QUAL SYLLABI FOR MATH 201ABC

February 2010

The topics marked with an asterisk are considered undergraduate material and will be only briefly reviewed in the graduate sequence Math 201A-B-C.

Groups
1.* Basic properties of groups and homomorphisms
2.* Cosets and Lagrange's Theorem
3.* Normal subgroups, quotient groups, fundamental homomorphism theorems
4.* Symmetric groups, Cayley's theorem
5.* Alternating and dihedral groups
6. Groups acting on sets
7. Sylow's theorems
8. Universal properties of products and coproducts
9. Free groups, presentations of groups

Rings
1.* Ideals, quotient rings, homomorphism theorems
2. Fields, characteristic of a field, field of fractions of an integral domain
3. Prime and maximal ideals
4. Elementary properties of localization
5. Polynomial rings, ring of polynomials in one variable over a field is a principal ideal domain
6. Factorization in commutative rings
7. Principal ideal domains are unique factorization domains
8. Euclidean domains are principal ideal domains
9. Unique factorization in polynomial rings
10. Eisenstein's irreducibility criterion

Modules and linear algebra
1.* Basic properties of bases and dimension of vector spaces
2.* The relationship between matrices and linear transformations
3.* Inner products and orthogonal bases, Gram-Schmidt process
4.* Determinants, eigenvalues, Cayley-Hamilton Theorem
5. Submodules, quotient modules, homomorphism theorems
6. Direct sum, free modules
7. Exact sequences, Short Five Lemma
8. Projective modules and injective modules, any module is a quotient of a projective module and a submodule of an injective module
9. Hom, dual of a vector space, dual bases and maps
10. Tensor product, tensor, symmetric and exterior algebras
11. Structure of finitely generated modules over principal ideal domains, applications to abelian groups
12. Rational canonical forms and Jordan canonical forms

Fields

1.* Elementary properties of field extensions, degree of a finite extension
2. Existence and uniqueness of splitting fields
3. Existence and uniqueness of algebraic closure
5. Separable, normal and Galois extensions
6. Fundamental theorem of Galois theory
7. Galois groups of quadratic and cubic extensions
8. Finite fields and their Galois theory
9. Transcendence basis and transcendence degree

References:

T.W. Hungerford, Algebra
N. Jacobson, Basic Algebra I
S. Lang, Algebra
D. Dummit, R. Foote, Abstract Algebra
M. Atiyah, I. Macdonald, Commutative Algebra

Kayla Murray
11/19/12 @ 2

Midterm 201 A, Fall 2012

Each question is worth 10 points. A perfect score is 45 points. You may attempt as many questions as you wish.

1. Consider the symmetric group $G = S_{2n}$ on $2n$ letters. Let G_1 be the subgroup of G consisting of permutations which fix $n+1, \cdots, 2n$, i.e, $\sigma \in G_1$ if and only if $\sigma(i) = i$ for all $n+1 \leq i \leq 2n$. Let G_2 be the subgroup consisting of permutations which fix $1, \cdots, n$. Let H be the subgroup of G generated by G_1 and G_2. Prove that H is isomorphic to the internal direct product of G_1 and G_2.

2. Suppose that G is a finite abelian group of order 36 and assume that G is not isomorphic to Z_{36}. Prove that G contains a non-cyclic subgroup of order 4 or of order 9.

3. Prove that a group of order 56 must contain a normal subgroup.

4. Let Z be the additive group of integers. Prove that $6\mathrm{Z}/30\mathrm{Z} \cong \mathrm{Z}_5$.

5. Let $f : G \to H$ be a group homomorphism. Assume that H is abelian. Prove that any subgroup of G which contains the kernel of f must be normal.

6. Prove that the center of the dihedral group of D_6 is isomorphic to Z_2. Recall that D_6 is the subgroup of S_6 generated by the six cycle $a = (1, 2, 3, 4, 5, 6)$ and the permutation $b = (2, 6)(3, 5)$.

M 201A - 2012

1) Consider the symmetric group $G = S_{2n}$ on $2n$ letters. Let G_1 be the subgroup of G consisting of permutations which fix $n+1, \dots, 2n$. Let G_2 be the subgroup consisting of permutations which fix $1, \dots, n$. Let $H \leq G$ generated by G_1 and G_2. Prove H is isomorphic to the internal direct product of G_1 & G_2.

Pf:
By construction $G_1 \cap G_2 = \{e\}$. Now we need to show G_1 and G_2 are normal in H.

Let $\sigma \in H = \langle G_1 \cup G_2 \rangle$.

since G_1 and G_2 are disjoint $\sigma = \sigma_1 \sigma_2$ for $\sigma_1 \in G_1$ and $\sigma_2 \in G_2$. (b/c we have $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$)

Now, $(\sigma_1 \sigma_2)\, \tau\, (\sigma_1 \sigma_2)^{-1} = \sigma_1 (\sigma_2\, \tau\, \sigma_2^{-1}) \sigma_1^{-1}$

($\tau \in G_1$)

$= \sigma_1 (\sigma_2 \sigma_2^{-1} \tau) \sigma_1^{-1}$ (since the cycles σ_2^{-1} and τ are disjoint.)

$= \sigma_1 \tau \sigma_1^{-1} \in G_1$

Therefore $G_1 \trianglelefteq H$. By a symmetric argument $G_2 \trianglelefteq H$. Thus $G_1, G_2 \trianglelefteq H$ and $H = G_1 G_2$ (assumption). So by Cor & 8.7, $H = G_1 \times G_2$. //

M 201A - 2012

2) Suppose that G is a finite abelian group of order 36 and assume that G is not isomorphic to $\mathbb{Z}_{36}$. Prove that G contains a non-cyclic subgroup of order 4 or of order 9.

Well, $36 = 2^2 \cdot 3^2$

So possible groups G could be isomorphic to are $\mathbb{Z}_{36}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

We are assuming $G \not\cong \mathbb{Z}_{36}$

So we are only considering: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

If $G \cong$ to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2}$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ then consider the subgroups $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \{e\}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \{e\} \oplus \{e\}$ of the former groups resp. Both of these subgroups are non-cyclic subgroups of order 4, since they contain $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

If $G \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Then consider the subgroup $\{e\} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. This subgroup is non-cyclic and of order 9, since it contains $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Thus G always contains a non-cyclic subgrp of order 4 or order 9. //

M 201 A-2012

3) Prove that a group of order 56 must contain a normal subgroup.

Well, $56 = 2^3 \cdot 7$

so ∃ sylow-2 subgroups of order 8 and sylow-7 subgroups of order 7

the number K of sylow p-subgroups must divide the order of the group and $K \equiv 1 \bmod p$.

divisors of 56: 1, 2, 4, 7, 8, 14, 28, 56.

if $p=2$: $(K \equiv 1 \bmod 2)$

$K = 1, 7$ $\quad |\text{sylow-2 subgroup}| = 8$

if $p=7$: $(K \equiv 1 \bmod 7)$

$K = 1, 8$ $\quad |\text{sylow-7 subgroup}| = 7$.

(bottom) since there is only one, it is normal. //

if ∃ a sylow 7-subgroup then it would be normal then it is normal and we are done.

assume ∃ 8 sylow 7-subgroups, say $H_1, \ldots, H_8$.

For each H_i, $1 \le i \le 8$, $|H_i| = 7$.

thus each H_i is isomorphic to $\mathbb{Z}_7$

Therefore, $H_i \cap H_j = \{e\}$ for $i \neq j$

Since $H_i \neq H_j$ and $H_i, H_j \cong \mathbb{Z}_7$.

thus we have $8(7-1) = 8 \cdot 6 = 48$ non-identity elmt of order 7. Thus, $56 - 48 = 8$ elmts of order a power of 2. Since the order of a sylow 2-subgrp is 8, there is only one sylow 2-subgrp (top).

M 201A-2012

4) Let $\mathbb{Z}$ be the additive group of integers. Prove that $6\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}_5$.

Pf:

Let $\mathbb{Z}$ be the additive group of integers.

Consider $\mathbb{Z}_5$. $\mathbb{Z}_5$ is finite, cyclic and abelian and $|\mathbb{Z}_5| = 5$.

Any finite abelian grp of order 5 is isomorphic to $\mathbb{Z}_5$.

NTS $6\mathbb{Z}/30\mathbb{Z}$ is a finite abelian group of order 5.

Elements in $6\mathbb{Z}/30\mathbb{Z}$ look like $a+30\mathbb{Z}$ with $a \in 6\mathbb{Z}$.

So $6\mathbb{Z}/30\mathbb{Z} = \{6+30\mathbb{Z}, 12+30\mathbb{Z}, 18+30\mathbb{Z}, 24+30\mathbb{Z}, 30\mathbb{Z}\}$

If we take any other element from $6\mathbb{Z}$ as a coset rep it will already be contained in one of these.

Also $6\mathbb{Z}/30\mathbb{Z}$ is abelian b/c addition of the integers is abelian.

Thus $6\mathbb{Z}/30\mathbb{Z}$ is a finite abelian grp of order 5, thus $6\mathbb{Z}/30\mathbb{Z}$ is isomorphic to $\mathbb{Z}_5$. //

M 201A – 2012

5) Let $f: G \to H$ be a group homom. Assume that H is abelian. Prove that any subgroup of G which contains the kernel of f must be normal.

Pf:

Let $f: G \to H$ be a grp homom. Let H be abelian. Let $N \leq G$ s.t. $\ker f \subset N$. We will show $N \trianglelefteq G$.

Let $a, n \in G$ with $n \in N$.

Consider, $f(ana^{-1}n^{-1}) = f(a)f(n)f(a^{-1})f(n^{-1})$

b/c f homom $\longrightarrow$ $= f(a)f(n)f(a)^{-1}f(n)^{-1}$

since H is abelian $\longrightarrow$ $= f(a)f(a)^{-1}f(n)f(n)^{-1}$

$= e \cdot e$

$= e$.

Thus, $ana^{-1}n^{-1} \in \ker f$

Thus $ana^{-1}n^{-1} \in N$

so $ana^{-1}n^{-1} = n'$ w/ $n' \in N$

$ana^{-1} = n'n$

but since $n', n \in N$ then $n'n \in N$ since $N \leq G$.

Thus $ana^{-1} \in N$

so $ana^{-1} \subset N$.

Thus $N \trianglelefteq G$. //

M 201A-2012

(6) Prove that the center of the dihedral group of D_6 is isomorphic to $\mathbb{Z}_2$.

Recall that D_6 is the subgroup of S_6 generated by the six cycle $a=(123456)$ and the permutation $b=(26)(35)$.

Pf:

Recall that D_6 is generated by a and b with the relationship $ba=a^{-1}b$. Since $ba=a^{-1}b$, every elmt of D_6 can be written as a^ib^j where $0\le i\le 5$ and $0\le j\le 1$. Suppose a^i is in the center of D_6 for some $0\le i\le 5$.

Then, $a^ib=ba^i=a^{-i}b$

since a^i is in the center of D_6 and $ba^i=a^{-i}b$. Thus $a^i=a^{-i}$

However this only holds for $a^0=e$ & a^3.

Now suppose a^ib is in the center of D_6.

Then, $a^{i-1}b=a^ia^{-1}b=(a^ib)a$ since $a^{-1}b=ba$

$=a(a^ib)$ since a^ib is in center of D_6

$=a^{i+1}b$.

So $a^{i-1}=a^{i+1}$ But this is not true for $0\le i\le 5$.

Thus the center of D_6 is $Z(D_6)=\{e, a^3\}$. Since $|Z(D_6)|=2$ so $Z(D_6)\simeq\mathbb{Z}_2$.

Midterm Math 201A, Fall 2010

Attempt as many questions as you like. A perfect score is 40. All questions are worth ten points each.

1. Let G be the group generated by elements a and b with $a^2 = b^3 = e$. Suppose that $ab = ba$.

(a) Prove that G is abelian and find its cardinality.

(b) Prove that G is a cyclic group and identify the cyclic generator of G.

(c) Find two subgroups H_1 and H_2 of G such that $G \cong H_1 \times H_2$.

2. The group D_4 is generated by $a = (1,2,3,4)$ and $b = (2,4)$. Prove that D_4 has eight elements. Consider the subgroup H_1 generated by a and prove that it is normal in D_4. Let H_2 be the subgroup generated by b. Prove that G is not isomorphic to $H_1 \times H_2$.

3. (a) Suppose that G is an abelian group with $|G| = 30$. Prove that it has a unique element of order 2.

(b) More generally prove that any group of order 30 has an element of order 2.

4. Let H and K be subgroups of G. Let P be the subgroup of G generated by H and K.

(a)Prove that P is the intersection of all subgroups M of G such that $H \cup K \subset M$.

(b) Suppose that $HK = KH$. Prove that HK is a subgroup of G. Conclude that $HK = P$.

5. What is the natural homomorphism of groups $\mathbb{Z} \to \mathbb{Z}_6$? What is the kernel of this map? Use the first homomorphism theorem to conclude that there is a homomorphism map from $\mathbb{Z}_{18} \to \mathbb{Z}_6$. Prove that the kernel of this homomorphism is isomorphic to $\mathbb{Z}_3$. Is it true that $\mathbb{Z}_{18} \cong \mathbb{Z}_6 \times \mathbb{Z}_3$?

6. Suppose that H is a normal subgroup of G. Assume that H and G/H are finitely generated. Prove that G is finitely generated. Suppose in fact that H and G/H are cyclic. What is the maximal number of generators you need to generate G?

M 201 A – 2010

1) Let G be the group generated by elements a and b with $a^2 = b^3 = e$. Suppose that $ab = ba$.

(a) Prove that G is abelian and find its cardinality

Since $ab = ba$, we can write any element of G as $a^{r_1} b^{r_2}$ w/ $r_1, r_2 \in \mathbb{Z}$

Let $x, y \in G$. Then $x = a^i b^j$ and $y = a^k b^e$ for $i, j, k, e \in \mathbb{Z}$.

Consider,
$$\begin{aligned} xy &= a^i b^j a^k b^e \\ &= a^i a^k b^j b^e \\ &= a^{i+k} b^{j+e} \\ &= a^{k+i} b^{e+j} \\ &= a^k a^i b^e b^j \\ &= a^k b^e a^i b^j = yx. \end{aligned}$$

So G is abelian.

Lastly, $|G| = 6$ since every element in G can be uniquely written as $a^{r_1} b^{r_2}$ with $0 \le r_1 \le 1$ and $0 \le r_2 \le 2$ (since $a^2 = e$ and $b^3 = e$).

So $G = \{e, a, b, b^2, ab, ab^2\}$

(b) Prove that G is a cyclic group and identify the cyclic generator of G.

claim: $\langle ab \rangle = G$.

Well, $(ab)^2 = abab = a^2b^2 = b^2$

$(ab)^3 = (ab)(ab)^2 = abb^2 = ab^3 = a$

$(ab)^4 = (ab)(ab)^3 = aba = a^2b = b$

$(ab)^5 = (ab)(ab)^4 = abb = ab^2$

$(ab)^6 = (ab)(ab)^5 = abab^2 = a^2b^3 = e$.

so $\langle ab \rangle = \{ ab, b^2, a, b, ab^2, e \}$

$= G$.

thus G is cyclic and $ab \in G$ generates G //

(c) Find two subgroups H_1 and H_2 of G s.t. $G \cong H_1 \times H_2$.

Consider,

$H_1 = \langle a \rangle = \{ a, e \}$ $\quad |H_1| = 2 \Rightarrow H_1 \cong \mathbb{Z}_2$

$H_2 = \langle b \rangle = \{ b, b^2, e \}$ $\quad |H_2| = 3 \Rightarrow H_2 \cong \mathbb{Z}_3$

so $H_1 \times H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

also, $|G| = 6$ and @ G is finite, cyclic & abelian.

then $G \cong \mathbb{Z}_6$.

