suppose the map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ defined by $\pi(n_1, \ldots, n_k) = n_1 + \cdots + n_k$ is an isomorphism of R-modules. State three other equivalent characterizations of this isomorphism.

Algebra Prelim

Modules

What is a free R-module?

Algebra Prelim

Modules

Clearly state the difference between the uniqueness property of direct sums and the uniqueness property of free modules.

Algebra Prelim

A submodule is cyclic if it is finitely generated by exactly 1 element of M, i.e. $N = Ra$ for some $a \in N$.

$RA = \{r_1a_1 + \cdots r_ma_m \mid r_i \in R, a_i \in A, i \in 1, \ldots, m\}$

In other words, RA is the set of all finite R-linear combinations of the elements of A.

False.

If R is a field, then M is a vector space. A minimal generating set for a vector space is a basis, and we know that there are multiple bases that can generate the vector space.

False.

If N is finitely generated, then it has a minimal generating set (not necessarily unique).

$\mathbb{Q}$ as a $\mathbb{Z}$-module has no minimal generating set.

Let $M_1, \ldots, M_k$ be a collection of R-modules. Then the k-tuples $(m_1, m_2, \ldots, m_k)$ where $m_i \in M_i$ with addition and action of R defined componenetwise is the *direct product* of $M_1, \ldots, M_k$, denoted $M_1 \times \cdots \times M_k$.

The *external direct sum* is the same thing but is infuriatingly denoted $M_1 \oplus \cdots \oplus M_k$

False.

Let F be a field and let $R = F[x_1, x_2, \ldots]$, the ring of polynomials in infinitely many variables. Let R be an R-module over itself. Then R is finitely generated by 1 but the submodule generated by $\{x_1, x_2, \ldots\}$ is not finitely generated.

1. M is the direct sum of $N_1, \ldots, N_k$.
2. $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j \in \{1, \ldots, k\}$.
3. Every $x \in N_1 + \cdots + N_k$ can be written uniquely in the form $n_1 + \cdots + n_k$ with $n_i \in N_i$.

Let I be a nonempty index set and for each $i \in I$, let M_i be an R-module. The *direct product* is their direct product as abelian groups with the action of R as componentwise multiplication.

The *direct sum* is the submodule of the direct product where only finitely many of the components m_i are nonzero.

In a direct sum, each element can uniquely be written as a sum of module elements.

In a free module, each element can be uniquely written as an R-linear combination of some generating set (i.e. basis).

An R-module F is *free* on the subset A of F if for every nonzero element $x \in F$, there are unique nonzero elements $r_1, \ldots, r_n \in R$ and unique $a_1, \ldots, a_n \in A$ such that $x = r_1a_1 + \cdots + r_na_n$.

Another way of describing this is to say that A is a basis for F.

Modules

What is the universal property of free modules?

Algebra Prelim

Modules

True or False: If F_1 and F_2 are free R-modules on the same set A, then there is a unique isomorphism between F_1 and F_2 which is the identity map on A. Give a proof or counterexample.

Algebra Prelim

Modules

Let R be an integral domain and let M be a free R-module of finite rank n. Prove that any $n+1$ elements of M are R-linearly dependent.

Algebra Prelim

Modules

Let R a ring and M an R-module. What does it mean for M to be a torsion module?

Algebra Prelim

Modules

Let R a ring and M an R-module. What does it mean for M to be torsion-free?

Algebra Prelim

Modules

Let R an integral domain and M an R-module. What is the torsion submodule denoted $\operatorname{Tor}(M)$?

Algebra Prelim

Modules

Let R be a ring, M be an R-module, and N a submodule of M. What is the annihilator of N?

Algebra Prelim

Modules

True or False: If M is an R-module for some ring R and N, L are submodules, then $N \subseteq L$ implies $\operatorname{Ann} N \subseteq \operatorname{Ann} L$.

Algebra Prelim

Modules

Let R be an integral domain. What is the rank of an R-module M?

Algebra Prelim

Modules

True or False: Let R be an integral domain, M a finitely generated R-module, and N a submodule of M. Then the rank of M is greater than or equal to the rank of N.

Algebra Prelim

True.

Proof sketch: F_1 and F_2 are both a bunch of copies of R indexed by the elements of A, so just map any copy of R to another copy of R.

Let A be a set, R a ring, and $F(A)$ the free R-module on the set A. If M is any R-module and $\varphi : A \to M$ is a set map, there is a unique R-module homomorphism $\psi : F(A) \to M$ such that $\psi(A) = \varphi(A)$.

$$\begin{tikzcd} A \arrow[r] \arrow[dr, "\varphi"'] & F(A) \arrow[d, dashed, "\psi"] \\ & M \end{tikzcd}$$

M is a torsion module if for every $m \in M$, there exists $r \in R$ such that r is not a zero divisor and r annihilates m, i.e. $rm = 0$. In other words, every element of M is a torsion element.

Let $x_1, \dots, x_{n+1} \in M$ be our set of $n + 1$ elements.

R is an integral domain, so embed it in its field of fractions F. Because $M \cong R^n$, we know $M \subseteq F^n$. Since F^n is an n-dimensional vector space, the $n+1$ elements are F-linearly dependent so there exists linear dependence relation with $f_1, \dots, f_{n+1} \in F$ not all zero such that $f_1 x_1 + \cdots f_{n+1} x_{n+1} = 0$. We can obtain an R-linear dependence relation by clearing the denominators.

The *torsion submodule* $\mathrm{Tor}(M)$ is the set of all torsion elements of M.

Note: If R is not commutative, $\mathrm{Tor}(M)$ may fail to be a submodule.

M is torsion free if for $m \in M$ and $r \in R$ where r is not a zero divisor, $rm = 0$ implies that $m = 0$. In other words, the only torsion element of M is 0.

False.

$\mathrm{Ann}(L) \subseteq \mathrm{Ann}(N)$

The *annihilator* of N is the ideal of R defined by

$$\mathrm{Ann}(N) = \{r \in R \mid rn = 0 \text{ for all } n \in N\}$$

False. Consider $\mathbb{Z}[x]$ as a module over itself. Then its rank is one while the rank of its submodule $(2, x)$ is two.

The *rank* of M is the maximum number of R-linearly independent elements of M.

Modules

State the structure theorem for modules over PIDs in invariant factor form.

Algebra Prelim

Modules

State the structure theorem for modules over PIDs in elementary divisor form.

Algebra Prelim

Modules

Let R be a PID and let M be a torsion R-module, $M \neq 0$. What is the p-primary component of M?

Algebra Prelim

Modules

True or False: Every nonzero torsion module over a PID is a direct sum of its p-primary components. Give a proof or counterexample.

Algebra Prelim

Modules

Let R be a PID and p prime in R. Let $F = R/(p)$. Prove that if $M = R^n$, then $M/pM \cong F^n$.

Algebra Prelim

Modules

What is an <u>R-algebra</u>?

Algebra Prelim

Modules

What is meant by the expression "Every R-algebra is also an R-module"?

Algebra Prelim

Modules

What is special about a module over a PID?

Algebra Prelim

Modules

True or False: Let F be a field. Any nonzero free $F[x]$-module is an infinite dimensional vector space over F. Give a proof or counterexample.

Algebra Prelim

Modules

True or False: Let R be a ring and M an R-module. if A is a minimal spanning set for M under R-linear combinations, then A is a basis. Give a proof or counterexample.

Algebra Prelim

Let R be a PID and M a finitely generated R-module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or generated by powers of primes in R, i.e.

$$M \cong R^n \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where n is a nonnegative integer and $p_i^{\alpha_i}$ are positive powers of not-necessarily-distinct primes in R.

Let R be a PID and M a finitely generated R-module. Then

1. $M \cong R^n \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$ where $a_i \in R$ nonzero and $a_1 \mid a_2 \mid \cdots \mid a_m$.
2. M is torsion-free if and only if M is free.
3. $\text{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$

True.

Let M be the aforementioned torsion module. By the structure theorem for modules over PIDs (elementary divisor form), the fact that M is torsion means that its free rank is zero. Then the structure theorem states exactly this - that M is isomorphic to a direct sum of its p-primary components.

p_i-primary component of M

$$= \{x \in M : xp_i^{\alpha} = 0 \text{ where } \alpha > 0\}$$

Let R be a commutative ring. An *R-algebra* is an R-module M together with binary multiplication $M \times M \to M$ (called M-multiplication) satisfying

- $[\alpha x + \beta y, z] = \alpha[x, z] + \beta[y, z]$
- $[z, \alpha x + \beta y] = \alpha[z, x] + \beta[z, y]$

for all scalars $\alpha, beta \in R$ and all elements $x, y, z \in A$.