Since $\gcd(2,3) = 1$, then $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

thus $G \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong H_1 \times H_2$. //

M 201 A – 2010

(2) The group D_4 is generated by $a=(1234)$ and $b=(24)$. Prove that D_4 has eight elmts.

D_4 is generated by a and b which satisfy $ba=a^{-1}b$.
So every element in D_4 can be uniquely written as $a^i b^j$ w/ $0 \le i \le 3$ and $0 \le j \le 1$.
Since $|a|=4$ and $|b|=2$.
So $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$

So $|D_4| = 8$. //

Consider the subgroup H_1 generated by a and prove that H_1 is normal in D_4.

Let $H_1 = \langle a \rangle = \{a, a^2, a^3, e\}$
since any element in G is of the form
$a^i b^j$ w/ $0 \le i \le 3$ and $0 \le j \le 1$.
To show $H_1 \trianglelefteq G$ we must show $a^i b^j H_1 (a^i b^j)^{-1} \subseteq H_1$.
If $j=0$ then $a^i \in H$ so by closure of H_1 we know this holds.
Thus we will now only consider the case when $j=1$.

So $a^i b H_1 (a^i b)^{-1} = a^i b H_1 b^{-1} a^{-i}$

$= a^i b H_1 b (a^i)^{-1}$ b/c $|b|=2$ so $b=b^{-1}$

$= a^i b a^j b (a^i)^{-1}$ for $j = 0, 1, 2, 3$

$= a^i b a a^{j-1} b (a^i)^{-1}$

$= a^i a^{-1} b a^{j-1} b (a^i)^{-1}$ ↓ relation $ba = a^{-1}b$

$= a^{i-1} b a^{j-1} b (a^i)^{-1}$ ↓ continue using relation.

$= a^{i-j} b b (a^i)^{-1}$

$= a^{i-j} (a^i)^{-1}$ b/c $|b|=2$

$= a^k$ for some $k = 0, 1, 2, 3$

Thus $a^k \in H_1$, so $a^i b H_1 (a^i b)^{-1} \in H_1$.

Thus $H_1 \trianglelefteq D_4$

Let H_2 be a subgroup generated by b. Prove that $G \not\cong H_1 \times H_2$.

So $H_1 = \langle a \rangle = \{a, a^2, a^3, e\}$

$H_2 = \langle b \rangle = \{b, e\}$

So $H_1 \cong \mathbb{Z}_4$ b/c cyclic and abelian

$H_2 \cong \mathbb{Z}_2$

So $H_1 \times H_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ which is abelian

so $H_1 \times H_2$ is abelian.

but G is not abelian b/c $ab \neq ba$ since $ba = a^{-1}b$.

Thus $G \not\cong H_1 \times H_2$.

M 201A - 2010

(3)(a) Suppose that G is an abelian group with $|G| = 30$. Prove that it has a unique elmt of order 2.

Pf:

Let G be an abelian group and $|G| = 30$.
assume G has an elmt of order 2 (proved in (b))
We will show this elmt is unique.
ATC $\exists$ two distinct elmts of order 2, call them $a, b \in G$.
Consider $H = \{e, a, b, a+b\}$. We know H contains three distinct elmts $e, a, \& b$. (by assumption).
also note, $a+b = b+a$ (b/c G abelian).
consider,
(1) $a+b = e$ then $a = b^{-1}$ $\rightarrow\leftarrow$ b/c a, b distinct.
(2) $a+b = a$ then $b = e$ $\rightarrow\leftarrow$
(3) $a+b = b$ then $a = e$ $\rightarrow\leftarrow$.
So $a+b$ is distinct elmt.
Note, $(a+b) + (a+b) = 2a+2b = e$.
So H is a subgroup of ~~order~~ G of order 4.
By by Lagranges Thm $|H| \mid |G|$ & $4 \nmid 30$.
$\rightarrow\leftarrow$ thus we cannot have two elmts of order 2.

Therefore, $\exists$ a unique elmt of order 2. //

(b) more generally prove that any group of order 30 has an elmt of order 2.

If a group has order 30.
Consider the prime decomposition:

$$30 = 2 \cdot 3 \cdot 5$$

So $\exists$ a sylow 2-subgroup of order 2 and it contains an elmt of order 2.

//

M 201A - 2010

(4) Let H and K be subgroups of G. Let $P \leq G$ generated by H and K.

(a) Prove that P is the intersection of all subgroups M of G s.t. $H \cup K \subset M$.

Pf:

Let $H, K \leq G$. Let $P \leq G$ generated by H and K.

So $P = \langle H \cup K \rangle \leq G$.

NTS $P = \bigcap_{i \in I} M_i$ where $M_i \leq G$ s.t. $H \cup K \subset M_i$.

Let $a \in \bigcap_{i \in I} M_i$. So $a \in M_i \ \forall \ i \in I$

So a is in every subgroup that contains $H \cup K$. P contains $H \cup K$ and $P \leq G$ thus $a \in P$. So $\bigcap_{i \in I} M_i \subseteq P$.

Let $a \in P = \langle H \cup K \rangle$.

Since $H \cup K \subset M_i \ \forall \ i \in I$ and $a \in \langle H \cup K \rangle$

then $a \in M_i \ \forall \ i \in I$.

Thus $a \in \bigcap_{i \in I} M_i$. So $P \leq \bigcap_{i \in I} M_i$.

Thus, $P = \bigcap_{i \in I} M_i$. //

(b) suppose that $HK = KH$. Prove HK is a subgroup of G. conclude that $HK = P$.

Pf:

Let $H, K \leq G$. Let $HK = KH$ NTS $HK \leq G$.

(1) nonempty.

$e \in H$ and $e \in K$ b/c $H, K \leq G$. so $e \in HK$

so HK is nonempty.

(2) closure

Let $a, b \in HK$. so $a = hk$ and $b = h'k'$

for $h, h' \in H$ and $k, k' \in K$.

Consider, $ab = hkh'k' = h(kh')k'$

Since $kh' \in KH$ and $KH = HK$ then $kh' = h''k''$ $h'' \in H, k'' \in K$

so $ab = hkh'k' = hh''k''k' \in HK$

since $h, h'' \in H$ ∴ $H \leq G$ and $k'', k' \in K$ ∴ $K \leq G$.

so $ab \in HK$.

(3) inverses

Let $a \in HK$ so $a = hk$ for $h \in H$, $k \in K$.

Consider $a^{-1} = (hk)^{-1} = k^{-1}h^{-1}$

since $k^{-1}h^{-1} \in KH$ and $KH = HK$ then $k^{-1}h^{-1} \in HK$

so $a^{-1} \in HK$.

Thus $HK \leq G$.

conclude that $HK = P$.

Well, $HK \subseteq \langle HUK \rangle = P$

Since $HK = KH$, we could apply a similar argument as above to elmts of $\langle HUK \rangle$, so $\langle HUK \rangle \subseteq HK$.

Thus $HK = P$. //

M 201A - 2010

5)

What is the natural homom of groups $\mathbb{Z} \to \mathbb{Z}_6$?

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_6$$
$$g \longmapsto g \pmod 6$$

What is the kernel of this map?

$$\ker f = \{ g \mid f(g) = 0 \pmod 6 \}$$
$$= 6\mathbb{Z}.$$

Use the 1st homom thm to conclude that there is a homom map from $\mathbb{Z}_{18}$ to $\mathbb{Z}_6$.

since $18\mathbb{Z} \subset 6\mathbb{Z}$ and $\ker f = 6\mathbb{Z}$

then $\exists\ \tilde{f} : \mathbb{Z}/18\mathbb{Z} \longrightarrow \mathbb{Z}_6$

or $\tilde{f} : \mathbb{Z}_{18} \longrightarrow \mathbb{Z}_6$

$n + 18\mathbb{Z} \longmapsto n \bmod 6$

$n \in \mathbb{Z}$

Using:
If $f: G \to H$ homom
$\{N \trianglelefteq G \ \{N \subset \ker f$
$\Rightarrow \tilde{f} : G/N \to H$

Is it true that $\mathbb{Z}_{18} \cong \mathbb{Z}_6 \times \mathbb{Z}_3$?

NO, $\mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$ and $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

but $\mathbb{Z}_2 \times \mathbb{Z}_9 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

//

M 201A - 2010

(6) Suppose $H \trianglelefteq G$. assume H and G/H are finitely generated. Prove that G is finitely generated.

Pf:

Let $H \trianglelefteq G$ Let H and G/H be finitely generated.

So $H = \langle a_1, \ldots, a_n \rangle$ and $G/H = \langle b_1 H, \ldots, b_m H \rangle$.

Consider $g \in G$. Then $g \in cH$ (some coset).

and $cH \in \langle b_1 H, \ldots, b_m H \rangle$ so cH can be written in terms of $b_1 H, \ldots, b_m H$.

$\Rightarrow cH = (b_{i_1}, \ldots b_{i_k} H)$ with

$0 \le i_1 \le m, \ldots, 0 \le i_k \le m$

where $b_{i_1}, \ldots, b_{i_k}$ are not necessarily distinct.

so $g \in b_{i_1} \ldots b_{i_k} H \Rightarrow g = b_{i_1} \ldots b_{i_k} h_0$ for $h_0 \in H$

But $h_0 \in \langle a_1, \ldots, a_n \rangle = H \Rightarrow h_0 = a_{j_1} \ldots a_{j_\ell}$ with

$0 \le j_1 \le n, \ldots, 0 \le j_\ell \le n$

$\Rightarrow g = b_{i_1} \ldots b_{i_k} a_{j_1} \ldots a_{j_\ell}$

$\Rightarrow g \in \langle b_1, \ldots, b_m, a_1, \ldots, a_n \rangle$.

Thus G is finitely generated. //

Suppose in fact that H and G/H are cyclic. what is the maximal # of generators you need to generate G?

if H, G/H cyclic $\Rightarrow \langle a \rangle = H$ and $\langle bH \rangle = G/H$.

thus G is generated by at most two generators $G = \langle a, b \rangle$.

Final 201 A, Fall 2012

The maximal possible score is 50 points. Attempt as many questions as you wish.

1.(5points) Define the notion of a prime element p in an integral domain D. Prove that p is prime iff the principal ideal generated by p is prime.

2.(20 points) Let $\mathbb{R}$ be the field of real numbers and consider the polynomial ring $\mathbb{R}[x]$ in one variable. You may use the fact that $\mathbb{R}[x]$ is a Euclidean domain.

(a) Prove that any prime ideal in $\mathbb{R}[x]$ is maximal.

(b) Determine if the ideal generated by $f(x) = x^2+x+1$ is prime. Repeat with the polynomial $g(x) = x^2 + 5x + 6$.

(c) Prove that the ideal in $\mathbb{R}[x]$ generated by elements $x^2 - 4$ and $x^4 - 12$ is not proper.

(d) Consider the ideal J in $\mathbb{R}[x]$ generated by $x^2 - x + 1$ and $x^3 + 1$. Find a polynomial $h(x)$ which generates J.

3.(15 points) Suppose that D is an integral domain of characteristic 5.

(a) Prove that for all $a, b \in D$ we have $(a + b)^5 = a^5 + b^5$.

(b) Prove that $D[x]$ is an integral domain of characteristic 5.

(c) Use parts (a) and (b) to prove that if $f \in D[x]$, then the only powers of x which appear with non–zero coefficients in f^5 are powers of x^5. You may assume that f has degree 3 if you like, to make writing the solution easier.

4. (5 points) Let $\mathbb{R}$ be the field of real numbers and $\mathbb{C}$ the field of complex numbers. Consider the ring homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{C}$ given by $\varphi(f(x)) = f(i\sqrt{2})$, i.e., we set $x = i\sqrt{2}$. Find the element h such that $\ker \varphi$ is the ideal generated by h. Prove that φ induces an isomorphism $\mathbb{R}[x]/\ker \varphi \cong \mathbb{C}$.

5. (a) (5 points) Let $\mathbb{R}$ be the field of real numbers. Consider the ring $R = \mathbb{R}[x]$ and let $S = \{x^p : p \in \mathbb{Z}_+\}$ where $\mathbb{Z}_+$ is the set of non–negative integers. Prove that S is a multiplicative subset of $\mathbb{R}[x]$. Prove that $S^{-1}R$ is principal ideal domain. (Hint: Use the fact that any ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I in R.)

(b) (10 points) Let R and S be as in part (a). What are all the units in R and $S^{-1}R$. (Hint: to determine the units in $S^{-1}R$, first prove that no polynomial with constant term can be invertible.)

6. (5 points) Prove that a finite integral domain is a field.

Make up questions for groups. This is meant for students who got below 35 on the midterm. If for instance you got 30 on the midterm, the most you can get from doing these questions is 5 points. If you got 25 then you would get 10. And so on. If you got 35 or more you get no additional points from doing these questions and they will not be graded.

7 1. (5 points) Suppose that $G/C(G)$ is cyclic, where G is a group and $C(G)$ is the center of G. Prove that G is abelian. — 2010 F (6a)

8 2. (5 points) Suppose that H is a normal subgroup of order p^k in a finite group. Prove that any Sylow–p subgroup of G contains H. (Use the first and second Sylow theorems).

9 3.(5 points) Prove that S_3 is not the direct product of any family of its proper subgroups.

10 4. (5 points) Suppose that G is an abelian group of order 12. Assume that G contains an element a of order 4 and an element b of order 3. Prove that G is isomorphic to $\mathbf{Z}_{12}$.

11 5. (5 points) Find the elementary divisors and invariant factors of $\mathbf{Z}_2 \ominus \mathbf{Z}_9 \oplus \mathbf{Z}_{35}$.

F 201A - 2012

1) Define the notion of a prime element p in an integral domain D.

a nonzero element a of an ID D is called a prime elmt if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Prove that p is prime iff the principal ideal generated by p is prime.

Pf:

($\Rightarrow$) Let $p \in D$ be prime.

Let $P = (p)$. NTS: P is a prime ideal

Let $ab \in P = (p)$

$\Rightarrow ab = px$ for some $x \in D$

$\Rightarrow p \mid ab$

Since p is prime elmt then $p \mid a$ or $p \mid b$

WLOG, let $p \mid a$

$\Rightarrow a = py$ for some $y \in D$

$\Rightarrow a \in P = (p)$

Thus $P = (p)$ is a prime ideal.

($\Leftarrow$)

Let (p) be a prime ideal for some $p \in D$.

p is not a unit since if p was a unit, $(p) = D \rightarrow\leftarrow$

Suppose $p \mid bc$ where $b, c \in D$

$\Rightarrow bc = px$ for some $x \in D$

$\Rightarrow bc \in (p)$

Since (p) prime

$\Rightarrow b \in (p)$ or $c \in (p)$

WLOG let $b \in (p)$.

$\Rightarrow b = py$ for some $y \in D$

$\Rightarrow p \mid b$

$\rightarrow p$ is prime elmt. //

F 201A-2012

2) Let $\mathbb{R}$ be the field of real # and consider the polynomial ring $\mathbb{R}[x]$ in one variable. You may use the fact that $\mathbb{R}[x]$ is a E.D.

a) Prove that any prime ideal in $\mathbb{R}[x]$ is maximal.

Pf:

Note Thm refers to Thm 3.4

Let P be a prime ideal in $\mathbb{R}[x]$. Since $\mathbb{R}$ is a field, $\mathbb{R}[x]$ is a PID (and ID).

So $P=(p)$ for some $p \in \mathbb{R}[x]$.