We will proceed by seeking a R-module homomorphism $\varphi : R^n \to (R/(p))^n$ with kernel pM.

Take $(a_1, \ldots, a_n) \in R^n$ and let $\varphi((a_1, \ldots, a_n)) = (a_1 \mod (p), \ldots, a_n \mod (p))$. This map is clearly surjective. The kernel is the set of elements whose every component are multiples of p, or in other words, pR^n. Thus $M/pM = R^n/pR^n \cong (R/(p))^n = F^n$.

A module over a PID has a decomposition based on the Structure Theorem for Modules over PIDs.

Any R-algebra is an R-module by simply forgetting the multiplicative structure of that R-algebra.

False.

Let $\mathbb{Z}/n\mathbb{Z}$ be a $\mathbb{Z}$-module. This module cannot have a basis because no element is linearly independent, i.e. every element can be multiplied by an appropriate nonzero element of $\mathbb{Z}$ to reach 0. So $1 \in \mathbb{Z}/n\mathbb{Z}$ is a minimal spanning set, yet it fails to be a basis.

True.

Since F is a field, $F[x]$ is a PID. By the Structure Theorem for Modules over PIDs, a free $F[x]$-module is isomorphic to a direct sum of copies of $F[x]$.

MODULES

True or False: Let R be a ring and M an R-module with a finite basis. Then every spanning set in M contains a basis and every linearly independent set in M is contained in a basis.

ALGEBRA PRELIM

MODULES

Give an example of a free module with a submodule that is not free.

ALGEBRA PRELIM

MODULES

True or False: If M is an R-module for some ring R, then M is a free R-module if and only if M has a basis.

ALGEBRA PRELIM

MODULES

For what kind of R-module is is true that we can uniquely define an R-module homomorphism by specifying the values that the elements of a basis map to?

ALGEBRA PRELIM

MODULES

Give an example of a quotient of a free module that is not free.

ALGEBRA PRELIM

MODULES

Give an example of an R-module that cannot be expressed as a direct sum of it submodules.

ALGEBRA PRELIM

MODULES

Let M be an R-module for some ring R and let N, P be submodules. Prove that if $M = N \oplus P$, then $P \cong M/N$.

ALGEBRA PRELIM

MODULES

Let M an R-module for some ring R. What condition needs to be placed on R to guarantee that any two bases of M have the same cardinality and the cardinality of a spanning set is greater than or equal to that of a basis?

ALGEBRA PRELIM

MODULES

Complete the sentence: Let R be a commutative ring with identity. Then two R-modules have the same rank if and only if ____________ .

ALGEBRA PRELIM

MODULES

Let R be PID and let M be a cyclic R-module. Let $\mathrm{Ann}(M)$ be the annihilator of M. Prove that $M \cong R/Ann(M)$.

ALGEBRA PRELIM

The set $\mathbb{Z} \times \mathbb{Z}$ is a free module over itself using componentwise multiplication. We know it is free because the singleton set $\{(1, 1)\}$ serves as a basis. The submodule $\mathbb{Z} \times \{0\}$ is a proper submodule that is not free. We know it is not free because no elements are linearly independent. Any $(a, 0)$ is torsion because multiplying by nonzero element $(0, b)$ will result in $(0, 0)$.	False.
This is true for free R-modules. Only free R-modules have bases anyway!	True.
$\mathbb{Z}$ is a module over itself. Its submodules are the ideals of the ring $\mathbb{Z}$. These are $n\mathbb{Z}$ for $n \in Z$. Given any two submodules $n\mathbb{Z}$ and $m\mathbb{Z}$, we know that their intersection is nontrivial. In fact, their interseciton is $k\mathbb{Z}$ where $k = \operatorname{lcm}(n, m)$. Since there are no submodules that intersect only trivially, this module cannot be expressed as a direct sum.	$\mathbb{Z}$ is a free module over itself because its basis is the set $\{1\}$. $n\mathbb{Z}$ is is a proper submodule that is also free because its basis is the set $\{n\}$. But $\mathbb{Z}/n\mathbb{Z}$ is not a free $\mathbb{Z}$-module because not even a single element is linearly independent.
R needs to be a commutative ring with identity.	Let π be the canonical projection $\pi : M \to P$. Then by the first isomorphism theorem, $M/N \cong P$.
Define the multiplication map φ such that for $r \in R$, $m \in M$, $\varphi(r) = rm$. This is an R-module homomorphism. The map is surjective since M is cyclic. The kernel of this map is the set of elements in R that map every element of M to zero - in other words, $\operatorname{Ann}(M)$. Thus by the first isomorphism theorem, $R/\operatorname{Ann}(M) \cong M$.	they are isomorphic

MODULES

What condition on a ring R guarantees that any submodule of a free R-module is also free?

ALGEBRA PRELIM

MODULES

True or False: Let M be a free module over R and let R be a PID. Let N be a submodule of M. Then any basis for N can be extended to form a basis for M. Give a proof or counterexample.

ALGEBRA PRELIM

MODULES

Let R be a PID, M a free R-module, and N a submodule. What is the closest analogue to the vector space property that there is a basis for M containing a basis for N?

ALGEBRA PRELIM

MODULES

True or False: Any free module over an integral domain is torsion-free. Give a proof or counterexample.

ALGEBRA PRELIM

MODULES

Complete the sentence: A finitely-generated module over a PID is a free module if and only if it is ____________ .

ALGEBRA PRELIM

MODULES

Complete the sentence: Any ____________ module over a PID R is the direct sum of a finitely generated free R-module and a finitely generated torsion R-module

ALGEBRA PRELIM

MODULES

Let R be a PID and M a finitely generated R-module so that $M \cong M_{\text{free}} \oplus M_{\text{tor}}$.
True or False:
(1) M_{free} is unique.
(2) M_{tor} is unique.

ALGEBRA PRELIM

LINEAR ALGEBRA

When does a matrix admit an LU decomposition into lower and upper triangular matrices?

ALGEBRA PRELIM

LINEAR ALGEBRA

What are the vector space axioms for a vector space V over a field F?

ALGEBRA PRELIM

LINEAR ALGEBRA

Fill in the blank: Each conjugacy class of ____________ is represented by exactly one matrix in rational canonical form

ALGEBRA PRELIM

False. $\mathbb{Z}$ is a module over itself and $2\mathbb{Z}$ is a submodule. The set $\{2\}$ is a basis for $2\mathbb{Z}$, but it cannot be extended to a basis for $\mathbb{Z}$.	R is a PID.
True. A free module of rank n over R where R is an integral domain is isomorphic to R^n. Since R is an integral domain, its action on R^n (n copies of itself) must be torsion-free.	Let M be of rank n and let N be of rank $k \leq n$. Then there is a basis $\mathcal{B}$ for M that contains a subset $S = \{v_1, \ldots, v_k\}$ for which $\{r_1 v_1, \ldots, r_k v_k\}$, $r_i \in R$ nonzero, is a basis for N. The elements r_i satisfy the divisility relations $r_1 \mid r_2 \mid \cdots \mid r_k$
finitely generated	torsion-free
An invertible matrix admits an LU decomposition if and only if all of its leading principal minors are nonsingular, i.e. all of the $(n-1) \times (n-1)$ minors are nonsingular.	1. False. M_{free} is unique up to isomorphism, i.e., its rank is unique 2. True. M_{tor} consists of all the torsion elements of M.
$GL_n(F)$ for some field F. This means that you can use RCF to count conjugacy classes in $GL_n(F)$ but not in some subgroup, say $SL_n(F)$.	For $u, v \in V$ and $a, b \in F$, we must have 1. V is a group under addition 2. $a(bv) = (ab)v$ 3. $1v = v$ where $1 \in F$ 4. a(u+v) = au + av 5. (a+b)v = av + bv

Linear Algebra

Given a matrix A, what is the trace of A? What are the three properties that completely characterize a matrix trace?

Algebra Prelim

Linear Algebra

True or False: Given a finite collection of matrices, the trace of their product is the same for any order matrix multiplication.

Algebra Prelim

Linear Algebra

Let V be a vector space over field F and S a subset of V. What does it mean for S to be a linearly independent set of vectors?

Algebra Prelim

Linear Algebra

Let V be a vector space. What is a basis for V?

Algebra Prelim

Linear Algebra

Let V, W be two n-dimensional vector spaces over a field F. Prove that V and W are isomorphic.

Algebra Prelim

Linear Algebra

Let V be a vector space over F and W a subspace of V. What is the dimension of V/W?

Algebra Prelim

Linear Algebra

Let $\varphi : V \to U$ be a linear transformation over F. What is the relationship between $\dim V$, $\dim \ker \varphi$, and $\dim \varphi(V)$?

Algebra Prelim

Linear Algebra

Let V be a k-dimensional vector space over F_q, the finite field with q elements. How many distinct bases of W are there? How does this relate to $|GL(V)|$, the group of invertible linear transformations from V to V?

Algebra Prelim

Linear Algebra

Suppose $\varphi : \mathbb{Q}^3 \to \mathbb{Q}^3$ is a linear transformation such for $x, y, z \in \mathbb{Q}$, $\varphi(x, y, z) = (9x+4y+5z, -4x-3z, -6x-4y-2z)$. Write the matrix representing φ.

Algebra Prelim

Linear Algebra

Let V, W be vector spaces over field F. What is the dimension of $\mathrm{Hom}_F(V, W)$? Give a proof.

Algebra Prelim

False.

The trace is only equal for *cyclic* permutations of the order of multiplication. Thus $\operatorname{trace}(ABC) = \operatorname{trace}(BCA) = \operatorname{trace}(CAB)$ but $\operatorname{trace}(ABC) \neq \operatorname{trace}(ACB)$

The trace of A is the sum along its diagonal. The three properties that completely characterize the trace are

1. $\operatorname{trace}(A + B) = \operatorname{trace}(A) + \operatorname{trace}(B)$
2. $\operatorname{trace}(cA) = c \operatorname{trace}(A)$ for constant c
3. $\operatorname{trace}(AB) = \operatorname{trace}(BA)$

A *basis* for V is a minimal spanning set. It can also be described as a maximal linearly independent set.

S is a *linearly independent* set of vectors if for $\alpha_1, \dots, \alpha_n \in F$ and $v_1, \dots, v_n \in S$, the equation $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ implies that $\alpha_1 = \cdots = \alpha_n = 0$.

$\dim V/W = \dim V - \dim W$

We will prove that V and W are both isomorphic to F^n. Let $v_1, \dots, v_n$ be a basis for V. Define the map

$$\varphi : F^n \to V \qquad by \qquad \varphi(\alpha_1, \dots, \alpha_n) = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

It is clear that φ is F-linear, surjective, and injective. Thus φ is an isomorphism.

There are $(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1})$ distinct bases of V. The first basis vector is one of the $q^k - 1$ nonzero vectors. The second one is a vector not in the span of the first, so there are $q^k - q$ possibilities. The third is not in the span of the first two vectors, so there are $q^k - q^2$ possibilities. We continue this way until we have k vectors.

$|GL(V)|$ is equal to this same number because an invertible map from V maps a fixed basis to any basis of V, so there are exactly as many as distinct bases for V.

$\dim V = \dim \ker \varphi + \dim \varphi(V)$

$\dim \operatorname{Hom}_F(V, W) = (\dim V)(\dim W)$

Pf: $\operatorname{Hom}_F(V, W)$ is isomorphic to the space of $(\dim V) \times (\dim W)$ matrices over F. The space of these matrices has dimension $(\dim V)(\dim W)$.

Erica says: Rows describe where you go. Columns describe where you're fro . . . lum.

$$\begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix}$$

Note that the first row is the coefficient of x, i.e. it's where x "goes". The first column lists the coefficients of x, y, z, thereby describing where the image is "frolum."

Linear Algebra

Let A, B be $n \times n$ matrices. What does it mean if A and B are similar?

Algebra Prelim

Linear Algebra

Let V be a vector space over field F. What is the dual space V^*?

Algebra Prelim

Linear Algebra

Let V be a vector space over field F. Given some basis $\{v_1, \ldots, v_n\}$ of V, what is the dual basis?

Algebra Prelim

Linear Algebra

True or False: Let V be a vector space and V^* its dual space. Then $\dim(V) = \dim(V^*)$.

Algebra Prelim

Linear Algebra

Let V be a vector space over field F. What is the double dual V^{**}?

Algebra Prelim

Linear Algebra

Let V be a finite-dimensional vector space. What does it mean to say that there is a natural isomorphism between V and its double dual V^{**}? What is this isomorphism?

Algebra Prelim

Linear Algebra

Given a matrix $A = (\alpha_{ij})$, what is the determinant?

Algebra Prelim

Linear Algebra

State Cramer's Rule.

Algebra Prelim

Linear Algebra

Let A be an $n \times n$ matrix over an integral domain R. What can we say about the columns of A if $\det A = 0$?

Algebra Prelim

Linear Algebra

True or False: Let A, B be $n \times n$ matrices over a commutative unital ring R. Then $\det AB = (\det A)(\det B)$.

Algebra Prelim

Cherry says: the lying down vectors!

$V^* = \mathrm{Hom}_F(V, F)$, i.e. the space of linear transformations from V to F.

The elements of V^* are called *linear functionals*.

A and B are *similar* if there exists an invertible $n \times n$ matrix P such that $A = P^{-1}BP$.

Geometrically, this means they represent the same linear transformation under a difference choice of basis.

False.

If V is finite dimensional, the statement is true since $\dim V^* = \dim \mathrm{Hom}_F(V, F) = (\dim V)(\dim F) = \dim V$.

If V is infinite dimensional, $\dim(V) < \dim(V^*)$.

The *dual basis* is the set $\{v_1^*, \ldots, v_n^*\}$ such that the action of any element of the dual basis on any element of the basis of V is defined by $v_i^*(v_j) = \delta_{ij}$, i.e. the Kronecker delta.

As the name suggests, the dual basis is a basis for dual space V^*.

It means that specifying an explicit isomorphism between the two spaces does not depend on choosing a basis.

This isomorphism is called *evaluation at v*. Define

$$E_v : V^* \to F \qquad \text{by} \qquad E_v(f) = f(v).$$

Then $\varphi : V \to V^{**}$ such that $\varphi(v) = E_v$ is an isomorphism.

It is the dual of V^*.

Let $A_1, \ldots, A_n$ be the columns of $n \times n$ matrix A. Suppose $B = \beta_1 A_1 + \cdots \beta_n A_n$ for $\beta_1, \ldots, \beta_n \in R$, R a ring. Then

$$\beta_i \det A = \det(A_1, \ldots, A_{i-1}, B, A_{i+1}, \ldots, A_n)$$

The determinant, denoted $\det(A)$, is given by

$$\det(\alpha_{ij}) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} \alpha_{\sigma(i)i}$$

where $\mathrm{sgn}(\sigma)$ is the sign (+ or -) of the permutation σ.

True.

$\det A = 0$ if and only if the columns of A are R-linearly dependent.

Linear Algebra

True or False: If W is any subspace of vector space V, then there exists subspace U such that $V = W \oplus U$. Give a proof or a counterexample.

Algebra Prelim

Linear Algebra

Let T be the matrix of a linear transformation. How does one calculate $\det(T)$ if T is upper triangular?

Algebra Prelim

Linear Algebra

Let T be the matrix of a linear transformation. How does one find the characteristic polynomial of T?

Algebra Prelim

Linear Algebra

What is the significance of the roots of the characteristic polynomial?

Algebra Prelim

Linear Algebra

What is the <u>minimal polynomial</u> of a matrix A?

Algebra Prelim

Linear Algebra

Explain the fact that the rational canonical form of a matrix A is based on an invariant factor decomposition of the finite-dimensional vector space V.

Algebra Prelim

Linear Algebra

True or False: The minimal polynomial is the smallest invariant factor of vector space V.

Algebra Prelim

Linear Algebra

Given an invariant factor $a(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, what is the companion matrix generated by this invariant factor?

Algebra Prelim

Linear Algebra

Let C_i be the companion matrix calculated from invariant factor $a_i(x)$ and let the invariant factors satisfy $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$. How do we form the rational canonical form from these companion matrices?

Algebra Prelim

Linear Algebra

True or False: Let S, T be linear transformations of V. Then S, T are similar if and only if they share the same rational canonical form.