Since (p) is prime, then p is prime (Thm).

But in ID, p prime $\Rightarrow$ p is irreducible (Thm)

also in ID, p irred $\Rightarrow$ (p) is maximal in the set of all proper principal ideals of $\mathbb{R}[x]$ (Thm).

Since $\mathbb{R}[x]$ is a PID, all ideals are principal.

Thus $(p)=P$ is maximal. //

b) Determine if the ideal generated by $f(x)=x^2+x+1$ is prime.

note: irreducible iff prime (elmts) (in a PID)

note: elmt prime iff ideal generated prime (in a ID)

$f(x)=x^2+x+1$

$$\text{roots} = \frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm i\sqrt{3}}{2}$$

$\Rightarrow$ roots of $f(x)$ are in $\mathbb{C}$

$\Rightarrow$ $f(x)$ is irreducible

$\Rightarrow$ $(f(x))$ is prime since $\mathbb{R}[x]$ is a PID.

Repeat for $g(x) = x^2+5x+6$.

$g(x) = x^2+5x+6 = (x+2)(x+3)$

$\Rightarrow g(x)$ is reducible

$\Rightarrow (g(x))$ is not prime.

c) Prove that the ideals in $\mathbb{R}[x]$ generated by elements x^2-4 and x^4-12 is not proper. ↑ together.

Pf:

Let I be the ideal generated by x^2-4 and x^4-12

Then $-1(x^4-12) \in I$ and $(x^2+4)(x^2-4) \in I$.

since $-1 \in \mathbb{R}[x]$ and $x^2+4 \in \mathbb{R}[x]$

so $(x^2+4)(x^2-4) - (x^4-12) \in I$

$x^4 - 16 - x^4 + 12 = -4$

thus $-4 \in I$.

But -4 is a unit in $\mathbb{R}[x]$.

so $I = \mathbb{R}[x]$, thus I is not proper. //

d) Consider the ideal J in $\mathbb{R}[x]$ generated by x^2-x+1 and x^3+1. Find a polynomial $h(x)$ which generates J.

Note: $x^3+1 = (x+1)(x^2-x+1)$

$\Rightarrow (x^3+1) \subseteq (x^2-x+1)$ (ideals) and x^2-x+1 is irred. in $\mathbb{R}[x]$ $\Rightarrow x^2-x+1$ is prime $\Rightarrow (x^2-x+1)$ is prime

thus $h(x) = x^2-x+1$ generates J. //

562-965-9765

F 201A - 2012

3) Suppose that D is an I.D. of characteristic 5.

a) Prove that $\forall\, a, b \in D$ we have $(a+b)^5 = a^5 + b^5$

Pf:

Let D be an I.D. of characteristic 5.

By the binomial thm for $a, b \in D$

$$(a+b)^5 = \sum_{k=0}^{5} \binom{5}{k} a^k b^{5-k}$$

but $5 \mid \binom{5}{k}$ when $k \neq 0, 5$

so since char $D = 5$

then $(a+b)^5 = a^5 + b^5$ //

b) Prove that D[x] is a I.D. of characteristic 5.

Pf:

unity: since $1 \in D \subseteq D[x]$ and $1 \cdot f(x) = f(x)$ $\forall\, f(x) \in D[x]$

$\Rightarrow$ D[x] has unity.

commutative: D[x] is commutative since the coeff of any poly in D[x] are in D, which is commutative.

no zero divisors:

Let $f(x) = a_n x^n + \ldots + a_0$ and $g(x) = b_m x^m + \ldots + b_0$ w/ $a_n, b_m \neq 0$.

then $f(x)g(x)$ has leading coeff of $a_n b_m$

and since D is an integral domain

then $a_n b_m \neq 0$.

Clearly D[x] is a ring.

characteristic: We know that char $D[x] = 0$ or prime (b/c I.D.)

Let $f(x) = a_n x^n + \ldots + a_0$, so $5 \cdot f(x) = 5a_n x^n + \ldots + 5a_0 = 0$ since $5 \cdot a_i = 0$ $\forall a_i \in D$

b/c char D = 5. Thus char D[x] = 5

q.e.d. //

c) Use parts (a) and (b) to prove that if $f \in D[x]$, then the only powers of x which appear with non-zero coeff in f^5 are powers of x^5. You may assume that f has degree 3 if you like to make writing the solution easier.

Pf:

Let $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in D[x]$.

From part (b) we know $\text{char } D[x] = 5$ and $D[x]$ is an I.D.

Well, $[(a_3x^3 + a_2x^2) + (a_1x + a_0)]^5$

$= (a_3x^3 + a_2x^2)^5 + (a_1x + a_0)^5$ by (a)

$= (a_3x^3)^5 + (a_2x^2)^5 + (a_1x)^5 + a_0^5$ by (a)

thus all the non-zero coeff in f^5 are a power of x^5 //

F 201A-2012

4) Let $\mathbb{R}$ be the field of real # and $\mathbb{C}$ be the field of complex #. Consider the ring homom, $\phi : \mathbb{R}[x] \to \mathbb{C}$ given by $\phi(f(x)) = f(i\sqrt{2})$.

i.e. we set $x = i\sqrt{2}$. Find the element h s.t. $\ker\phi$ is the ideal generated by h.

Pf:

claim: $\ker\phi = (x^2+2)$.

"$\supseteq$" Let $f(x) \in (x^2+2)$

Then $f(x) = g(x)[x^2+2]$ for $g(x) \in \mathbb{R}[x]$.

well $f(i\sqrt{2}) = g(i\sqrt{2})[(i\sqrt{2})^2+2] = 0$

So $f(x) \in \ker\phi$

"$\subseteq$"

Let $f(x) \in \ker\phi$

$\Rightarrow f(i\sqrt{2}) = 0$.

since $f(x)$ and $x^2+2 \in \mathbb{R}[x]$,

then by the division algorithm

$f(x) = q_f(x)(x^2+2) + r(x)$ w/ $\deg r(x) \leq 1$

$\Rightarrow r(x) = ax+b$ w/ $a, b \in \mathbb{R}$

So $0 = f(i\sqrt{2}) = q_f(i\sqrt{2})((i\sqrt{2})^2+2) + r(i\sqrt{2})$

$\Rightarrow 0 = 0 + r(i\sqrt{2})$

$\Rightarrow r(i\sqrt{2}) = 0$

$\Rightarrow a(i\sqrt{2}) + b = 0$

$\Rightarrow a = 0 \Rightarrow b = 0$

$\Rightarrow r(x) = 0$.

$\Rightarrow f(x) = q_f(x)(x^2+2)$

So $f(x) \in (x^2+2)$

Thus, $\ker\phi = (x^2+2)$. //

Prove that ϕ induces an isomorphism $\mathbb{R}[x]/\ker\phi \cong \mathbb{C}$.

recall, $\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$
$f(x) \longmapsto f(i\sqrt{2})$

Let $a+bi \in \mathbb{C}$

consider $f(x) = a + \frac{b}{\sqrt{2}}x$

so $f(i\sqrt{2}) = a + \frac{b}{\sqrt{2}}(i\sqrt{2}) = a+bi$

so ϕ is surjective

Thus $\phi(\mathbb{R}[x]) = \mathbb{C}$.

Therefore by 1st isomorphism thm

$\mathbb{R}[x]/\ker\phi \cong \phi(\mathbb{R}[x]) = \mathbb{C}$. //

F 201A - 2012

6)

(a) Let $\mathbb{R}$ be the field of real #. Consider the ring $R = \mathbb{R}[X]$ and let $S = \{X^p \mid p \in \mathbb{Z}_+\}$ where $\mathbb{Z}_+$ is the set of non-negative integers. Prove that S is a multiplicative subset of $\mathbb{R}[X]$. Prove that $S^{-1}R$ is a PID. (Hint: Use the fact that any ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some I in R.

Pf:

First we will show S is a multiplicative subset of $\mathbb{R}[X]$.

Well $S = \{X^p \mid p \in \mathbb{Z}_+\}$. Let $X^n, X^m \in S$

$\Rightarrow X^n \cdot X^m = X^{n+m}$ since $n, m \in \mathbb{Z}_+ \Rightarrow n+m \in \mathbb{Z}_+$

$\Rightarrow X^n \cdot X^m \in S$.

Thus S is multiplicative.

Next we will show $S^{-1}R$ is a PID.

We know R is a PID and S is a multiplicative subset of $\mathbb{R}[X]$. Also every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some I in R.

Since $\mathbb{R}[X]$ is a nonzero ring with no zero divisors and $0 \notin S$ then $S^{-1}R$ is an ID.

Next we will show it is principal.

Since I is an ideal in R and R a PID then

$I = (a)$ for some $a \in R$

$\Rightarrow S^{-1}I = \{(b, s) : b \in I, s \in S\}$

claim $S^{-1}I = ((as, s))$ for some $s \in S$.

"$\subseteq$"

let $(b, s') \in S^{-1}I$

$\Rightarrow b \in I$

$\Rightarrow b = ra$ for some $r \in R$.

$\Rightarrow_{c_{(b,s')}} ((b, s')) = ((ra, s'))$

$= ((ras, s's))$

$= ((r, s')(as, s))$

$\subseteq ((as, s))$

"$\supseteq$"

$(as, s) \in S^{-1}I$

since $as \in I$ and $s \in S$.

thus $((as, s)) \subseteq S^{-1}I$

note: $as \in I$ b/c $s \in S \subseteq R$, $a \in I$, and I ideal so $as \in I$

thus $S^{-1}I = ((as, s))$

$\Rightarrow S^{-1}R$ is a PID.

b) Let R and S be as in part (a). What are all the units in R and $S^{-1}R$. (Hint: to determine units in $S^{-1}R$, first prove that no polynomial with constant term can be invertible).

Units in R:

- constant polynomials, since $\mathbb{R}$ is a field.
- since x does not have an inverse in $\mathbb{R}[x]$, there are no other units.

units in $S^{-1}R$:

Suppose $(f(x), x^p)$ is a unit in $S^{-1}R$

then $\exists\ (g(x), x^q)$ s.t.

$$(f(x), x^p)(g(x), x^q) = (1,1)$$

$$\Rightarrow (f(x)g(x),\ x^{p+q}) = (1,1)$$

$$\Rightarrow f(x)g(x) = x^{p+q} \qquad (*)$$

Recall: any linear polynomial is irred in $\mathbb{R}[x]$, in particular x is irred.
Now $\mathbb{R}[x]$ is a PID $\Rightarrow \mathbb{R}[x]$ is a UFD.

Looking at $*$, decompose f and g into irred. in $\mathbb{R}[x]$. This product is equal to x^{p+q}. Since any decomposition into irred in a UFD is unique up to permutation (and a unit)

$\Rightarrow f = cx^k$, $0 \le k \le p+q$, c a unit in $\mathbb{R}[x]$.

Thus we have that elmts of the form (rx^k, x^p) where $k \le p+q$ are units

also, (x^k, x^p) is a unit for any k, p since you could choose q to satisfy $k \le p+q$. //

F 201A - 2012

(e) Prove that a finite integral domain is a field.

Pf:

Let D be a finite I.D. with unity 1.

Let a be any nonzero elmt of D. We must show a is a unit.

If $a=1$, a is its own inverse, so assume $a \neq 1$.

Consider the following sequence of elmts of D:

$$a, a^2, a^3, \ldots$$

Since D is finite, there must be two positive integers i and j s.t. $i > j$ and $a^i = a^j$

So $\Rightarrow$ $a^i = a^{i-j} a^j = a^j$

So by cancellation $a^{i-j} = 1$.

Since $a \neq 1$, we know $i - j > 1$

Thus a^{i-j-1} is the inverse of a.

Note: $a a^{i-j-1} = a^{i-j-1+1} = a^{i-j} = 1$. //

F 201A - 2012

8) Suppose that H is a normal subgroup of order p^k in a finite group. Prove that any sylow-p subgroup of G contains H. (use 1st/2nd sylow thms)

Pf:

Let $H \trianglelefteq G$ with $|H| = p^k$ and G finite order.

By sylow 1st thm, $\exists$ a sylow-p subgroup that contains H, let it be P'.

Let P be any sylow-p subgroup.

By sylow 2nd thm, P is conjugate to P'

so $\exists\ y \in G$ s.t. $P = y P' y^{-1}$

Note that $H = y H y^{-1}$ since $H \trianglelefteq G$

since $H \leq P' \Rightarrow H \trianglelefteq P$.

So any sylow-p subgroup of G contains H.

//

F 201 A-2012

9) Prove that S_3 is not the direct product of any family of its proper subgroups.

Pf:

A.T.C. $\exists\ H_1, H_2 \leq S_3$ s.t. $S_3 \cong H_1 \times H_2$.

Since $|S_3| = 6 \Rightarrow$ WLOG $|H_1| = 2$ and $|H_2| = 3$

$\Rightarrow H_1 \cong \mathbb{Z}_2$ and $H_2 \cong \mathbb{Z}_3$

$\Rightarrow H_1 \times H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

and $\mathbb{Z}_6$ is cyclic, but S_3 is not cyclic.

$\rightarrow\leftarrow$ //

F 201A - 2012

10) Suppose that G is an abelian group of order 12. Assume that G contains an element a of order 4 and an element b of order 3. Prove $G \cong \mathbb{Z}_{12}$.

Pf:

Since G is a finite abelian group of order 12. Then G is isomorphic to one of the following groups, $\mathbb{Z}_{12} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$. However $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ does not have an element of order 4, thus

$G \cong \mathbb{Z}_{12}$.

//

F 201 A-2012

11) Find the elementary divisors and invariant factors of $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35}$

Well, $G = \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$

elementary divisors: $2, 3^2, 5, 7$

invariant factors: $2 \times 3^2 \times 5 \times 7 = \boxed{630}$

So $G \cong \mathbb{Z}_{630}$.

b) Repeat for $\mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54} = H$

Well, $H \cong \mathbb{Z}_5 \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_{5^2} \oplus (\mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^2}) \oplus (\mathbb{Z}_{3^3} \oplus \mathbb{Z}_2)$

elementary divisors: $5, 5, 3, 5^2, 3^2, 2^2, 3^3, 2$

$\boxed{2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2}$

Invariant factors:

	3	5	15
2	3^2	5	90
2^2	3^3	5^2	2700

$\boxed{15, 90, 2700}$

So $H \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{2700}$

Final Math 201A, Fall 2010

Attempt as many questions as you like. A perfect score is 75. Each question is worth 12 points.

1. Suppose that D is a principal ideal domain and R is any ring with identity. Let $\phi : D \to R$ be a homomorphism of rings. Prove that,

(a) $\phi(D)$ is a commutative ring in which every ideal is principal.

(b) Is it true that R must be commutative?

(c) Prove or give a counterexample to: $\phi(D)$ is an integral domain. (d) Suppose that we take $D = \mathbb{Z}$ and R to be the ring of 2×2 matrices. Define $\phi : D \to R$ by

$$\phi(n) = nI,$$

where I is the 2×2 identity matrix. Prove that ϕ is a homomorphism of rings.

2. (a) Let F be a field and $F[x]$ the ring of polynomials in one variable. Let I be an ideal in $F[x]$. Prove that I is a prime ideal iff I is maximal.

(b) Find all the prime and maximal ideals in Z_{11} and Z_{12}.

3. (a) Let $\mathbb{R}$ be the field of real numbers and $\mathbb{C}$ the field of complex numbers. Let $\varphi : \mathbb{R}[x] \to \mathbb{C}$ be the homomorphism of rings which is the evaluation at i, i.e

$$\varphi(f) = f(i).$$

Prove that φ is surjective and that $ker\varphi$ is a maximal ideal. Determine the kernel of φ, i.e what is a necessary and sufficient condition for a polynomial to be in $\ker\varphi$.

(b) Repeat (a) but assuming now that $\varphi : \mathrm{C}[x] \to \mathrm{C}$ is the evaluation at i.

---

4. (a) Prove that any free abelian group of rank 2 is isomorphic to $\mathrm{Z} \times \mathrm{Z}$.

(b) Give an example of a subset of $\mathrm{Z} \times \mathrm{Z}$ which generates $\mathrm{Z} \times \mathrm{Z}$ as a group but is not a basis.

(c) Find two non–isomorphic subgroup of $\mathrm{Z} \times \mathrm{Z}$ with index 4.

5. Let G be a finite abelian group and let H be a subgroup of G.

(a) Prove that there exists a subgroup K of G which is isomorphic to G/H.

(b) Prove that G is isomorphic to the direct product $H \times G/H$.

(c) Suppose that $G = Z_6 \times Z_{15}$ and $H = \{(0,0),(3,0)\}$. Check that H is a subgroup of G and find the group K which is isomorphic to G/H.

6. (a) Prove that G is abelian if $G/C(G)$ is cyclic. Is the converse true ?

(b) Prove that a group of order p^2 is abelian.

7. Let G be the group of 2×2 invertible matrices with real entries. Let H be the subgroup consisting of diagonal matrices. Prove that $C_G(H) = H$ and that $N_G(H)$ is the group of 2×2 matrices of the form

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0, ab = 0, cd = 0 \right\}.$$

Prove that $C_G(H)$ is a normal subgroup in $N_G(H)$ and find the index $[N_G(H) : C_G(H)]$.

8. Find the Sylow–3 subgroups of S_5.

9. Prove that a group of order 12 has a normal Sylow subgroup.

10. Let N be a normal subgroup of G.

(a) Define a group action of G on N. You must check that it is a group action.

(b) Define an action of G on the set of cosets G/N. Prove that the kernel of the induced homomorphism $G \to A(G/N)$ is N.

F 201A - 2010

1) Suppose that D is a PID and R is any ring with identity. Let $\phi: D \to R$ be a homom of rings. Prove that,

(a) $\phi(D)$ is a commutative ring in which every ideal is principal.

Pf:

Let D be a PID and R any ring with identity.

Let $\phi: D \to R$ be a homom of rings.

NTS $\phi(D)$ is a commutative ring in which every ideal is principal.

Since $\phi: D \to R$ is a ring homom, then $\phi(D)$ is a subring of R.

TO show $\phi(D)$ commutative consider,

$\phi(a), \phi(b) \in \phi(D)$ s.t. $a, b \in D$.

Well, $\phi(a)\phi(b) = \phi(ab)$ since ϕ homom

$= \phi(ba)$ since $ab \in D$ & D is PID.

$= \phi(b)\phi(a)$ since ϕ homom.

Thus $\phi(D)$ is a commutative ring.

Now we will show that all ideals of $\phi(D)$ are principal.

Let I be an ideal of $\phi(D)$.

NTS: $\phi^{-1}(I)$ is an ideal in D.

Let $a, b \in \phi^{-1}(I)$ and $r \in D$.

So $\phi(a), \phi(b) \in I$.

Since I is an ideal, $\phi(a) - \phi(b) \in I$.

So $\phi(a) - \phi(b) = \phi(a-b) \in I$. So $a - b \in \phi^{-1}(I)$.

since I ideal and $\phi(a) \in I$, then $\phi(r)\phi(a) \in I$

but $\phi(r)\phi(a) = \phi(ra)$.

So $\phi(ra) \in I$, so $ra \in \phi^{-1}(I)$.

thus $\phi^{-1}(I)$ is an ideal in D.

Since D is a PID then $\phi^{-1}(I)$ is a principal ideal.

~~Let $\phi^{-1}(I) = J = (j) = \{rj \mid r \in D, j \in J\}$~~

~~So $\phi(\phi^{-1}(I)) = \phi(J) = \phi((j))$~~

~~$\Downarrow$~~

~~Now show $I = (\phi(j))$. It suffices to show $\phi((j)) = (\phi(j))$~~

Let $\phi^{-1}(I) = (d)$,

so $\phi(\phi^{-1}(I)) = \phi((d)) \implies I = \phi((d))$

claim: $\phi((d)) = (\phi(d))$

($\supseteq$) let $x \in (\phi(d))$

so $x = r \cdot \phi(d)$ for $r \in \phi(D)$

so $\exists\ y \in D$ s.t. $r = \phi(y)$

so $x = \phi(y)\phi(d) = \phi(y \cdot d) \in \phi((d))$

($\subseteq$) let $x \in \phi((d))$

so $x = \phi(r \cdot d)$ where $r \in D$

$= \phi(r)\phi(d) \in (\phi(d))$

thus $I = (\phi(d))$ and every ideal is principal. //

(b) Is it true that R must be comm?

No, $\phi: \mathbb{Z} \to$ ~~2x2 matrices~~ $Mat_2(\mathbb{Z})$

ϕ is a homom by (d)

but $\{2\times 2$ matrices$\}$ are not commutative.
$\quad = Mat_2(\mathbb{Z})$

(c) Prove or disprove: $\phi(D)$ is an I.D.

Counter example,

$$\phi: \mathbb{Z} \to \mathbb{Z}_6$$
$$x \longmapsto x \bmod 6$$

Note: $\phi(\mathbb{Z}) = \mathbb{Z}_6$ b/c ϕ surjective.

but $\mathbb{Z}_6$ is not an integral domain.

since $\exists$ zero divisors in $\mathbb{Z}_6$

$(2\cdot 3 = 0 \in \mathbb{Z}_6$ but $2, 3 \neq 0 \in \mathbb{Z}_6)$

(d) Suppose that we take $D = \mathbb{Z}$ and R to be the ring of 2×2 matrices. Define $\phi: D \to R$ by $\phi(n) = nI$ where I is 2×2 identity matrix. Prove ϕ is a homom of rings.

Pf:

let $\phi: \mathbb{Z} \to R$ by $\phi(n) = nI$ where $R = Mat_2(\mathbb{Z})$

NTS: $\phi(x)\phi(y) = \phi(xy)$ and $\phi(x) + \phi(y) = \phi(x+y)$. $\forall\, x, y \in \mathbb{Z}$

Well, $\phi(x)\phi(y) = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}\begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} = \begin{bmatrix} xy & 0 \\ 0 & xy \end{bmatrix} = \phi(xy)$

$\phi(x) + \phi(y) = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} + \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} = \begin{bmatrix} x+y & 0 \\ 0 & x+y \end{bmatrix} = \phi(x+y)$.

So ϕ is a homom of rings. //

F 201A – 2010

2)

(a) Let F be a field and F[x] the ring of polynomials in one variable. Let I be an ideal in F[x]. Prove that I is a prime ideal iff I is maximal.

Pf:

($\Rightarrow$)

direct version:

let F be a field and F[x] the ring of poly in one variable.

let I be a prime ideal in F[x].

since F is a field then F[x] is a PID.

Thus $I = (p)$ where $p \in F[x]$

let $(p) \subsetneq (m) \subsetneq F[x]$

So $p = rm$ for some $r \in F[x]$

Since (p) is prime and F[x] is commutative, then either $r \in (p)$ or $m \in (p)$.

If $m \in (p) \Rightarrow (m) = (p) \Rightarrow$ (p) is maximal

If $r \in (p) \Rightarrow r = s \cdot p$ for some $s \in F[x]$

$\Rightarrow p = s \cdot p \cdot m = p \cdot (sm) \Rightarrow s \cdot m$ is a unit

$\Rightarrow m$ is also a unit $\Rightarrow (m) = F[x]$

$\Rightarrow (p)$ is maximal.

Thus I is maximal.

($\Rightarrow$)
Thm version
let F be a field $\Rightarrow$ F[x] is a PID.
Let I be a prime ideal in F[x].
Since F[x] is a PID, $I = (p)$ for some $p \in F[x]$
since (p) prime & F[x] ID $\Rightarrow$ p is prime (Thm 3.4)
since F[x] PID & p prime $\Rightarrow$ p irreducible (")
Since F[x] ID & p irred $\Rightarrow$ (p) is maximal
in the set of all proper principal ideals of F[x].
since F[x] PID, all ideals principals.
Thus (p) is maximal.
Hence I maximal.

($\Leftarrow$)
Let F be a field $\Rightarrow$ F[x] PID.
since F[x] commutative with identity then
every maximal ideal is prime. //

(b) Find all prime and maximal ideals in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{12}$.

$\mathbb{Z}_{11}$ is a field
$\Rightarrow$ {0} and $\mathbb{Z}_{11}$ are only ideals (cor 2.21)
$\Rightarrow$ (0) is the only prime and the only maximal ideal in $\mathbb{Z}_{11}$

$\mathbb{Z}_{12}$
all ideals in a cyclic ring are principal, the following are the only ideals in $\mathbb{Z}_{12}$ are:

(0)
(2) = {0, 2, 4, 6, 8, 10}
(3) = {0, 3, 6, 9}
(4) = {0, 4, 8}
(6) = {0, 6}
$\mathbb{Z}_{12}$

if $ab = 2n \Rightarrow$ a or b is a multiple of 2 $\Rightarrow$ a or b $\in$ (2) $\Rightarrow$ (2) prime
Likewise $ab = 3n \Rightarrow$ a or b multiple of 3 $\Rightarrow$ a or b $\in$ (3) $\Rightarrow$ (3) prime.

since (2) & (3) are not contained in another ideal they are maximal.

since $3 \cdot 4 = 0 \in (6)$ and 3 or 4 $\notin$ (6) $\Rightarrow$ (6) is not prime
since $2 \cdot 2 = 4 \in (4)$ and $2 \notin (4)$ $\Rightarrow$ (4) is not prime
since $2 \cdot 6 = 0 \in (0)$ and 2 or 6 $\notin$ (0), (0) is not prime

F 201A -2010

3)

(a) Let $\mathbb{R}$ be the field of real numbers and $\mathbb{C}$ the field of complex numbers. Let $\phi: \mathbb{R}[x] \to \mathbb{C}$ be the homom of rings which is the evaluation at i ie. $\phi(f) = f(i)$.

Prove that ϕ is surjective and that $\ker\phi$ is a maximal ideal. Determine the kernel of ϕ, ie. what is a necessary and sufficient condition for a polynomial to be in $\ker\phi$.

Pf:

Define $\phi: \mathbb{R}[x] \longrightarrow \mathbb{C}$
$f(x) \longmapsto f(i)$.

Let $a+bi \in \mathbb{C}$, $f(x) = a+bx \in \mathbb{R}[x]$ and $\phi(f) = a+bi$. Thus ϕ is surjective

Now we will show $\ker\phi$ is a max ideal.

We know that $\ker\phi$ is an ideal.

Since $\mathbb{R}$ is a field $\Rightarrow \mathbb{R}[x]$ a PID $\Rightarrow$ $\ker\phi$ is principal.

Suppose $\ker\phi = (f(x))$ is not maximal.

ie $\exists\ (g(x))$ s.t. $\ker\phi = (f(x)) \subsetneq (g(x)) \subsetneq \mathbb{R}[x]$.

Thus $f(x) = r(x)g(x)$ for some $r(x) \in \mathbb{R}[x]$

$\Rightarrow f(i) = r(i)g(i) = 0$.

But $\mathbb{C}$ is an ID thus $r(i) = 0$ or $g(i) = 0$.

if $g(i) = 0 \Rightarrow g(x) \in \ker\phi$ $\longrightarrow\!\!\!\longleftarrow$

if $r(i) = 0 \Rightarrow r(x) \in \ker\phi$

$\Rightarrow r(x) = f(x)s(x)$ for some $s(x) \in \mathbb{R}[x]$.

$\Rightarrow f(x) = f(x)s(x)g(x) \Rightarrow (g(x)) = \mathbb{R}[x]$ $\longrightarrow\!\!\!\longleftarrow$

Thus $\ker\phi$ is maximal.

Claim: $\ker \phi = (X^2+1)$

"$\subseteq$" let $f \in \ker \phi$.

consider $f(X) = g(x)(x^2+1) + r(x)$ where $\deg r(x) \leq 1$

$\Rightarrow r(X) = ax+b$

$\Rightarrow ai+b=0$

$\Rightarrow b = -ai$ $\longrightarrow\!\leftarrow$

$\Rightarrow r(x) = 0$

$\Rightarrow f(x) \in (X^2+1)$

"$\supseteq$" let $f(x) \in (X^2+1)$

$\Rightarrow f(x) = g(x)(X^2+1)$

$\Rightarrow f(i) = g(i)(i^2+1) = 0$

$\Rightarrow f \in \ker \phi$.

//

Thus $\ker \phi = (X^2+1)$.

(b) Repeat (a) but assuming now $\phi : \mathbb{C}[X] \longrightarrow \mathbb{C}$ is evaluation at i.

Let $a+bi \in \mathbb{C}$ where $\phi : \mathbb{C}[X] \longrightarrow \mathbb{C}$
$f(x) \longmapsto f(i)$

Let $f(x) = a+bX \Rightarrow f(i) = a+bi \Rightarrow \phi$ surjective.

Since $\mathbb{C}[X]$ is still a PID, so argument for $\ker \phi$ maximal is exactly the same as (a).

Claim: $\ker \phi = (X-i)$

"$\subseteq$" let $f(x) \in \ker \phi$

consider $f(x) = g(x)(X-i) + r(x)$ where $\deg(r(x)) = 0$

so $r(x) = a$ but $r(i) = 0 \Rightarrow a = 0$

$\Rightarrow r(x) = 0$.

$\Rightarrow f(x) \in (X-i)$

"$\supseteq$" let $f(x) \in (X-i)$

$\Rightarrow f(x) = g(x)(X-i)$

$\Rightarrow f(i) = 0$

$\Rightarrow f \in \ker \phi$.

Thus

$\ker \phi = (X-i)$ //

F 201A - 2010

4)

(a) Prove that any free abelian group of rank 2 is isomorphic to $\mathbb{Z} \times \mathbb{Z}$.

note - rank = # of generators.

Pf:
Let F be a free abelian group of rank 2.
Since F has rank 2 it is generated by two elements say a, b so $F = \langle \{a, b\} \rangle$.
Let $g \in F$. Then $g = n_1 a + n_2 b$ for some $n_1, n_2 \in \mathbb{Z}$.
Define $\phi: F \longrightarrow \mathbb{Z} \times \mathbb{Z}$ NTS ϕ is isomorphism
$g \longmapsto (n_1, n_2)$

homom: • Let $g, h \in F$. Let $n_1, n_2, m_1, m_2 \in \mathbb{Z}$ s.t. $\phi(g) = (n_1, n_2)$ & $\phi(h) = (m_1, m_2)$

$\phi(gh) = (n_1 + m_1, n_2 + m_2)$
$= (n_1, n_2) + (m_1, m_2) = \phi(g) + \phi(h)$. ✓

1-1: Let $\phi(g) = \phi(h) \Rightarrow (n_1, n_2) = (m_1, m_2)$
$\Rightarrow n_1 = m_1$ and $n_2 = m_2 \Rightarrow g = h$ so ϕ 1-1. ✓

onto: Let $(n_1, n_2) \in \mathbb{Z} \times \mathbb{Z}$.
then $\exists$ a $g \in F$ s.t. $\phi(g) = (n_1, n_2)$
because $g = n_1 a + n_2 b$ (ie F is free)
$\Rightarrow \phi$ surjective. ✓.