Algebra Prelim

$\det(T) =$ the product along the diagonal

True. Every subspace has a complement.

Let B_W be a basis for W. We can extend it to form a basis for V. Let this basis for V be called B_V. Then U is the span of $B_V \setminus B_W$. By the construction of B_V, it is clear that $V = W \oplus U$.

They are eigenvalues.

The characteristic polynomial is $\det(xI - T)$.

Given a particular matrix A, V is an $F[x]$-module. Since $F[x]$ is a PID (actually it's Euclidean), we can use the structure theorem for modules over PIDs. Then

$$V \cong F[x]/(a_1(x)) \oplus F[x]/(a_2(x)) \oplus \cdots \oplus F[x]/(a_m(x))$$

where the generators of the quotienting ideals are invariant factors.

The *minimal polynomial* $m(x)$ is the unique monic polynomial of lowest degree such that $m(A) = 0$ (the zero operator)

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -b_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -b_{n-1} \end{pmatrix}$$

False.

It is the largest invariant factor. All other invariant factors must divide it.

True.

$$\begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_m \end{pmatrix}$$

LINEAR ALGEBRA

True or False: Let A be an $n \times n$ matrix over field F and let K be an extension of F. Then the rational canonical forms of A over K and over F are the same.

ALGEBRA PRELIM

LINEAR ALGEBRA

What is an $\underline{n \times n \text{ Jordan block for eigenvalue } \lambda}$?

ALGEBRA PRELIM

LINEAR ALGEBRA

Complete the sentence: A matrix is diagonalizable if and only if its Jordan canonical form is ____________ .

ALGEBRA PRELIM

LINEAR ALGEBRA

In what sense is the Jordan canonical form of a matrix unique?

ALGEBRA PRELIM

LINEAR ALGEBRA

What does it mean for a matrix to be in <u>Jordan canonical form</u>?

ALGEBRA PRELIM

LINEAR ALGEBRA

True or False: Two diagonal matrices are similar if and only if their diagonal entries are the same up to a permutation.

ALGEBRA PRELIM

LINEAR ALGEBRA

A matrix M is diagonalizable if and only if what condition is placed on its minimal polynomial? Give a proof.

ALGEBRA PRELIM

FIELDS

In what fields does that quadratic formula apply?

ALGEBRA PRELIM

FIELDS

Let L/F be a finite extension of fields. For $\alpha \in L$, left multiplication by α is an F-linear transformation of F. What is the relationship between the field norm of α and this linear transformation induced by α?

ALGEBRA PRELIM

FIELDS

Let L/F be a finite extension of fields. For $\alpha \in L$, what is the field norm $N_{L/F}(\alpha)$?

ALGEBRA PRELIM

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$	True.
It is unique up to permutation of the Jordan blocks.	diagonal
True. If their diagonal entries are the same up to permutation, then their Jordan canonical forms are the same, which means they are similar.	A matrix is in *Jordan canonical form* if it is block diagonal and each block is a Jordan block.
The quadratic formula applies in any field that is not of characteristic 2.	Its minimal polynomial $m(x)$ must have no repeated roots. ($\Longleftarrow$) If $m(x)$ has no repeated roots, by the divisibility conditions of invariant factors, the elementary divisors are linear polynomials. Thus the JCF of M is diagonal ($\Longrightarrow$) If M is similar to a diagonal matrix D, then M and D have the same minimal polynomial. The minimal polynomial of D must contain all distinct linear factors, each corresponding to the 1×1 blocks that make up D.
Let $f(x)$ be the minimal polynomial for α over F. Let $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ be the roots (counted with multiplicity) of $f(x)$. Then $$N_{L/F}(\alpha) = \left(\prod_{j=1}^{n} \sigma_j(\alpha)\right)^{[L:F(\alpha)]}$$ i.e., it is the product of all Galois conjugates of α. One can also think of it as the constant term of the minimal polynomial times $(-1)^n$ where n is the degree of $f(x)$.	Let T be the matrix that represents the linear transformation. Then the field norm of α is the determinant of T.

Fields

Let K/F be a finite extension of fields. For $\alpha \in K$, left multiplication by α on K is an F-linear transformation T_α of K. How does the minimal polynomial of α over F relate to T_α?

Algebra Prelim

Fields

Let K/F be a finite extension of fields. For $\alpha \in K$, left multiplication by α on K is an F-linear transformation T_α of K. What is the trace $Tr_{K/F}(\alpha)$? How does $Tr_{K/F}(\alpha)$ relate to T_α?

Algebra Prelim

Fields

Let K/F be a finite extension of fields. For $\alpha \in K$, left multiplication by α is an F-linear transformation of F. What is the relationship between $Tr_{K/F}(\alpha)$ and this linear transformation induced by α?

Algebra Prelim

Fields

Let F_{p^n} and F_{p^m} be finite fields of characteristic p. What is the smallest finite field that contains both of them? Give a proof.

Algebra Prelim

Fields

For what type of polynomial is is true that the polynomial is irreducible if and only if it does not have a root in field F?

Algebra Prelim

Fields

State the rational roots theorem

Algebra Prelim

Fields

Let G be a finite subgroup of the multiplicative group of a field. What property does G have? Give an example for the field F_p for prime p.

Algebra Prelim

Fields

True or False: In a finite field, adjoining one root of an irreducible polynomial results in the splitting field of the polynomial.

Algebra Prelim

Fields

What is the characteristic of a field?

Algebra Prelim

Fields

What is the characteristic of a field in terms of its prime subfield?

Algebra Prelim

Let $f(x)$ be the minimal polynomial for α over F. Let $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ be the roots (counted with multiplicity) of $f(x)$. Then $$Tr_{K/F}(\alpha) = \left(\sum_{j=1}^{n} \sigma_j(\alpha)\right)^{[L:F(\alpha)]}$$ i.e., it is the sum of all Galois conjugates of α. One can also think of it as the coefficient of the second-highest degree term of $f(x)$ times -1.	The minimal polynomial of α over F is equal to the minimal polynomial of the matrix T_α.
Let $k = \text{lcm}(n, m)$. Then the smallest finite field that contains both fields if F_{p^k}. F_n contains the n roots of $x^{p^n} - x$ and F_m contains the m roots of $x^{p^m} - x$. The smallest polynomial of the form $x^{p^k} - x$ that is divisible by both $x^{p^n} - x$ and $x^{p^m} - x$ is the one where $k = \text{lcm}(n, m)$. Thus the smallest field that contains both fields is F_{p^k}.	$Tr_{K/F}(\alpha)$ is equal to the trace (matrix trace, i.e. sum along diagonal) of the matrix that represents the linear transformation.
Let $p(x)$ be a polynomial with integer coefficients. For $r/s \in \mathbb{Q}$, r/s is a root of $p(x)$ if and only if r divides the constant term and s divides the leading coefficient.	A polynomial of degree 2 or 3, since these are the only kinds that factor if and only if they have a linear factor.
True.	G is cyclic. For F_p, its group of units $F_p^\times$ is a finite subgroup of the multiplicative group of a field. Therefore, $F_p^\times$ is cyclic.
$\text{char}(F) = 0$ if and only if its prime subfield is isomorphic to $\mathbb{Q}$ $\text{char}(F) = p$ if and only if its prime subfield is isomorphic to $\mathbb{F}_p$.	Let F be a field. Then its *characteristic*, $\text{char}(F)$, is the smallest positive integer p such that $p \cdot \alpha = 0$ for all $\alpha \in F$. If no such p exists, $\text{char}(F) = 0$

Fields

What is the prime subfield of a field F?

Algebra Prelim

Fields

What is a field extension of a field F?

Algebra Prelim

Fields

What is the degree of an extension K/F?

Algebra Prelim

Fields

Let $\varphi : F \to F'$ be a homomorphism of fields. What can we say about φ?

Algebra Prelim

Fields

What is a splitting field for an irreducible polynomial $p(x) \in F[x]$?

Algebra Prelim

Fields

Let $p(x) \in F[x]$ be an irreducible polynomial of degree n and let $K = F[x]/(p(x))$. What is one convenient basis for representing K as a vector space over F?

Algebra Prelim

Fields

What is a simple extension of field F?

Algebra Prelim

Fields

Let K be a finite extension over field F. Name two conclusions that can be drawn from this statement.

Algebra Prelim

Fields

What does it mean for an element α to be algebraic over field F? What does it mean for extension K to be algebraic over F?