Thus ϕ is an isomorphism //

(b) Give an example of a subset of $\mathbb{Z} \times \mathbb{Z}$ which generates $\mathbb{Z} \times \mathbb{Z}$ as a group but is not a basis.

Consider $\{(0,1), (1,0), (1,1)\} \subseteq \mathbb{Z} \times \mathbb{Z}$ and generates $\mathbb{Z} \times \mathbb{Z}$ but $(0,1) + (1,0) + (-1)(1,1) = 0$

$\Rightarrow \{(0,1), (1,0), (1,1)\}$ is not linearly independent so its not a basis. //

c) Find two non-isomorphic subgroups of $\mathbb{Z}\times\mathbb{Z}$ with index 4.

Consider $2\mathbb{Z}\times 2\mathbb{Z}$, $4\mathbb{Z}\times\mathbb{Z}$ as subgroups of $\mathbb{Z}\times\mathbb{Z}$.

Well, $\mathbb{Z}\times\mathbb{Z}/\ 2\mathbb{Z}\times 2\mathbb{Z} = \{\ 2\mathbb{Z}\times 2\mathbb{Z},\ (1,1)+(2\mathbb{Z}\times 2\mathbb{Z}),\ (0,1)+(2\mathbb{Z}\times 2\mathbb{Z}),$
$(1,0)+(2\mathbb{Z}\times 2\mathbb{Z})\ \}$

and $\mathbb{Z}\times\mathbb{Z}/\ 4\mathbb{Z}\times\mathbb{Z} = \{\ 4\mathbb{Z}\times\mathbb{Z},\ (1,0)\times(4\mathbb{Z}\times\mathbb{Z}),\ (2,0)+(4\mathbb{Z}\times\mathbb{Z}),$
$(3,0)+(4\mathbb{Z}\times\mathbb{Z})\ \}$.

so both are subgroups with index 4.

These are non-isomorphic subgroups.

Since $\mathbb{Z}\times\mathbb{Z}/\ 4\mathbb{Z}\times\mathbb{Z}$ is cyclic

because $\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z} = \langle (1,0)\times(4\mathbb{Z}\times\mathbb{Z})\rangle$

and $\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times 2\mathbb{Z}$ is not cyclic

because $\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times 2\mathbb{Z} = \langle (1,1)+(2\mathbb{Z}\times 2\mathbb{Z}),\ (0,1)+(2\mathbb{Z}\times 2\mathbb{Z})$

F 201A-2010

5) Let G be a finite abelian group and let H be a subgroup of G.

(a) Prove that $\exists$ a subgrp K of G which is isomorphic to G/H.

Pf:

Let G be a finite abelian group and let $H \trianglelefteq G$.

Since G is finite abelian, $G \cong \mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{i_n}}$

also note G finite abelian $\Rightarrow H \trianglelefteq G$, $\Rightarrow G/H$ finite abelian and $|G/H| \mid |G|$

that is $G/H \cong \mathbb{Z}_{p_1^{j_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{j_n}}$ where $j_\ell \le i_\ell$

but $G/H \cong \mathbb{Z}_{p_1^{j_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{j_n}}$

$\cong p_1^{k_1}\mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus p_n^{k_n}\mathbb{Z}_{p^{i_n}}$ where $i_\ell = k_\ell + j_\ell$ (see $\star$)

$\le \mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{i_n}}$

$\cong G$.

Thus since G/H is isomorphic to a subgrp of $\mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{i_n}} \cong G$, then $\exists$ a subgrp of G, call it K s.t. $K \cong G/H$

($\star$) to show $\mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{i_n}} \cong p_1^{k_1}\mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus p_n^{k_n}\mathbb{Z}_{p^{i_n}}$

ISTS $a\mathbb{Z}_{ab} \cong \mathbb{Z}_b$

Let $\phi: \mathbb{Z}_b \longrightarrow a\mathbb{Z}_{ab}$

$\bar{x} \longmapsto \overline{ax}$

suppose $\phi(\bar{x}) = \phi(\bar{y})$

so $\overline{ax} = \overline{ay} \Rightarrow \overline{ax} - \overline{ay} = 0$

$\Rightarrow ab \mid (ax - ay)$

$\Rightarrow b \mid (x-y)$

$\Rightarrow \bar{x} = \bar{y}$

$\Rightarrow \phi$ injective.

well, $|a\mathbb{Z}_{ab}| = \frac{ab}{a} = b = |\mathbb{Z}_b|$

$\Rightarrow \phi$ is bijective.

$\phi(\bar{x}+\bar{y}) = \bar{a}(\bar{x}+\bar{y}) = \overline{ax} + \overline{ay} = \phi(\bar{x}) + \phi(\bar{y})$

Thus ϕ isomorphism.

well-defined:

Let $\bar{x} = \bar{y}$ in $\mathbb{Z}_b$

$\Rightarrow b \mid (x-y)$

$\Rightarrow ab \mid (ax - ay)$

$\Rightarrow \overline{ax} = \overline{ay}$

$\Rightarrow \phi(\bar{x}) = \phi(\bar{y})$

Thus ϕ is well-defined. //

(b) Prove that G is isomorphic to the direct product $H \times G/H$

Pf:
From part (a) we know $\exists$ an iso. $\phi : G/H \longrightarrow K$
$aH \longmapsto k$.

Let $g \in aH$ so $g = ah$ for $h \in H$.

Define $\psi : G \longrightarrow H \times K \cong H \times G/H$
$g \longmapsto (h, \phi(aH))$

NTS ψ is iso.

homom: $\psi(g_1 g_2) = (h_1 h_2, \phi(a_1 a_2 H))$
$= (h_1, \phi(a_1 H))(h_2, \phi(a_2 H))$ } b/c ϕ iso
$= \psi(g_1)\psi(g_2)$

1-1: Let $\psi(g_1) = \psi(g_2)$
$\Rightarrow (h_1, \phi(a_1 H)) = (h_2, \phi(a_2 H))$
$\Rightarrow h_1 = h_2$ and $\phi(a_1 H) = \phi(a_2 H)$
$\Rightarrow h_1 = h_2$ and $a_1 H = a_2 H$ b/c ϕ iso
$\Rightarrow g_1 = g_2$

onto: Let $(h, \phi(aH)) \in H \times K$
Consider $g \in G$ s.t. $g = aH$
so $\exists$ $\psi(g) = (h, \phi(aH))$.

Thus ψ isomorphism. //

c) Suppose that $G = \mathbb{Z}_6 \times \mathbb{Z}_{15}$ and $H = \{(0,0), (3,0)\}$. check that H is a subgroup of G and find the group K which is isomorphic to G/H.

check that $H \leq G$.

$H = \{(0,0), (3,0)\}$

Thus $H \leq G$.

$|H| = 2$.

① H is nonempty b/c $(0,0) \in H$

② products.

$(0,0) + (3,0) = (3,0) \in H$

$(3,0) + (3,0) = (0,0) \in H$

③ inverses

$(3,0) + (3,0) = (0,0) \in H$. ✓

Find $K \cong G/H$.

$G = \mathbb{Z}_6 \times \mathbb{Z}_{15}$ so $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$|G| = 90 \Rightarrow |G/H| = \frac{|G|}{|H|} = \frac{90}{2} = 45$

so by (a) $\exists$ a subgrp of G of order 45

Every abelian grp is isomorphic to either.

$\mathbb{Z}_{45} \cong \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

BUT G has no elmt of order 9

So $G/H \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$\|$

K.

//

F 201A – 2010

(6)

(a) Prove that G is abelian if $G/C(G)$ is cyclic. Is the converse true?

Pf:

Let $G/C(G)$ be cyclic. So $\exists\, g \in G$ s.t. $\langle gC(G)\rangle = G/C(G)$.

Let $a, b \in G$, so $\exists\, i, j \in \mathbb{Z}$ s.t.

$$aC(G) = g^i C(G) \quad \text{and} \quad bC(G) = g^j C(G).$$

So $a = g^i x$ and $b = g^j y$ for $x, y \in C(G)$

Consider, $ab = g^i x g^j y$

$= g^i g^j x y$ — b/c $x \in C(G)$

$= g^j g^i y x$ — b/c $y \in C(G)$

$= g^j y g^i x$ — b/c $y \in C(G)$

$= ba.$ Thus G is abelian. //

Converse.

True. assume G is abelian.

Then $C(G) = G$

Thus $G/C(G) = G/G \cong$ [illegible]. Eg.

which is trivially cyclic.

ie. generated by the identity element.

(b) Prove that a group of order p^2 is abelian.

Pf:

Let $|G| = p^2$.

Since $C(G) \leq G$ then by Lagranges Thm

$|C(G)| = 1, p,$ OR p^2.

So $|G/C(G)| = |G|/|C(G)| =: \frac{p^2}{1} = p^2$ OR

$p^2/p = p$ OR

$p^2/p^2 = 1$

Case 1:

$|G/C(G)| = 1 \Rightarrow$

$|C(G)| = p^2 \Rightarrow G = C(G)$

But $C(G)$ is abelian $\Rightarrow G$ is abelian.

Case 2:

$|G/C(G)| = p \Rightarrow$

$G/C(G)$ is cyclic $\Rightarrow G$ is abelian by part (a).

Case 3:

$|G/C(G)| = p^2 \Rightarrow$

$|C(G)| = 1$ so $C(G) = \{e\}$.

$\rightarrow\!\leftarrow$ b/c the center of a nontrivial finite p-grp G contains more than one elmt.

Thus G is abelian. //

Cor 5.4 - The center of a nontrivial finite p-group G contains more than one elmt.

Pf:

Consider the grp action $\phi: G \times G \to G$ by conjugation.
$(g, x) \mapsto gxg^{-1}$

This is a grp action b/c

$\phi(e, x) = exe^{-1} = x$.

$\phi(g_1 g_2, x) = g_1 g_2 x (g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1}$

$\phi(g_1, g_2 x) = g_1 \phi(g_2 x) g_1^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1}$ $\Big\} = \checkmark$.

Define $X_0 = \{x \in G \mid gxg^{-1} = x \ \forall\ g \in G\} = C(G)$.

Since $[G : C_G(x_i)] > 1$ and $p \mid |G|$ then we get the class equation:

$$|G| = |C(G)| + \sum_{i=1}^{r} [G : C_G(x_i)].$$

So $[G : C_G(x_i)] \geq 2$ and $[G : C_G(x_i)] \mid |G|$

but the only prime that divides $|G|$ is p so $[G : C_G(x_i)] = p^k$ for some $k \geq 0$.

If $k = 0$, then $[G : C_G(x_i)] = 1 \to \leftarrow$.

thus $p \mid [G : C_G(x_i)]$.

also recall $p \mid |G|$ so $p \mid |C(G)|$

Thus $|C(G)| \neq 1$.

So $C(G)$ contains more than one elmt. //

F 201A - 2010

7) Let G be the group of 2×2 invertible matrices with real entries. Let H be the subgroup consisting of diagonal matrices. Prove that $C_G(H) = H$ and that $N_G(H)$ is the group of 2×2 matrices of the form.

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0, \; ab = 0, \; cd = 0 \right\}.$$

~~PROVE DONE~~

7) Let G be the group of 2×2 invertible matrices with real entries. Let H be the subgroup consisting of diagonal matrices. Prove $C_G(H)=H$ and $N_G(H)$ is the group of 2×2 matrices of the form $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad-bc\neq 0,\ ab=0,\ cd=0\right\}$. Prove that $C_G(H)$ is a normal subgroup in $N_G(H)$ and find the index $[N_G(H): C_G(H)]$.

Pf:

(1) Let $A\in C_G(H)$ then $AB=BA\ \forall B\in H$

Let $B=\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $B=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ s.t. $a\neq b$

$$AB=\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}=\begin{pmatrix} pa & qb \\ ra & sb \end{pmatrix}$$

$$BA=\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}=\begin{pmatrix} ap & aq \\ br & bs \end{pmatrix}$$

So $qb=aq$ and $br=ra$

$\Rightarrow q(a-b)=0$ and $r(a-b)=0$ $\mathbb{R}$ is a field and $a\neq b$

$\Rightarrow q=0$ and $r=0$

$\Rightarrow A=\begin{pmatrix} p & 0 \\ 0 & s \end{pmatrix}\in H$

Thus $C_G(H)=H$

(2) n.t.s. $N_G(H)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad-bc\neq 0,\ ab=0,\ cd=0\right\}$

Let $A\in N_G(H)$, then $ABA^{-1}\in H\ \forall B\in H$

If $A=\begin{pmatrix} p & q \\ r & s \end{pmatrix}\Rightarrow A^{-1}=\frac{1}{ps-rq}\begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$ (note $ps-rq\neq 0$ since G contains all invertible matrices)

$$ABA^{-1}=\frac{1}{ps-rq}\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} s & -q \\ -r & p \end{pmatrix}=\frac{1}{ps-rq}\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} as & -aq \\ -br & bp \end{pmatrix}$$

$$=\frac{1}{ps-rq}\begin{pmatrix} pas-brq & -apq+bpq \\ ras-brs & -aqr+bps \end{pmatrix}\in H$$

$\Rightarrow pq(b-a)=0$ and $rs(a-b)=0$

generally $a\neq b$; $pq=0$ and $rs=0$

$\Rightarrow A\in\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad-bc\neq 0,\ ab=0,\ cd=0\right\}$

Thus $N_G(H)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad-bc\neq 0, ab=0, cd=0\right\}$

(3) [on back]

F 201A-2010

8) Find the sylow-3 subgroups of S_5.

Well, $|S_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$

so $\exists$ sylow 2, sylow 3, sylow 5.

w/ $|\text{sylow } 3| = 3$.

divisors of 120: 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120.

so if $p=3$: $3k+1$

choices for k: 1, 4, 10, 40.

claim: $\exists$ 10 sylow-3 subgrps of S_5, each of order 3

$\{e, (123), (132)\}$	$\{e, (134), (143)\}$	$\{e, (234), (243)\}$
$\{e, (124), (142)\}$	$\{e, (135), (153)\}$	$\{e, (235), (253)\}$
$\{e, (125), (152)\}$	$\{e, (145), (154)\}$	$\{e, (245), (254)\}$
		$\{e, (345), (354)\}$

$\nexists$ any more bic $|\text{sylow 3 subgrp}| = 3$ so all $\simeq$ to $\mathbb{Z}_3$.

Thus any sylow 3-subgrp is cyclic so it contains an elmt of order 3 that generates it.

~~In S_5 $\exists$ only 10 elmts of order 3~~ Thus $\exists$ only 10 distinct subgrp of order 3. So $\exists$ only 10 sylow-3 subgrp of S_5. //

F 201A - 2010

9) Prove that a grp of order 12 has a normal sylow subgroup.

Well $12 = 2^2 \cdot 3$

so $\exists$ sylow-2 subgroups of order 4 and
sylow-3 subgroups of order 3

divisors of 12: 1, 2, 3, 4, 6, 12.

Since the # of sylow p-subgroups must divide $|G|$ & be of the form $kp+1$.

So $p=2$: $2k+1$ OR $k \equiv 1 \bmod 2$
$k = 1, 3$.

$p=3$: $3k+1$ OR $k \equiv 1 \bmod 3$
$k = 1, 4$.

} so either 1 or 3 sylow 2's & 1 or 4 sylow 3's

Case 1: $\exists$ only 1 sylow 3-subgroup $\Rightarrow$ its normal $\Rightarrow$ done.

Case 2: $\exists$ 4 sylow 3 subgroups & $|\text{sylow 3-subgrp}| = 3$.
so we have H_1, H_2, H_3, H_4. Then $|H_i| = 3$ &
$H_i \cong \mathbb{Z}_3 \quad \forall\, 1 \le i \le 4$
also $H_i \cap H_j = \{e\}$ for $i \neq j$ since $H_i \neq H_j$ and
$H_j, H_i \trianglelefteq \mathbb{Z}_3$.