Algebra Prelim

Fields

Let α be an algebraic element over field F. What is $m_{\alpha,F}(x)$, the minimal polynomial of α?

Algebra Prelim

A *field extension* of a field F is a field K such that $F \subseteq K$. This extension is denoted K/F.

The *prime subfield* of a field F is the subfield generated by 1_F. It is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$.

φ is either an injective or the zero map. This is because the kernel of the homomorphism must be an ideal of F (viewed as a ring), but F has only 0 and F as ideals.

The *degree* of extension K/F is the dimension of K as a vector space over F.

Let $\theta = x \mod (p(x))$. Then $1, \theta, \theta^2, \ldots, \theta^{n-1}$ can serve as a basis for K as a vector space over F.

The splitting field for $p(x)$ is the field $F[x]/(p(x))$.

1. K is algebraic over F, so every element in K is the root of some polynomial in $F[x]$.
2. K is generated by a finite number of algebraic elements over F.

A *simple* extension is a field K/F that is generated by a single element, i.e. $K = F(\alpha)$.

The minimal polynomial $m_{\alpha,F}(x)$ is the unique monic irreducible polynomial in $F[x]$ with α as a root.

An element α is *algebraic* over F if α is the root of some polynomial in $F[x]$. K/F is *algebraic* if every element of K is algebraic over F

Fields

Let $p(x) \in F[x]$ have α as a root. What can we say about the minimal polynomial of α?

Algebra Prelim

Fields

True or False: If K/F is an extension of fields and α is algebraic over both K and F, then $m_{\alpha,F}(x)$ divides $m_{\alpha,K}(x)$.

Algebra Prelim

Fields

Let F be a field and let α be algebraic over F. What is the degree of α?

Algebra Prelim

Fields

Let α be algebraic over field F. Prove that $[F(\alpha) : F] = \deg(\alpha)$

Algebra Prelim

Fields

Complete the sentence: The field extension $F(\alpha)/F$ is finite if and only if ____________ .

Algebra Prelim

Fields

What is the tower rule for field extensions?

Algebra Prelim

Fields

What does it mean for a field extension K/F to be finitely generated?

Algebra Prelim

Fields

(Artin's Theorem) Complete the sentence: Let K/F be a finite extension. Then $K = F(\alpha)$ for some $\alpha \in K$ if and only if ____________ .

Algebra Prelim

Fields

What condition on field extension K/F guarantees that $K = F(\alpha)$ for some $\alpha \in K$? What can we say if the base field is of characteristic 0?

Algebra Prelim

Fields

Suppose α, β are algebraic over F. Prove that $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ $(\beta \neq 0)$ are all algebraic over F.

Algebra Prelim

False. $m_{\alpha,K}(x)$ divides $m_{\alpha,F}(x)$	The minimal polynomial of α divides $p(x)$.
Let $deg(\alpha) = n$. Since $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$, we know $F(\alpha)$ can be viewed as polynomials of degree $n-1$, which is a vector space of dimension n over F.	The *degree* of α is the degree of its minimal polynomial.
Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K][K : F]$. Nat calls it "Lagrange's for fields"	α is algebraic over F
there exist finitely many intermediate fields (alternatively) if the extension is finite and separable.	K/F is finitely generated if there are elements $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$.
All of these elements lie in $\mathbb{F}(\alpha, \beta)/F$. Since this extension over F is generated by finitely many algebraic elements, the extension is finite. A finite extension is always algebraic, and thus every above-listed element is algebraic.	The conclusion holds if K/F is a finite separable extension. If the base field is of characteristic zero, then every extension is separable, so any finite extension is a simple extension.

FIELDS

If K_1, K_2 are subfields of field K, what is the composite field *K_1K_2?*

ALGEBRA PRELIM

FIELDS

True or False: If K_1, K_2 are finite extensions of F contained in K, then $[K_1K_2 : F] \le [K_1 : F][K_2 : F]$. Give a proof or counterexample.

ALGEBRA PRELIM

FIELDS

Let K_1, K_2 be finite extensions of F contained in K. Let $[K_1 : F] = n$, $[K_2 : F] = m$, and $(n, m) = 1$. Prove that $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

ALGEBRA PRELIM

FIELDS

Prove that if $[F(\alpha) : F]$ is odd, then $F(\alpha) = F(\alpha^2)$.

ALGEBRA PRELIM

FIELDS

Complete the sentence: Let $F \subset \mathbb{R}$. Then $\alpha \in R$ can be obtained by compass and straightedge constructions if and only if ____________ .

ALGEBRA PRELIM

FIELDS

Prove that given a cube, one cannot construct another cube with double the volume by using compass and straightedge constructions.

ALGEBRA PRELIM

FIELDS

Complete the sentence: The regular n-gon is constructible by compass and straightedge constuctions if and only if ____________ .

ALGEBRA PRELIM

FIELDS

What is a Fermat prime*?*

ALGEBRA PRELIM

FIELDS

What is a splitting field*?*

ALGEBRA PRELIM

FIELDS

What is a normal *extension?*

ALGEBRA PRELIM

True.

K_1, K_2 are finite extensions, so they are finitely generated. Say $K_1 = F(\alpha_1, \ldots, \alpha_n)$ and $K_2 = F(\beta_1, \ldots, \beta_m)$. Then $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = K_1(\beta_1, \ldots, \beta_m)$. This means $\{\beta_i\}$ spans K_1K_2 over K_1, so $[K_1K_2 : K_1] \leq m$. Then applying the tower rule completes the proof.

Note: The inequality becomes an equality if and only if an F-basis for one of the fields remains linearly independent over the other field.

K_1K_2 is the smallest subfield of K that contains K_1 and K_2.

Clearly $F(\alpha^2) \subseteq F(\alpha)$. Then $[F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ is odd. The minimal polynomial for α over $F(\alpha^2)$ is of degree at most 2 since α is a root of $x^2 - \alpha^2$.

If $m_\alpha(x)$ is of degree 2, then $[F(\alpha) : F(\alpha^2)] = 2$, which contradicts that $[F(\alpha) : F(\alpha^2)][F(\alpha)^2 : F]$ is odd. Thus $m_\alpha(x)$ is of degree 1 and $\alpha \in F(\alpha^2)$.

K_1 and K_2 are subfields of K_1K_2, so both n and m divide $[K_1K_2 : F]$. Then $[K_1K_2 : F]$ is divisible by $\text{lcm}(n, m) = nm$. Finally since it is known that $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$, we conclude $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

Suppose the original cube has side length 1. Then a cube with double the volume has side length $\sqrt[3]{2}$. This element has degree 3 over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \neq 2^k$ for nonnegative integer k. Thus the cube of doubled volume is not constructible.

$[F(\alpha) : F] = 2^k$ for some integer $k \geq 0$

A *Fermat prime* is a prime number of the form $2^{2^n} + 1$ for nonnegative integer n.

$n = 2^k p_1 \cdots p_r$ where k is a nonnegative integer and $p_1, \ldots, p_r$ are distinct Fermat primes.

Let K be an algebraic extension of F. If K is the splitting field for some collection of polynomials $f(x) \in F[x]$, then K is a *normal* extension.

Let K be an extension of F. Then K is a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors into linear factors in $K[x]$ and fails to factor completely in any proper subfield of K containing F.

FIELDS

Complete the sentence: Let $f(x) \in F[x]$ be a polynomial of degree n. Then adjoining one root of $f(x)$ to F generates an extension of degree n if and only if ____________ .

ALGEBRA PRELIM

FIELDS

Let $f(x) \in F[x]$ be of degree n. What is the largest possible degree of the extension that is the splitting field of $f(x)$?

ALGEBRA PRELIM

FIELDS

What is a <u>primitive</u> root of unity?

ALGEBRA PRELIM

FIELDS

How many n^{th} roots of unity are primitive roots of unity?

ALGEBRA PRELIM

FIELDS

What is the <u>cyclotomic field of n^{th} roots of unity</u>?

ALGEBRA PRELIM

FIELDS

Let ζ_p be a primitive p^{th} root of unity for prime p. What is the minimal polynomial for ζ_p?

ALGEBRA PRELIM

FIELDS

What is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ where ζ_n is a primitive n^{th} root of unity?

ALGEBRA PRELIM

FIELDS

What is an <u>algebraic closure</u> of F?

ALGEBRA PRELIM

FIELDS

What is a <u>separable</u> polynomial?