So there are $4(3-1) = 4(2) = 8$ distinct non-identity elmt of order 3. Thus $\exists$ $12-8=4$ elmts of order a power of 2. So $\exists$ only one sylow 2-subgroup of order 4. $\Rightarrow$ its normal.

F 201A – 2010

10) Let $N \trianglelefteq G$.

(a) Define a group action of G on N.
You must check that it is a group action.

Define $\phi : G \times N \longrightarrow N$
$\phi(g, n) \longmapsto gng^{-1}$

Note $gng^{-1} \in N$ b/c $N \trianglelefteq G$.

Check that this is a group action.

$\phi(e, n) = ene^{-1} = n$

$\phi(g_1 g_2, n) = g_1 g_2 n (g_1 g_2)^{-1} = g_1 g_2 n g_2^{-1} g_1^{-1}$

$\phi(g_1, g_2 n) = g_1 \phi(g_2 n) g_1^{-1}$
$= g_1 g_2 n g_2^{-1} g_1^{-1}$ $= \checkmark$.

b) Define an action of G on the set of cosets G/N.
Prove that the kernel of the induced homom $G \longrightarrow A(G/N)$ is N.

Define $\psi : G \times G/N \longrightarrow G/N$
$(g, g'N) \longmapsto gg'N$

Well-defined:
Let $g_1 N = g_2 N$
$\Rightarrow g_2^{-1} g_1 \in N$
$\Rightarrow g_2^{-1}(g^{-1}g) g_1 \in N$
$\Rightarrow (gg_2)^{-1}(gg_1) \in N$
$\Rightarrow gg_1 N = gg_2 N$
$\Rightarrow \psi(g, g_1 N) = \psi(g, g_2 N)$.

check it's an action:
$\psi(e, g'N) = eg'N = g'N$.
$\psi(g_1 g_2, g'N) = g_1 g_2 g'N$
$\psi(g_1, g_2 g'N) = g_1 \psi(g_2 g'N)$
$= g_1 g_2 g'N$ $= \checkmark$

Define $\psi_g : G/N \longrightarrow G/N$

$g'N \longmapsto \psi(g, g'N)$

Define $\gamma : G \longrightarrow A(G/N)$

$g \longmapsto \psi_g$

Note γ is a homom since it is induced by a group action.

Consider $\ker \gamma = \{ g \in G \mid \psi(g, g'N) = g'N \quad \forall g' \in G \}$

so $\psi(g, g'N) = g'N$

$\Rightarrow gg'N = g'N$

so $gg'n_1 = g'n_2$ for $n_1, n_2 \in N$

$\Rightarrow g = g'n_2 (g'n_1)^{-1}$

$= g' n_2 n_1^{-1} (g')^{-1}$

$\underbrace{\quad}_{\in N}$

since $N \triangleleft G$

$\Rightarrow g' n_2 n_1^{-1} (g')^{-1} \in N$

so $g \in N$

so $\ker \gamma = \{ g \in N \}$

so $\ker \gamma$ is N. //

2012

Rush

Algebra Qualifier, Part A

September 29, 2012

Do four out of the five problems.

1. Let G be a finite group and let p be a prime integer.

(a) Show that if p divides $(G:1)$, then G contains an element of order p. (You may assume this holds if G is abelian.)

(b) Show that if each $x \in G$ has order p^k for some $k \geq 0$, then $(G:1)$ is a power of p.

2. Prove or disprove the following.

(a) The ring $\mathbb{Z}[\sqrt{-19}]$ is a PID.

(b) Each nonzero nonunit of $\mathbb{Z}[\sqrt{-19}]$ is a product of irreducible elements.

3. Let R be a commutative unitary ring. A multiplcative subset S of R is said to be *saturated* if $xy \in S$ for $x, y \in R$ implies $x, y \in S$.

(a) Show that if S is a saturated multiplicative subset of R, then $R \setminus S$ is a union of prime ideals of R.

(b) An element $a \in R$ is a *zero-divisor* if $ab = 0$ for some $b \neq 0$ in R. Show that the set of zero-divisors of R is a union of prime ideals of R.

4. How many elements of order 7 are there in a simple group of order 168? Prove your answer.

5. (a) Define the characteristic of a ring.

(b) Assume R is a commutative unitary ring having only one maximal ideal M. Show that the characteristic of R is either zero or a power of a prime.

(c) Show that if R/M has characteristic zero, where R is as in (b), then R contains a field.

(d) Give an example of a ring R, as in (b), of characteristic zero having a non-maximal prime ideal P such that the characteristic of R/P is **not** zero.

Fall 2011

Chari

2011.

each question worth 10 pts, perfect score is 60 pts

Part A.

1. (a) Suppose that G is a group and that H_1 and H_2 are two distinct subgroups of G. State and prove a sufficient condition for $H_1 \cup H_2$ to be a group.

   (b) Give an example of a group G and two subgroups K_1 and K_2 such that $K_1 \cup K_2$ is strictly contained in the subgroup generated by K_1 and K_2.

2. Suppose that G is a group and H, K are subgroups of G such that G is the internal direct product of H and K. Prove that H and K are normal subgroups of G and $G/H \simeq K$. Deduce that there does not exist a subgroup H of S_5 such that S_5 is isomorphic to the direct product of H and A_5.

3. Prove that a free abelian group is a free group if and only if it is cyclic. Give an example to show that a cyclic group may not be free.

4. How many subgroup of order 9 does the group $\mathbf{Z}_9 \oplus \mathbf{Z}_{27}$ have? How many non-isomorphic subgroups of order 9 does it have?

5. Suppose that H acts on a set S. Given $s \in S$, define the H-orbit of s. Prove that if $s' \in S$ is another element then either s' is in the orbit of s or that the orbits of s and s' are disjoint.

6. Prove that a group of order 200 is not simple.

7. Let t be an indeterminate and consider the ring of polynomials $\mathbf{R}[t]$ where $\mathbf{R}$ is the set of real numbers. Using the fact that $\mathbf{R}[t]$ is a principal ideal domain, prove that the ideal generated by t^2+2 is maximal. Suppose now that we work with the ring $\mathbf{C}[t]$ where $\mathbf{C}$ is the set of complex numbers. Find a polynomial f such that the ideal generated by f is proper and strictly contains the ideal generated by t^2+2.

8. Suppose that R is the ring $\mathbf{Z}_6$ and $S = \{2, 4\}$ is a subset of R. Prove that $S^{-1}R$ is a finite field and identify the field.

Fall 2010

2011 A 1

Let G be a group.

(1) Given distinct subgroups H_1, H_2 of G, state and prove a sufficient conditions for $H_1 \cup H_2$ to be a subgroup.

condition: $H_1 \cup H_2$ must be closed under the group operation

Pf:

Let G be a group and $H_1, H_2 < G$ (distinct)

since $H_1, H_2 < G$ then $e \in H_1$, and $e \in H_2$.

So $e \in H_1 \cup H_2$. Thus $H_1 \cup H_2$ is nonempty.

Let $a, b \in H_1 \cup H_2$

NTS: $ab \in H_1 \cup H_2$ & $a^{-1} \in H_1 \cup H_2$.

By condition we assumed $H_1 \cup H_2$ is closed under the operation so $ab \in H_1 \cup H_2$.

Since $a \in H_1 \cup H_2$ then $a \in H_1$ or $a \in H_2$.

WLOG let $a \in H_1$, since $H_1 < G$, $a^{-1} \in H_1$,

so $a^{-1} \in H_1 \cup H_2$. Thus $H_1 \cup H_2$ is a subgroup under this condition. //

(2) Give an example of a group G and two subgroups K_1, K_2 s.t. $K_1 \cup K_2$ is properly contained in the subgroup generated by K_1, K_2.

EX:

$G = \mathbb{Z}_6$

$K_1 = \langle 2 \rangle = \{2, 4, 0\}$ $\quad K_2 = \langle 3 \rangle = \{3, 0\}$.

well K_1 and K_2 generate the join

$$\langle K_1 \cup K_2 \rangle = K_1 \vee K_2 = \{ a b \mid a \in K_1 \& b \in K_2 \}.$$

$K_1 \vee K_2 = \{0, 2, 3, 4, 5, 1\} = \mathbb{Z}_6$

$K_1 \cup K_2 = \{0, 2, 3, 4\}$.

Note, $K_1 \cup K_2$ is properly contained in $K_1 \vee K_2$.

2011 A2:

Suppose that G is a group and H, K are subgroups of G s.t. G is the internal direct product of H and K. Prove that $H, K \trianglelefteq G$ and $G/H \cong K$. Deduce that $\nexists$ a subgp H of S_5 s.t. $S_5 \cong H \times A_5$

Pf:

Let G be a group and $H, K < G$ s.t. G is the internal direct product of H and K. So $G \cong H \oplus K$. By definition of internal direct product $H, K \trianglelefteq G$.

NTS $G/H \cong K$.

Consider $\pi : H \oplus K \longrightarrow K$
$(h, k) \longmapsto k$.

clearly $\ker \pi = H \oplus e \cong H$. and $\mathrm{Im}(\pi) = K$.

So by the first isomorphism thm,

$$H \oplus K / H \cong K$$

Hence $G/H \cong K$. //

ATC $\exists$ $H < S_5$ s.t. $S_5 \cong H \oplus A_5$.

By above, $H \trianglelefteq S_5$ and $S_5/A_5 \cong H$.

$\Rightarrow |H| = [S_5 : A_5] = 2$.

$\Rightarrow H = \langle (ij) \rangle$ for some distinct $i, j \in \{1, \dots, 5\}$

$\forall \sigma \in S_5$ we have $\sigma(ij)\sigma^{-1} = (\sigma(i)\sigma(j))$

Since $H \trianglelefteq S_5$ & $|H| = 2$, $(\sigma(i)\sigma(j)) = (i, j)$ $\rightarrow\leftarrow$.

Thus $\nexists$ $H < S_5$ s.t. $S_5 \cong H \oplus A_5$. //

2011 A3:

Prove that a free abelian group is a free group iff it is cyclic.

Pf:

($\Rightarrow$) Suppose G is a free abelian group that is also a free group.

Suppose G is generated by the set $X = \{x, y\}$

Since G is free, $xyx^{-1}y^{-1}$ is a reduced word

$\Rightarrow xyx^{-1}y^{-1} \neq e$

$\Rightarrow xy \neq yx$ $\rightarrow\leftarrow$ since G is abelian.

So X can only be generated by one elmt.

Thus G is cyclic

($\Leftarrow$) Suppose G is a free abelian group that is cyclic

$\Rightarrow G = \langle x \rangle$

So G has a nonempty basis, namly $\{x\}$

Thus it must be free. //

Give an example to show that a cyclic group may not be free.

$\mathbb{Z}_2$ bic $\mathbb{Z}_2$ ~~* to direct copies of $\mathbb{Z}$.~~ has a relation [bic ~~called about~~ take $x = 1$, xx is reduced word but $xx = 1+1 = 0 = id$ $\leftarrow$

2011 A4

How many subgrps of order 9 does the group $\mathbb{Z}_9 \oplus \mathbb{Z}_{27}$ have? How many non-iso subgrps of order 9 does it have?

Pf:

Since $\mathbb{Z}_9 \oplus \mathbb{Z}_{27}$ is abelian, the subgrps of order 9 are either iso to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_9$.

- consider subgrps iso to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

in $\mathbb{Z}_9$, $\langle 3 \rangle = \langle 6 \rangle$ & $|\langle 3 \rangle| = 3$ (3 & 6 only elmts of order 3)

in $\mathbb{Z}_{27}$, $\langle 9 \rangle = \langle 18 \rangle$ & $|\langle 9 \rangle| = 3$ (9 & 18 only elmts of order 3)

so there is only one subgroup iso to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ which is $\{0, 3, 6\} \oplus \{0, 9, 18\}$.

- subgrp iso to $\mathbb{Z}_9$ (cyclic)

so need to find elmts of order 9 in $\mathbb{Z}_9 \oplus \mathbb{Z}_{27}$.

Let $a \in \mathbb{Z}_9$ & $b \in \mathbb{Z}_{27}$ the order of (a,b) is $\text{lcm}(|a|, |b|)$

ϕ = Euler function ($\phi(a) = \#$ of $< a$ that are rel. prime to a) $= 9$

$\phi(1) = 1$.

$\lvert a \rvert$	$\lvert b \rvert$	$\phi(a)\phi(b)$
9	1	$6 \cdot 1 = 6$
9	3	$6 \cdot 2 = 12$
9	9	$6 \cdot 6 = 36$
1	9	$1 \cdot 6 = 6$
3	9	$2 \cdot 6 = 12$

$+ = 72$ elmts of order 9.

but in $\mathbb{Z}_9$ there are $\phi(9) = 6$ elmts that generate $\mathbb{Z}_9$ so there are $\frac{72}{6} = 12$ distinct subgrp iso to $\mathbb{Z}_9$

and only two noniso subgrps of order 9 so there are $12 + 1 = 13$ subgrps

2011 A5:

Suppose that H acts on a set S. Given $s \in S$, define the H-orbit of s. Prove that if $s' \in S$ is another elmt then either s' is in the orbit of s or that the orbits of s and s' are disjoint.

Def:

The H-orbit of s is $\{ s' \in S \mid hs = s' \text{ for some } h \in H \}$

denote the H-orbit of s as $\bar{s}$

Pf:

Suppose $s' \in S$ s.t. $s' \neq s$ and suppose $s' \notin \bar{s}$

let $x \in \bar{s} \cap \bar{s'}$

$\Rightarrow \exists\ h, h' \in H$ s.t. $hs = h's' = x$

~~$(h')^{-1} hs = (h')^{-1} h's$~~

~~$[(h')^{-1} h] s = es = s$~~

Now acting on x by $(h')^{-1} \in H$ (since $h' \in H$ & H is a group)

we get $(h')^{-1} hs = (h')^{-1} h's'$.

Now we get, $((h')^{-1} h) s = ((h')^{-1} h') s' = es' = s'$

since H is a group, $(h')^{-1} h \in H$. $\Rightarrow$ and $s' \in \bar{s}$, $\longrightarrow\!\longleftarrow$ b/c $s' \notin \bar{s}$

Thus $\bar{s} \cap \bar{s'} = \emptyset$.

Therefore, either s' is in the orbit of s or

the orbit of s and s' are disjoint. //

2011 A 6:

Prove that a group of order 200 is not simple.

Pf:

Let G be a group of order $200 = 2^3 \cdot 5^2$.

By the first sylow thm ∃

sylow-2 subgroups of order 8

sylow-5 subgroups of order 25.

divisors of 200: 1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200

By the 3rd sylow thm, the # k of sylow p-subgroups must divide $|G|$ & be of the form $kp+1$.

so $p=2$: $2k+1$ or $k \equiv 1 \bmod 2$.

$k = 1, 5, 25$

$p=5$: $5k+1$ or $k \equiv 1 \bmod 5$

$k = 1$

Thus there is only one sylow-5 subgroup

hence it is normal.

Thus a group of order 200 is not simple. //

2011 A 7:

Let t be an indeterminant and consider the ring of polynomials $\mathbb{R}[t]$ where $\mathbb{R}$ is the set of real #. Using the fact that $\mathbb{R}[t]$ is a PID, prove that the ideal generated by t^2+2 is maximal.

Pf:

Since $\mathbb{R}[t]$ is a PID, then irred. elmt generate maximal ideals. Since the only roots of t^2+2 are $\pm i\sqrt{2} \notin \mathbb{R}$, t^2+2 is an irred. poly. Hence, the ideal it generates is maximal.

Suppose now that we work with the ring $\mathbb{C}[t]$ where $\mathbb{C}$ is the set of complex #. Find a poly f s.t. the ideal generated by f is proper & strictly contains the ideal generated by t^2+2.

Now suppose we are working with ring $\mathbb{C}[t]$. Then $t-i\sqrt{2}$ is irreducable since irreducable poly over $\mathbb{C}[t]$ are degree 1 polynomials. Since $t^2+2 = (t-i\sqrt{2})(t+i\sqrt{2})$ and $t+i\sqrt{2} \in \mathbb{C}[t]$, $t^2+2t \in (t-i\sqrt{2})$ then $(t^2+2t) \subsetneq (t-i\sqrt{2}) \subsetneq \mathbb{C}[t]$.

//

2011 A8:

Suppose that R is the ring $\mathbb{Z}_6$ and $S = \{2, 4\}$ is a subset of R. Prove that $S^{-1}R$ is a finite field and identify the field.

Pf:

Using the relation $(r_1, s_1) = (r_2, s_2)$ iff $t(r_1 s_2 - r_2 s_1) = 0$ for some $t \in S$, we can identify the field $S^{-1}R$.

all possible elmts for $S^{-1}R$ are:

$\{(0,2), (0,4), (1,2), (1,4), (2,2), (2,4), (3,2), (3,4),$
$(4,2), (4,4), (5,2), (5,4)\}$.

$(0,2) = (0,4)$ b/c $0 \cdot 4 - 0 \cdot 2 = 0$.

$(0,2) = (3,2)$ b/c $0 \cdot 2 - 2 \cdot 3 = 6 \equiv 0$

$(0,2) = (3,4)$ b/c $0 \cdot 4 - 2 \cdot 3 = 6 \equiv 0$

$(1,2) = (2,4)$ b/c $1 \cdot 4 - 2 \cdot 2 = 0$

$(1,2) = (4,2)$ b/c $1 \cdot 2 - 2 \cdot 4 = 2 - 8 = 6 \equiv 0$

$(1,2) = (5,4)$ b/c $1 \cdot 4 - 2 \cdot 5 = 4 - 10 = 6 \equiv 0$

$(2,2) = (4,4)$ b/c $2 \cdot 4 - 2 \cdot 4 = 0$

$(2,2) = (1,4)$ b/c $2 \cdot 4 - 2 \cdot 1 = 8 - 2 = 6 \equiv 0$

$(2,2) = (5,2)$ b/c $2 \cdot 2 - 5 \cdot 2 = 4 - 10 = -6 \equiv 0$.

Thus $S^{-1}R = \{(0,2), (1,2), (2,2)\} \cong \mathbb{Z}_3$

Greenstein

2010.

Part A.

1. Let G be a group and let A be an abelian group. Let $\theta : G \to \mathrm{Aut}(A)$ be a group homomorphism. Let $X \times_\theta G$ be the set $A \times G$ with the binary operation

$$(a, g)(a', g') = (a + \theta(g)(a'), gg').$$

   (i) Prove that $A \times_\theta G$ is a group.

   (ii) Find $\theta : \mathbf{Z}_2 \to \mathrm{Aut}(\mathbf{Z}_m)$ such that the dihedral group D_m is isomorphic to $\mathbf{Z}_m \times_\theta \mathbf{Z}_2$. *Do not forget to prove the isomorphism!*

2. (i) Let G be a group of order np where p is a prime. Find a sufficient condition for a subgroup of order p to be normal.

   (ii) List all isomorphism classes of abelian groups of order 120.

   (iii) Is there a simple group of order 120?

   (iv) What is the maximal possible number of elements of order 5 in a group of order 120?

3. Let G be a group acting on a set X. We say that the action of G on X is transitive if for all $x, x' \in X$ there exists $g \in G$ such that $gx = x'$. Prove the following statements.

   (i) For all $x \in X$, $Gx = X$. In particular, $[G : \mathrm{Stab}_G\, x] = |X|$ and if $|G|$ is finite then $|X|$ divides $|G|$.

   (ii) The subgroups $\mathrm{Stab}_G\, x$ are conjugate for all $x \in X$.

   (iii) Suppose that $|X| = k$ and let $\pi : G \to S_k = \mathrm{Bij}(X)$ be the group of homomorphism given by the action. Then k divides $n = [G : \ker \pi]$ and n divides $k!$.

4. An element e in a ring R is said to be idempotent if $e^2 = e$. The center $Z(R)$ of a ring R is the set of all elements $x \in R$ such that $xr = rx$ for all $r \in R$. An element of $Z(R)$ is called central. Two central idempotents $f, g \in R$ are called orthogonal if $fg = 0$. Suppose that R is a unital ring.

   (i) if e is a central idempotent, then so is $1_R - e$, and e and $1_R - e$ are orthogonal.

   (ii) eR and $(1_R - e)R$ are ideals and $R = eR \times (1_R - e)R$.

   (iii) If $R_1, \ldots, R_n$ are rings with identity then the following statements are equivalent

      (a) $R \simeq R_1 \times \cdots \times R_n$

2009
Fall 2010

(b) R contains a set of orthogonal central idempotents $e_1, \ldots, e_n$ such that $e_1 + \cdots + e_n = 1_R$ and $e_i R \simeq R$, $1 \leqslant i \leqslant n$.

(c) $R = I_1 \times \cdots \times I_n$ where I_k is an ideal of R and $R_k \simeq I_k$.

5. An element a of a ring R is called nipotent if $a^n = 0$ for some positive integer n. A ring is said to be local if it contains a unique maximal ideal. Prove the following statements.

(i) The set of all nilpotent elements in a commutative ring R is an ideal.

(ii) A commutative unital ring R is local if and only if for all $x, y \in R$, $x + 1 = 1_R$ implies that x is a unit.

(iii) Suppose that R is a commutative unital ring with the following property: if $x \in R$ is not a unit then x is nilpotent. Then R is local.

(iv) Let $\mathbf{Z}[i] = \{x + yi : x, y \in \mathbf{Z}\}$, $i^2 = -1$. Clearly, $\mathbf{Z}$ identifies with a subring of $\mathbf{Z}[i]$. Find a prime ideal in $\mathbf{Z}[i]$ and an ideal I such that $I \cap \mathbf{Z}$ is prime but I is not prime.

2010 A 2 (iii)

Is there a simple group of order 120?

Pf:

ATC $\exists$ G group s.t. $|G| = 120$ and G is simple.

Since $120 = 2^3 \cdot 3 \cdot 5$ then by sylows 1st thm $\exists$ a sylow-5 subgroup of order 5.

divisors of 120: 1, 2, 3, 4, 5, 6, 8, 10, 120, 60, 40, 30, 24, 20, 15, 12

by sylows 3rd thm there are either 1 or 6 sylow-5 subgp ($K \equiv 1 \bmod 5$)

Since G is simple, there is more than 1 sylow-5 subgp (if not that one would be normal $\rightarrow\leftarrow$)

Thus $\exists$ 6 sylow-5 subgroups say $H_1, \dots, H_6$.

s.t. $|H_i| = 5 \quad \forall \quad i = \{1, 2, 3, 4, 5, 6\}$

Define a group action on H_i

$$\phi : G \times \{H_i\}_{i=1}^{6} \longrightarrow \{H_i\}_{i=1}^{6}$$

$$(g, H_j) \longrightarrow g H_j g^{-1} = H_K$$

So ϕ induces an $\hookrightarrow$ map from G to S_6

$$|GA_6| = \frac{|G||A_6|}{|G \cap A_6|}$$

note: $|G| = [G : G \cap A_6]$

$$\Rightarrow |GA_6| = [G : G \cap A_6] \cdot |A_6|$$

$$\Rightarrow |GA_6| = 360 \text{ or } 720$$

Since G is iso. to a subgroup of S_6

case i: $G \leq A_6$

$$[A_6 : G] = \frac{|A_6|}{|G|} = \frac{360}{120} = 3$$

Let $\psi : A_6 \times \{\sigma_i G\}_{i=1}^{3} \longrightarrow \{\sigma_i G\}_{i=1}^{3}$

$$(\tau, \sigma_i G) \longmapsto \tau \sigma_i G$$

ψ induces an 1-1 map (by simplicity of A_6) from A_6 to S_3 $\rightarrow\leftarrow$ (cardinality problem)

case ii: $G \nleq A_6$

$\Rightarrow |GA_6| = 720$ and $|A_6| = 360$

$$\Rightarrow [G : G \cap A_6] = \frac{|GA_6|}{|A_6|} = \frac{720}{360} = 2$$

$\Rightarrow G \cap A_6 \lhd G$ $\rightarrow\leftarrow$ since G is simple.

Thus a group of order 120 cannot be simple. //

Chang

2009.

Part A.

1. Let $D_8 = \langle a, b \rangle$ be the dihedral group of degree 8. What are the equivalent classes of D_8?

2. Let G be a group of order n. If $n > m!$ and G has m Sylow p-subgroups, then G is not simple.

3. Find all Sylow 3-subgroups of S_6.

4. Let $(P, \{\pi_i\})$ and $(Q, \{\psi_i\})$ be coproducts of the family $\{A_i : i \in I\}$ of objects of a category G. Prove that P and Q are equivalent.

5. Let $R = \mathbf{Z}_{96}$ and $S = \{2^i : i = 1, 2, \dots\}$.

   (a). Find $S^{-1}R$.

   (b). What are the ideals of $S^{-1}R$?

6. Find the center of the ring of all $n \times n$ matrices over $\mathbf{Z}_6$.

7. The ring $R = \{a + b\sqrt{2}i : a, b \in \mathbf{Z}\}$ is an Euclidean domain.

8. A UFD is integrally closed.

Fall 2008

2009 A3

Find all Sylow 3-subgroups of S_6.

Pf:

$|S_6| = 6! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 2^4 \cdot 3^2 \cdot 5 = 720$

by Sylows 1st thm $\exists$ sylow-3 subgroups of order 9

so 720,

divisors of 720 are

1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 30, 36, 40, 45, 48, 60, 72, 80, 90, 120, 144, 180, 240, 360, 720

By Sylows 3rd thm

possible subgroups must be of the form $3k+1$ or $k \equiv 1 \bmod 3$

possible k's are: 1, 4, 10, 16, 40,

So $\exists$ either 1, 4, 10, 16 or 40 sylow 3-subgroups

Consider

$H_1 = \langle (123), (456) \rangle$

$= \{e, (123), (132), (456), (465),$

$(123)(456), (132)(456), (123)(465), (132)(456)\}$

Since all sylow p subgroups are conjugate then we obtain

$H_2 = (14) H_1 (14) = \langle (423), (156) \rangle$

$H_3 = (15) H_1 (15)$

$H_4 = (16) H_1 (16)$

$H_5 = (24) H_1 (24)$

$H_6 = (25) H_1 (25)$

$H_7 = (26) H_1 (26)$

$H_8 = (34) H_1 (34)$

$H_9 = (35) H_1 (35)$

$H_{10} = (36) H_1 (36)$

So $\exists$ 10 sylow 3-subgroups of S_6.

Greenstein

2008.

Part A.

1. Let G be a group and let A be an abelian group. Let $\theta : G \to \mathrm{Aut}(A)$ be a group homomorphism. Let $A \times_\theta G$ be the set $A \times G$ with the binary operation

$$(a, g)(a', g') = (a + \theta(g)(a'), gg').$$

   (i) Prove that $A \times_\theta G$ is a group.

   (ii) Prove that the dihedral group D_m is isomorphic to $\mathbf{Z}_m \times_\theta \mathbf{Z}_2$ for some $\theta : \mathbf{Z}_2 \to \mathrm{Aut}(\mathbf{Z}_m)$.

2. Prove that a finite group of order $p^n q$, $n > 0$, where $p > q$ are primes is not simple.

3. Let G be a group of order 120.

   (i) List all isomorphism classes of abelian groups of order 120.

   (ii) Can G be simple?

   (iii) What is the maximal possible number of elements of order 5 in G?

   (iv) How many conjugacy classes are there in S_6?

4. Let $\mathbf{Z}[i] = \{x + yi : x, y \in \mathbf{Z}\}$, $i^2 = -1$. This is a unital ring and $\mathbf{Z}$ identifies with a subring of $\mathbf{Z}[i]$.

   (i) Is the ideal of $\mathbf{Z}[i]$ generated by 5 prime?

   (ii) Is $\mathbf{Z}[i]$ a domain? If so, describe its field of fractions.

   (iii) Choose a maximal ideal P in $\mathbf{Z}[i]$ and describe the localization of $\mathbf{Z}[i]$ at P.

5. (i) Give an example of a category in which a morphism between two objects is epic if and only if it is surjective.

   (ii) Give an example of a category $\mathcal{C}$ and of an epic morphism between two objects of $\mathcal{C}$ which is not surjective.

Fall 2007

2008 A5

1) In sets, epic iff surjective.

Recall – a morphism $f: X \to Y$ in a category $\mathcal{C}$ is epic if $\forall$ objects Z with morphisms $g, h: Y \to Z$ the equality $gf = hf \Rightarrow g = h$.

note: in $\mathcal{C}$ objects are sets morphisms functions

Pf:

($\Leftarrow$) assume $f: X \to Y$ and $Y = fX$.

Suppose a set Z is given along w/ functions $g, h: Y \to Z$ satisfying $gf = hf$.

For each $y \in Y$, $\exists\ x \in X$ s.t. $y = fx$. Now

$$gy = g(fx) = (gf)x = (hf)x = hy$$

since y was arbitrary it follows that $g = h$ //

($\Rightarrow$) assume f is epic and take $Z = Y$

the identity morphism $1_Y: Y \to Y$ is available.

and by virtue of setup we have the inclusion $i: fX \hookrightarrow Y$

Note that $\mathrm{Hom}_{set}(fX, Y) \subset \mathrm{Hom}_{set}(Y, Y)$

and $\forall\ x \in X$,

$$if: X \mapsto fx \hookrightarrow fx,$$

$$1_Y f: X \mapsto fx \mapsto fx.$$

Accordingly $if = 1_Y f$ and since f is epic $i = 1_Y$. In particular their domains coincide. //

2) Give a example of a category in which there is an epic, non-surjective morphism.

EX:

Take $\mathcal{C}$ = ring.

lemma: If R is a ring and $g, h : \mathbb{Q} \longrightarrow R$ satisfying $g|_{\mathbb{Z}} = h|_{\mathbb{Z}}$ then $g = h$.

Let $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ be inclusion

the lemma says $\forall R \in Ob(\mathcal{C})$ w/

$g, h : \mathbb{Q} \longrightarrow R$ $gi = hi \Rightarrow g = h$.

So i is epic and non-surjective. //

nonsurjective b/c not every $\mathbb{Q}$ is "hit" by $\mathbb{Z}$.

Rush

2007.

Part A.

1. If G is a group, a left G-module is an abelian group $(A,+)$ with a group action $\sigma : G \times A \to A$ such that if we denote $\sigma(g,a)$ by ga, we have $g(a+b) = ga + gb$ for all $g \in G$, $a, b \in A$. If A is a G-module, the *(external) semidirect product* $A \times_\theta G$ is the set $A \times G$ with the product defined by $(a,g)(b,h) = (a+gb, gh)$.

   (a) Show that $A \times_\theta G$ is a group.

   (b) Show that $S_3 \simeq \mathbf{Z}_3 \times_\theta \{1,-1\}$ for some G-module action $\sigma : \{1,-1\} \times \mathbf{Z}_3 \to \mathbf{Z}_3$.