ALGEBRA PRELIM

FIELDS

How can we use the derivative to check whether a polynomial is separable?

ALGEBRA PRELIM

The splitting field is an extension of degree at most $n!$.	$f(x)$ is irreducible over F
$\varphi(n)$, where φ is the Euler φ-function.	A generator in the cyclic group of all n^{th} roots of unity is called a *primitive* n^{th} root of unity.
It is $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$.	$\mathbb{Q}(e^{2\pi i/n})$
The field $\overline{F}$ is an *algebraic closure* of F if $\overline{F}$ is algebraic over F and every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$.	$\varphi(n)$, where φ is the Euler φ-function.
Let $f(x)$ be a polynomial. Then $f(x)$ is separable if and only if $f(x)$ and $f'(x)$ share no common factors.	A polynomial over field F is *separable* if it has no multiple roots.

Fields

Prove that every irreducible polynomial over a field of characteristic 0 is separable. Explain why this proof fails in fields of characteristic p.

Algebra Prelim

Fields

What is the Frobenius endomorphism of F?

Algebra Prelim

Fields

Let F be a field of characteristic p. Prove that the Frobenius map is a bijection.

Algebra Prelim

Fields

What is a perfect field?

Algebra Prelim

Fields

List several equivalent characterizations of a perfect field F.

Algebra Prelim

Fields

True or False: All fields of characteristic zero and all finite fields are perfect.

Algebra Prelim

Fields

Complete the sentence: Every irreducible polynomial over a ____________ field is separable.

Algebra Prelim

Fields

True or False: Finite fields of any order p^n are unique up to isomorphism. Give a proof or counterexample.

Algebra Prelim

Fields

Let $f(x)$ be an irreducible polynomial over a field F of characteristic p. Prove that there is a unique integer $k \geq 0$ and unique irreducible separable polynomial $f_{sep}(x) \in F[x]$ such that $f(x) = f_{sep}\left(x^{p^k}\right)$.

Algebra Prelim

Fields

Let $f(x)$ be irreducible over a field F of characteristic p. What is the separable degree of $f(x)$? What is the inseparable degree of $f(x)$?

Algebra Prelim

Let F be a field of characteristic p. The *Frobenius endomorphism* is the map $\varphi : F \to F$ such that $\varphi(\alpha) = \alpha^p$.	Let F be of characteristic zero and $p(x) \in F[x]$ is irreducible of degree n. The only factors of $p(x)$ are 1 and $p(x)$. The derivative $p'(x)$ has factors of degree at most $n-1$. Thus the only factor that $p(x)$ and $p'(x)$ can share is 1. Thus $p(x)$ is separable. In a field of characteristic p, the derivative of x^{pm} is zero, so the degree of the derivative may drop more than 1. However, if $p'(x)$ is nonzero (and $p(x)$ is irreducible as before), then $p(x)$ is separable.
A field K of characteristic p is perfect if every element of K is a p^{th} power in K. Any field of characteristic 0 is also perfect.	Let $\varphi(a) = a^p$ for $a \in F$ be the Frobenius map. Since φ is a map between fields, the map is injective. Also, φ maps F to itself so injectivity is enough to prove that φ is a bijection.
True.	TFAE: • F is perfect • Every irreducible polynomial over F has distinct roots • Every irreducible polynomial over F is separable • Every finite extension of F is separable • Every algebraic extension of F is separable • Either F has characteristic 0 or when F has characteristic p, then every element is a p^{th} power
True. A finite field of order p^n is the splitting field over $\mathbb{F}_p$ of the polynomial $x^{p^n} - x$. All splitting fields are unique up to isomorphism.	perfect
Let $f_{sep}(x)$ be the unique irreducible separable polynomial in $F[x]$ such that $f(x) = f_{sep}\left(x^{p^k}\right)$. The *separable degree of* $f(x)$ is the degree of $f_{sep}(x)$. The *inseparable degree of* $f(x)$ is the integer p^k. *Note:* These definitions only make sense for *irreducible* polynomials!	If $f(x)$ is separable, then $f = f_{sep}$. If $f(x)$ is not separable, then $f'(x) = 0$ and every power of x in $f(x)$ is a multiple of p. Thus there exists polynomial $f_1(x)$ such that $f(x) = f_1(x^p)$. Continue this process until $f_k(x)$ is separable (i.e. has nonzero derivative). Such an f_k is clearly irreducible since any factorization of f_k would produce a corresponding factorization of f. This f_k is the f_{sep} we seek.

FIELDS *What is a separable field extension?* ALGEBRA PRELIM	FIELDS *What is the n^{th} cyclotomic polynomial $\Phi_n(x)$?* ALGEBRA PRELIM
FIELDS *Prove that if a field contains the n^{th} roots of unity for n odd, then it also contains the $2n^{th}$ roots of unity.* ALGEBRA PRELIM	FIELDS *Let K/F be an extension of fields. What is $\mathrm{Aut}(K/F)$?* ALGEBRA PRELIM
FIELDS *Let K/F be a field extension and $\alpha \in K$ be algebraic over F. Let $\sigma \in \mathrm{Aut}(K/F)$. What can we say about $\sigma(\alpha)$?* ALGEBRA PRELIM	FIELDS *What is the fixed field of a set of automorphisms H?* ALGEBRA PRELIM
FIELDS *True or False: Let K/F be an extension of fields. Then $[K : F] \leq \mathrm{Aut}(K/F)$. Give a proof or counterexample.* ALGEBRA PRELIM	FIELDS *What is a Galois extension?* ALGEBRA PRELIM
FIELDS *List five equivalent characterizations of K/F being a Galois extension.* ALGEBRA PRELIM	FIELDS *What is the Galois group of the splitting field of $x^3 - 2$ over $\mathbb{Q}$?* ALGEBRA PRELIM

Let μ_n be the group of n^{th} roots of unity over $\mathbb{Q}$.

$$\Phi_n(x) = \prod_{\zeta \text{ primitive } \in \mu_n} (x - \zeta) = \prod_{\substack{1 \le a < n \\ (a,n)=1}} (x - \zeta_n^a)$$

In other words, it is the polynomial whose roots are exactly the primitive n^{th} roots of unity.

A field K is *separable* over F if every element of K is the root of a separable polynomial over F. Equivalently, K is separable if every element of K has a separable minimal polynomial over F.

$\mathrm{Aut}(K/F)$ is the group (under composition) of automorphisms of K that fix every element of F.

Notice $x^{2n} - 1 = (x^n - 1)(x^n + 1)$. Let ζ be a root of $x^n - 1$. Then $-\zeta$ is a root of $x^n + 1$. Thus any field with the n^{th} roots of unity also contains the $2n^{th}$ roots of unity.

Geometrically, we can see that the set of roots of $x^n + 1$ is a rotation of the roots of $x^n - 1$ by $180°$.

Let K be a field and let H be a subset of $\mathrm{Aut}(K)$. Then the *fixed field* of H is the subfield of K such that H fixes all the elements of this subfield.

$\sigma(\alpha)$ is a root of the minimal polynomial of α.

Let K/F be a finite extension. Then K is *Galois* over F if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, then the group of automorphisms is denoted $\mathrm{Gal}(K/F)$.

False.

Let $\alpha = \sqrt[3]{2}$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, but $|\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 1$. To see this, recall $m_\alpha(x) = x^3 - 2$. In the splitting field K of $m_\alpha(x)$, $\mathrm{Aut}(K/\mathbb{Q})$ would shuffle the three roots. But $\mathbb{Q}(\alpha)/\mathbb{Q}$ contains the only real root, so automorphisms that fix the base field can only map α to itself. Hence $|\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 1$.

Let $\alpha = \sqrt[3]{2}$, $\zeta = e^{2\pi i/3}$. The splitting field is $\mathbb{Q}(\alpha, \zeta)$. Then

$$\begin{aligned}[\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}] &= [\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \\ &= 2 \cdot 3 \\ &= 6.\end{aligned}$$

Since the extension is of degree 6, the Galois group has 6 elements. Our polynomial has 3 roots, so the Galois group must be a subgroup of S_3. By considerations regarding order, the Galois group must be S_3.

TFAE:

- K/F is Galois
- $|\mathrm{Aut}(K/F)| = [K : F]$
- K is the splitting field over F for a separable polynomial
- K/F is algebraic and F is the fixed field of $\mathrm{Aut}(K/F)$
- Every irreducible polynomial in $F[x]$ with one root in K splits over K and is separable.
- K/F is a normal, separable, and finite extension.

Fields

True or False: A Galois extension of a Galois extension is also Galois. Give a proof or counterexample.

Algebra Prelim

Fields

True or False: Any quadratic extension K/F is Galois.

Algebra Prelim

Fields

What is a Galois conjugate?

Algebra Prelim

Fields

Let K/F be a Galois extension and $G = \mathrm{Gal}(K/F)$. Let E be a subfield of K containing F. Draw and label the lattices for K/F and G according to the Fundamental Theorem of Galois Theory,

Algebra Prelim

Fields

Let K/F be a Galois extension and $G = \mathrm{Gal}(K/F)$. Let E be a subfield of K containing F. According to the Fundamental Theorem of Galois Theory, E/F is Galois under what condition? What is the Galois group?

Algebra Prelim

Fields

Let K/F be a Galois extension and $G = \mathrm{Gal}(K/F)$. Let E be a subfield of K containing F. Let $H = \mathrm{Gal}(K/E)$. According to the Fundamental Theorem of Galois Theory, what can be said about the cosets of H in G?

Algebra Prelim

Fields

Give an example of a field that is not perfect.

Algebra Prelim

Fields

What is the degree of the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$?

Algebra Prelim

Fields

True or False: The field $\mathbb{F}_{p^n}$ is always Galois over $\mathbb{F}_p$. Give a proof or counterexample.

Algebra Prelim

Fields

What is the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$?

Algebra Prelim

Almost true.

It is true if F is not of characteristic 2

False.

$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are both Galois because they are both quadratic extensions of a field with characteristic $\neq 2$. But $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois.

$$g\left[\begin{array}{l} h\left[\begin{array}{c} K \\ | \\ E \end{array}\right. \\ \quad\;\; | \\ \quad\;\; F \end{array}\right. \qquad \begin{array}{c} \{1\} \\ | \\ H = \mathrm{Gal}(K/E) \\ \text{(has order } h) \\ | \\ G = \mathrm{Gal}(K/F) \\ \text{(has order } g) \end{array}$$

Let K/F be a Galois extension. If $\alpha \in K$, then the elements $\sigma(\alpha)$ for any $\sigma \in \mathrm{Gal}(K/F)$ are the Galois conjugate of α over F. In other words, the Galois conjugates are the other roots of the minimal polynomial of α.

There is a one-to-one correspondence between the isomorphisms of E that fix F and the cosets of H in G.

If $H \trianglelefteq G$, then $\mathrm{Aut}(E/F) = \mathrm{Gal}(E/F) \cong G/H$.

E/F is Galois if and only if $\mathrm{Aut}(E/F) \trianglelefteq G = \mathrm{Gal}(K/F)$.

$\mathrm{Gal}(E/F) \cong G/H$ where $H = \mathrm{Gal}(K/E)$

$[\mathbb{F}_{p_n} : \mathbb{F}_p] = n$

Since all fields of characteristic 0 and all finite fields are perfect, we seek an infinite field of characteristic p. Recall that a field is perfect if and only if every irreducible polynomial is separable.

Consider $\mathbb{F}_p(t)$, the field of rational functions in transcendental t. The polynomial $x^p - t \in \mathbb{F}_p(t)[x]$ is irreducible by Eisenstein's using the prime element t. Let α be a root. Then $\alpha^p = t$, so $x^p - \alpha^p = (x-\alpha)^p$, which is not separable.

It is the cyclic group of order n generated by the Frobenius automorphism, i.e.

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$

where $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ so that $\sigma_p(\alpha) = \alpha^p$.

True.

$\mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^n} - x$ and hence it is a Galois extension.

Fields

Under what condition on n, m is is true that $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$?

Algebra Prelim

Fields

Prove that the irreducible polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime.

Algebra Prelim

Fields

Let $p(x)$ be irreducible over $\mathbb{F}_{p^n}$ and let α be a root of $p(x)$. What can we say about the field $\mathbb{F}_{p^n}(\alpha)$? Give a proof.

Algebra Prelim

Fields

Describe one method for recursively producing irreducible polynomials over $\mathbb{F}_p$.

Algebra Prelim

Fields

Prove that $x^{p^n} - x$ is the product of all irreducible polynomials over $\mathbb{F}_p$ with degree d dividing n.

Algebra Prelim

Fields

What is the <u>algebraic closure of $\mathbb{F}_p$</u>?

Algebra Prelim

Fields

Suppose K/F is Galois and F'/F is any extension. Prove that KF'/F' is also Galois. What is its Galois group?

Algebra Prelim

Fields

Complete the formula: Suppose K/F is Galois and F'/F is any extension.
Then $[KF' : F] =$ ______________ .

Algebra Prelim

Fields

Let K_1, K_2 be Galois extensions of a field F. Prove that $K_1 \cap K_2$ is Galois over F.

Algebra Prelim

Fields

Let K_1, K_2 be Galois extensions of F. Is K_1K_2 Galois? If so, what is its Galois group?

Algebra Prelim

If $p = 2$, then $x^4 + 1 = (x + 1)^4$ and so it is reducible.

If p is odd, note that $p^2 - 1$ is divisible by 8. Thus $x^{p^2-1} - 1$ is divisible by $x^8 - 1$. Then

$$x^4 + 1 \mid x^8 - 1 \mid x^{p^2-1} - 1 \mid x^{p^2} - x,$$

the last of which generates $\mathbb{F}_{p^2}$, an extension of degree 2. So any extension generated by a root of $x^4 + 1$ is of degree at most 2, which means it is not irreducible over $\mathbb{F}_p$.

This is true only when n divides m.

$x^{p^n} - x$ is precisely the product of all irreducible polynomials over $\mathbb{F}_p$ of degree d dividing n.

For example, say we seek all irreducible degree 6 polynomials over $\mathbb{F}_3$. Since $1, 2, 3, 6$ are the divisors of 6, take $x^{3^6} - x$ and divide by all irreducible polynomials of degrees 1, 2, and 3. The divisors of the quotient are all the irreducible degree 6 polynomials.

$\mathbb{F}_{p^n}(\alpha)$ is the splitting field for $p(x)$

Let $\deg(p(x)) = d$. Then $[\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_{p^n}] = d$ and since all finite fields of a particular order are isomorphic, $\mathbb{F}_{p^n}(\alpha) \cong \mathbb{F}_{p^{nd}}$. Thus α is a root of $x^{p^{nd}} - x$. Since $x^{p^{nd}} - x$ contains precisely all irreducible polynomials of degree dividing nd, we know $p(x) \mid x^{p^{nd}} - x$ and so all roots of $p(x)$ are in $\mathbb{F}_{p^n}(\alpha)$.

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$$

The roots of $\mathbb{F}_{p^n}$ are precisely the roots of $x^{p^n} - x$. We know that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if $d \mid n$. Extending $\mathbb{F}_p$ to the splitting field of any degree d irreducible polynomial will result in $\mathbb{F}_{p^d}$ since all finite fields of the same size are isomorphic. Thus every minimal polynomial of degree d splits in $\mathbb{F}_{p^d}$. Grouping together all minimal polynomials of the same degree, we see that their product is $x^{p^n} - x$.

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}$$

K/F is Galois, so $\exists$ separable $p(x)$ such that K is its splitting field. This same polynomial is separable over F', so its splitting field over F' is KF'. Thus KF'/F' is Galois.

$$\begin{tikzcd}[arrows=dash] & KF' \arrow[dl] \arrow[dr] & \\ K \arrow[dr] & & F' \arrow[dl] \\ & K \cap F' \arrow[d] & \\ & F & \end{tikzcd}$$

$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$$

Yes, K_1K_2 is Galois.

Its Galois group is isomorphic to the subgroup

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

of the direct product $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to the intersection $K_1 \cap K_2$ are equal.

Recall that an extension is Galois if and only any irreducible polynomial that has at least one root in the extension splits completely in the extension.

Let $p(x)$ be irreducible in $F[x]$ with a root α in $K_1 \cap K_2$. By the above characterization of Galois extensions, all roots of $p(x)$ are in both K_1 and K_2. But then all roots of $p(x)$ are in $K_1 \cap K_2$ and so $K_1 \cap K_2$ is Galois.

FIELDS

What is the Galois closure of finite separable extension E/F?

ALGEBRA PRELIM

FIELDS

Prove that if K/F is finite and separable, then K/F is simple.

ALGEBRA PRELIM

FIELDS

What is a separable field extension?

ALGEBRA PRELIM

FIELDS

Prove that any finite field extension over a field of characteristic 0 is simple.

ALGEBRA PRELIM

FIELDS

Let $\mathbb{Q}(\zeta_n)$ be the cyclotomic field of n^{th} roots of unity. What is its Galois group?

ALGEBRA PRELIM

FIELDS

Let $\mathbb{Q}(\zeta_p)$ be the cyclotomic field extension over $\mathbb{Q}$ for prime p. What is the Galois group of this extension?

ALGEBRA PRELIM

FIELDS

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the factorization of positive integer n into distinct prime powers. Prove that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{\alpha_1}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{\alpha_k}})/\mathbb{Q})$.

ALGEBRA PRELIM

FIELDS

What is an abelian field extension?

ALGEBRA PRELIM

FIELDS

Let G be a finite abelian group. Prove that there is a field $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

ALGEBRA PRELIM

FIELDS

What is the discriminant of a polynomial?

ALGEBRA PRELIM

Let L be the Galois closure of K/F. By the Fundamental Theorem of Galois Theory, any intermediate field between K and F corresponds to a subgroup of $\mathrm{Gal}(L/F)$. Since there are finitely many subgroups, there are also finitely many intermediate fields. By Artin's Theorem, K/F is simple.	The *Galois closure* is an extension K/F which is Galois over F and is minimal in the sense that in a fixed algebraic closure of K, any other Galois extension of F containing E contains K. Note that the Galois closure is defined for *finite separable* extensions.
Any finite extension K/F of a field of characteristic 0 is separable. If the extension is finite and separable, we can consider its Galois closure. The corresponding Galois group of this Galois closure has finitely many subgroups and thus K/F has only finitely many intermediate fields. By Artin's Theorem, K/F is simple.	A field extension is *separable* if the minimal polynomial of every element is separable.
The cyclic group $\mathbb{Z}/(p-1)\mathbb{Z}$.	Its Galois group is the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.
The extension K/F is called *abelian* if K/F is Galois and $\mathrm{Gal}(K/F)$ is an abelian group.	Note that $\zeta_n^{p_2^{\alpha_2}\cdots p_k^{\alpha_k}}$ is a primitive $p_1^{\alpha_1}$-th root of unity, so the field $\mathbb{Q}(\zeta_{p_1^{\alpha_1}})$ is a subfield of $\mathbb{Q}(\zeta_n)$. The same applies to the other prime powers. Their composite field is $\mathbb{Q}(\zeta_n)$ and their intersection is $\mathbb{Q}$. This means that the Galois group of $\mathbb{Q}(\zeta_n)$ is the direct product of the Galois groups of each of the aforementioned subfields, i.e. $$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{\alpha_1}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{\alpha_k}})/\mathbb{Q})$$
Let $x_1, \ldots, x_n$ be the roots of a polynomial. Then the discriminant of the polynomial is $D = \prod_{i<j}(x_i - x_j)^2$	The FTFGAG guarantees that $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. Let p_i be prime such that $p_i \cong 1 \mod n_i$ (there are infinitely many such primes) for $i = 1, \ldots, k$. Let $n = p_1 \cdots p_k$. Then $(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^k (\mathbb{Z}/p_i\mathbb{Z})^\times \cong \prod_{i=1}^k \mathbb{Z}/(p_i - 1)\mathbb{Z}$. Since $n_i \mid (p_1 - 1)$, there exists $H_i \leq \mathbb{Z}/(p_i - 1)\mathbb{Z}$ such that the quotient by H_i is cyclic of order n_i. By the fundamental theorem of Galois theory, there is a subfield of $\mathbb{Q}(\zeta_n)$ that is Galois over $\mathbb{Q}$ and has G as its Galois group.

Fields

What can we say about the Galois group of a polynomial if the square root of its discriminant is an element of the base field?

Algebra Prelim

Fields

Discuss the Galois group of a general irreducible cubic polynomial.

Algebra Prelim

Fields

List the transitive subgroups of S_4. What is the significance of this list of subgroups of S_4 for Galois theory?

Algebra Prelim

Fields

List the transitive subgroups of S_5. What is the significance of this list of subgroup of S_5 for Galois theory?

Algebra Prelim

Fields

What is a <u>cyclic</u> extension?

Algebra Prelim

Fields

Let F be a field of characteristic not dividing n. Let F contain the n^{th} roots of unity. Prove that $F(\sqrt[n]{a})$ for $a \in F$ is Galois over F.

Algebra Prelim

Fields

What does it mean if an element α that is algebraic over F can be <u>expressed by radicals</u>?

Algebra Prelim

Fields

What does it mean for a polynomial $f(x) \in F[x]$ to be <u>solvable by radicals</u>?

Algebra Prelim

Fields

Complete the sentence: A polynomial $f(x)$ can be solved by radicals if and only if ____________ .

Algebra Prelim

Fields

True or False: No quintic polynomial is solvable by radicals. Give a proof or counterexample.

Algebra Prelim

The Galois group must be a subgroup of S_3 and have order at least 3 since adjoining a single root will already result in an extension of degree 3. If the discriminant is a square of an element of the base field, then the Galois group in A_3, i.e. it's precisely A_3. If the discriminant is not a square, then the Galois group must properly contain A_3, i.e. it's precisely S_3.

The Galois group contains automorphisms that fix the base field, so if $\sqrt{D} = \prod_{i<j}(x_i - x_j)$ is contained in the base field, the any automorphism in the Galois gorup fixes $\sqrt{D}$. This means that the number of transpositions of the roots is even, since an odd number of transpositions would change the sign of $\sqrt{D}$. We conclude that the Galois group is a subgroup of A_n where n is the degree of the polynomial in question.

The transitive subgroups of S_5 are S_5, A_5, D_{10}, F_{20}, and $\mathbb{Z}/5\mathbb{Z}$.
These are the only possible Galois groups for an irreducible degree 5 polynomial.

The transitive subgroups of S_4 are S_4, A_4, D_8, V_4, and $\mathbb{Z}/4\mathbb{Z}$.

These are the only possible Galois groups for an irreducible degree 4 polynomial.

The minimal polynomial for $\sqrt[n]{a}$ is $x^n - a$. This polynomial is separable. Since adjoining $\sqrt[n]{a}$ generates the splitting field, the extension is Galois.

An extension K/F is *cyclic* if it is Galois with a cyclic Galois group.

A polynomial is *solvable by radicals* if all its roots can be expressed by radicals.

An element α can be *expressed by radicals* if α is an element of a field K that can be formed by a succession of simple radical extensions

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$.

False.

This is true if and only if the Galois group of the polynomial is S_5 or A_5, which are both not solvable groups. For example, $f(x) = x^5 - 6x + 3 \in /Q[x]$ has Galois group S_5 and so it is not solvable by radicals. But $g(x) = x^5 - 1$ contains the 5^{th} roots of unity, so this polynomial is solvable by radicals.

its Galois group is a solvable group

FIELDS

Let p be a prime not dividing the discriminant D of $f(x) \in \mathbb{Z}[x]$. What relationship does the Galois group of over $\mathbb{Q}$ of $f(x)$ have to the Galois group over $\mathbb{F}_p$ of $\overline{f(x)}$?

ALGEBRA PRELIM

FIELDS

Complete the sentence: An algebraic extension over a field of characteristic 0 is ____________ .

ALGEBRA PRELIM

FIELDS

What is the Frobenius map? What is its relation to the Galois group of a finite extension over a finite field?

ALGEBRA PRELIM

MISCELLANEOUS

State Zorn's lemma.

ALGEBRA PRELIM

MISCELLANEOUS

What is an equivalence relation?

ALGEBRA PRELIM

separable

The Galois group of $\overline{f(x)}$ is isomorphic to a subgroup of the Galois group of $f(x)$.

Suppose a partially ordered set P has the property that every chain (i.e. totally ordered subset) has an upper bound in P. Then the set P contains at least one maximal element.

In a field of characteristic p, the Frobenius map is the map $\sigma : a \to a^p$ for any element a in the field.

A finite extension of a finite field is cyclic, and the Galois group is generated by the Frobenius map.

An equivalence relation is a binary relation on a set that is reflexive, symmetric, and transitive.