2. Let R be a PID and define $\varphi : R\backslash\{0\} \to \mathbf{N}_0$ by $\varphi(a) = n$ if $a = up_1p_2\cdots p_n$ for a unit u and prime elements p_i of R. Consider the condition:

   $(*)$ for every $a_1, a_2 \in R$ there exists $d \in R$ such that $a_1R + a_2R = (a_1 + da_2)R$.

   (a) Show that if R satisfies the condition $(*)$, then R is a Euclidean domain with Euclidean function φ.

   (b) Show that $(*)$ implies $\mathcal{U}(R) \to \mathcal{U}(R/A)$ is onto for each ideal A of R, where $\mathcal{U}(T)$ denotes the group of units of the commutative ring T.

   (c) Show that $\mathbf{Z}$ does not satisfy $(*)$.

3. Let S_5 operate on itself by conjugation. How many orbits does S_5 have?

4. Let G be a finite group of order p^nq, p and q primes with $p > q$. Show that G is not simple.

5. Give examples of the following and explain how you know they have the properties claimed.

   (a) A Noetherian integral domain that is not a PID.

   (b) An integral domain R of characteristic zero having a non-maximal prime ideal P such that the characteristic of R/P is not zero.

Fall 2006

Chang

2006.

Part A.

1. Find all normal subgroups of D_{24}.

2. Find the Sylow 2-subgroups of S_5.

3. Let $H = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{Z}_{12} \right\}$ be a set of 3×3 matrices. Prove or disprove that H is a nilpotent group under ordinary matrix multiplication.

4. (i) Determine the units in $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\}$.
   (ii) Is 7 irreducible? Prove your answer.

5. Prove or disprove that the ring of Gaussian integers $\mathbf{Z}[i]$ is a PID.

Fall 2005

Chari

2005.

answer any 4 questions

Part A.

1. Consider the additive quotient group ~~$\mathbf{Q}/\mathbf{Z}$~~ $\mathbb{Q}/\mathbb{Z}$, where $\mathbf{Q}$ is the set of rational numbers and $\mathbf{Z}$ the set of integers.

   (a) Show that every coset contains exactly one element $q \in \mathbf{Q}$ with $0 \leqslant q \leqslant 1$.

   (b) Show that every element in $\mathbf{Q}/\mathbf{Z}$ has finite order but that there are elements of infinitely large order.

   (c) Consider now the group $\mathbf{R}/\mathbf{Z}$ where $\mathbf{R}$ is the set of real numbers. Prove that any element of finite order in $\mathbf{R}/\mathbf{Z}$ is in $\mathbf{Q}/\mathbf{Z}$.

2. (a) Exhibit two distinct Sylow 2 subgroups of S_5 and an element of S_5 that conjugates one into another.

   (b) How many elements of order 7 are there in a simple group of order 168.

3. (a) Prove that D_8 is not isomorphic to $D_4 \times \mathbf{Z}_2$.

   (b) Prove that if G is a group of order p^n, then it has a normal subgroup of order p^k for all $0 \leqslant k \leqslant n$.

4. Let F be a field and let R be the subset of $F[x]$ consisting of polynomials whose coefficient of x is 0. Prove that F is a subring of R. Prove also that R is not a UFD by showing that $x^6 \in R$ has two different factorizations in R into irreducibles.

5. Let R be a commutative ring. Assume that $R[x]$ is a principal ideal domain. Prove that (a) R is a domain, (b) the ideal (x) of $R[x]$ generated by x is prime, (c) explain why (x) is then maximal and (d) conclude finally that R must be a field.

   Hint: Recall the equivalent conditions for an ideal in a commutative ring to be prime (resp. maximal), and recall also the evaluation homomorphism ev_a for $a \in R$.

Fall 2004

2005 A1

consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

consider the congruence relationship $a \sim b$ iff $a-b \in \mathbb{Z}$

The set of equivalences classes with this relation is denoted by $\mathbb{Q}/\mathbb{Z}$. (addition $\bar{a}+\bar{b}=\overline{a+b}$)

a) show that every coset contains exactly one element $q \in \mathbb{Q}$ with $0 \le q < 1$.

ATC $p, q \in \bar{a}$ where $p \neq q$ & $0 \le p, q < 1$

and $p \sim q$

So $p-q \in \mathbb{Z} \Rightarrow p-q = n$, $n \in \mathbb{Z}$

but $0 < |p-q| < 1$

$\longrightarrow\!\!\!\!\!\!\times\longleftarrow$ b/c $p-q=n$ where $n \in \mathbb{Z}$. //

b) show that every elmt in $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elmts of infinitely large order

WLOG let $(p,q)=1$, $p, q \neq 0$.

Since $\underbrace{\frac{p}{q}+\frac{p}{q}+\cdots+\frac{p}{q}}_{q \text{ times}} = q \cdot \frac{p}{q} = p \in \mathbb{Z}$

$\Rightarrow \left|\frac{p}{q}\right| = q$. /

If q is infinitely large then $\left|\frac{p}{q}\right|$ is finitely large. //

2005 A1:

(c) consider now the group $\mathbb{R}/\mathbb{Z}$ where $\mathbb{R}$ is the set of real #. Prove that any elmt of finite order in $\mathbb{R}/\mathbb{Z}$ is in $\mathbb{Q}/\mathbb{Z}$.

Let $a \in \mathbb{R}$.

assume $a+\mathbb{Z}$ has finite order w/ $a \notin \mathbb{Z}$.

Let $|a+\mathbb{Z}| = n$. $\quad n \in \mathbb{Z} \setminus \{0\}$

So $n(a+\mathbb{Z}) = 0 + \mathbb{Z}$

$\Rightarrow na \in \mathbb{Z}$

$\Rightarrow na = m$ for $m \in \mathbb{Z}$

$\Rightarrow a = \frac{m}{n} \in \mathbb{Q}$ b/c $m, n \in \mathbb{Z}$

thus $a + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. //

2005 A2:

(a) Exhibit two distinct Sylow 2 subgrps of S_5 and an elmt of S_5 that conjugates one into another.

Well $|S_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$

By 1st sylow thm $\exists$ sylow-2 subgrp of order 8.

Take $H_1 = \{ e, (12), (34), (12)(34), (1423), (1324), (14)(23), (13)(24) \}$

(12), (34): pick disjoint; (12)(34): put together; (1423): out-out in-in; (1324): inverse; (14)(23), (13)(24): split

$H_2 = \{ e, (13), (24), (13)(24), (1432), (1234), (14)(32), (12)(34) \}$

take $\sigma \in S_5$ to be a 2-cycle which is the swap between the disjoints

(12), (34)

↓ ↓

(13), (24)

$2 \leftrightarrow 3 \Rightarrow (23)$

Consider, $(23) \in S_5$

claim: $(23) H_1 (23)^{-1} = H_2$.

OR $(23) H_1 (23) = H_2$

Check:

$(23)(12)(23) = (23)(123) = (13)$ ✓

$(23)(34)(23) = (23)(243) = (24)$ ✓

$(23)(12)(34)(23) = (23)(12)(243) = (23)(1243) = (13)(24)$ ✓

$(23)(1423)(23) = (23)(142) = (1432)$ ✓

$(23)(1324)(23) = (23)(134) = (1234)$ ✓

$(23)(14)(23)(23) = (23)(14) = (14)(23)$ ✓

$(23)(13)(24)(23) = (23)(13)(234) = (23)(1342) = (12)(34)$ ✓

//

(b) How many elmt of order 7 are there in a simple group of order 168.

Pf:

$|G| = 168 = 2^3 \cdot 3 \cdot 7$

So by 1st sylow thm, $\exists$ a sylow-7 subgroup of order 7.

divisors of 168: 1, 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56, 84, 168.

Lets determine the possible # of sylow 7-subgroups.

for $p=7$ we kneed $7k+1$ or $k \equiv 1 \bmod 7$.

choices for k are 1, 8.

since we assumed G is simple then $\nexists$ normal subgroups, thus $k \neq 1$ because if it did then we would have only 1 sylow-7 subgroup which would be normal $\rightarrow\leftarrow$.

thus $k = 8$.

so let $H_1, \dots, H_8$ be sylow-7 subgrp

since $|H_i| = 7 \Rightarrow H_i \cong \mathbb{Z}_7$.

$\Rightarrow H_i \cap H_j = \{e\}$ when $i \neq j$

So we have $8(7-1) = 8 \cdot 6 = 48$ (non-identity) elmts of order 7.

//

2005 A3

(a) Prove $D_8 \not\cong D_4 \times \mathbb{Z}_2$

Pf:

Recall - for $n \geq 3$, D_n is a group of order $2n$ whose generators satisfy $a^n = e$, $b^2 = e$, $a^k \neq e$ if $0 < k < n$. and $ba = a^{-1}b$.

Let $H = \langle a \rangle$, so $H < D_8$

since $a^8 = e$ & $a^k \neq e$ for $0 < k < n$

then $|a| = 8 = |\langle a \rangle| = |H|$

so D_8 has a cyclic subgrp of order 8 $\Rightarrow$ it has an elmt of order 8.

NTS: all elmts in $D_4 \times \mathbb{Z}_2$ has order ≤ 4

well elmts in order $D_4 \times \mathbb{Z}_2$ are of the form either (a^i, x) w/ $0 \leq i \leq 3$ or $(a^i b, x)$ w/ $0 \leq i \leq 3$ & $x \in \mathbb{Z}_2$.

Take $(a^i, x) \in D_4 \times \mathbb{Z}_2$

well $(a^i, x)^4 = (a^{4i}, 4x) = (0, 0) = id$.

so $|(a^i, x)| \leq 4$.

Take $(a^i b, x)^4 \in D_4 \times \mathbb{Z}_2$

well $(a^i b, x)^4 = (b^4, 4x) = (0, 0) = id$

so $|(a^i b, x)| \leq 4$ so $\nexists$ an elmt of order 8 $\Rightarrow D_8 \not\cong D_4 \times \mathbb{Z}_2$

Note:
$a^i b a^i b$
$= a^i a^{-i} b b = b^2 = e$

(6)

(b) Prove that if G is a group of order p^n, then it has a normal subgroup of order p^k $\forall\ 0 \le k \le n$.

Pf: induct on n.

Base case: $n=0$, $|G| = p^0 = 1$. done.

assume statement holds for $n-1$.

Let $|G| = p^n$. as a p-group, G has a non-trivial center.

By Lagranges thm $|Z(G)| \mid p^n$ (so $p^n = |Z(G)|a'$)

In particular $p \mid |Z(G)|$ (so $|Z(G)| = p \cdot b'$)

Cauchy thm says that b/c $p \mid |Z(G)|$

then $\exists$ an elmt $a \in Z(G)$ s.t. $|a| = p$.

thus $\langle a \rangle \le Z(G)$ & $|\langle a \rangle| = p$.

By Lagranges thm the group $G/\langle a \rangle$ has order p^{n-1}.

the induction hypothesis gives normal subgroups $N_i \trianglelefteq G/\langle a \rangle$ of order p^i for each $i = 0, \dots, n-1$

$\Rightarrow \exists$ normal subgroups K_i of G, containing $\langle a \rangle$ for each i. So by Lagranges thm

$$|K_i| = p^{i+1}.$$

thus the result follows //

2005 A4:

Let F be a field and R be the subset of $F[x]$ consisting of polynomials whose coefficients of x is 0. Prove F is a subring of R.

Consider $i: F \to R$
$a \longmapsto a + 0x + 0x^2 + \dots$
which is a monomorphism of rings.

Since i is a ring homom,
then $\operatorname{Im} i$ is a subring of R

By construction $\operatorname{Im} i = F$
$\Rightarrow F$ is a subring of R. //

Prove also that R is not a UFD by showing that $x^6 \in R$ has two different factorizations in R into irreducible.

Consider $x^6 \in R$. Note $x^2 \cdot x^2 \cdot x^2 = x^6 = x^3 \cdot x^3$.

Claim: x^3 is irred.
atc it is reducible then $x^3 = x^i x^j$ where $i+j=3$ $(i,j \in \mathbb{N})$
if i or j is zero then that term is a unit
if i or j is one then that term is just x
$\to\leftarrow$ since $x \notin R$
thus x^3 is irred.

Claim: x^2 is irred.
atc it is reducible then $x^2 = x^i x^j$ where $i+j=2$ $(i,j \in \mathbb{N})$
if i or j is zero then that term is a unit.
if i or j is one then that term is just x
$\to\leftarrow$ since $x \notin R$.
thus x^2 is irred.

thus $x^2 \cdot x^2 \cdot x^2 = x^6 = x^3 \cdot x^3$ (*) //

(*) are two different factors of irreducibles of x^6 in R $\therefore R$ is not a UFD

2005 A5:

Let R be a commutative rng. Let $R[x]$ be a PID.

a) Prove R is a domain.

Consider $i: R \longrightarrow R[x]$

$r \longmapsto r + 0x + 0x^2 + \cdots$

Note that i is a rng monomorphism.

Since i is a rng homom, then $\operatorname{Im} i$ is a subrng of $R[x]$

By construction $\operatorname{Im} i \cong R$

a subrng of a domain is a domain $\Rightarrow$ R is a domain //

b) Prove that the ideal (x) of $R[x]$ generated by x is prime.

Let $f, g \in R[x]$ and $fg \in (x)$. NTS $f \in (x)$ or $g \in (x)$.

Note $(x) = \{hx \mid h \in R[x]\} = \left\{ \sum_{i=1}^{n} a_i x^i \mid a_i \in R \right\}$.

Let $f = \sum_{j=0}^{m} b_j x^j$ and $g = \sum_{k=0}^{p} c_k x^k$ and $fg = \sum_{e=0}^{q} d_e x^e$

Observe that $d_0 = b_0 c_0$

Since $fg \in (x)$ then $b_0 c_0 = 0$

By part (a) $\Rightarrow$ b_0 or $c_0 = 0$

$\Rightarrow$ f or g is an elmt of (x).

Thus (x) is prime. //

c) ~~Suppose I is an ideal of R[x] s.t. $(x) \subsetneq I$~~

Explain why (x) is then maximal.

Pf:

Suppose I is an ideal of $R[x]$ s.t. $(x) \subsetneq I$

Since $R[x]$ is a PID, $\exists\, h \in R[x]$ s.t. $I = (h)$.

$\Rightarrow (x) \subsetneq (h)$

So $x = h \cdot g$ where $g \in R[x]$

so $h \mid x$

but (x) is prime iff x is prime.

In a PID, prime iff irreducible.

$\Rightarrow x$ is irreducible.

$\Rightarrow (x)$ is maximal in the set of proper principal ideals of $R[x]$

but all ideals are principal in $R[x]$.

Thus (x) is maximal in $R[x]$. //

d) Conclude that R must be a field.

Pf:
We know $R[X]/(X)$ is a field iff (X) is maximal.

Consider $\phi: R \longrightarrow R[X]/(X)$

$a \longmapsto a+(X)$

Well-defined. Let $a=b$,

so $\phi(a) = a+(X)$ & $\phi(b) = b+(X)$

Since $a=b \Rightarrow a+(X) = b+(X)$

so $\phi(a) = \phi(b)$.

so ϕ well-defined.

Let $a, b \in R$.

$$\text{So } \phi(a+b) = (a+b)+(X) = (a+(X)) + (b+(X))$$
$$= \phi(a) + \phi(b)$$

$$\phi(ab) = ab+(X) = (a+(X))(b+(X))$$
$$= \phi(a)\phi(b)$$

so ϕ is homom.

Let $\phi(a) = \phi(b)$

$\Rightarrow a+(X) = b+(X)$

$\Rightarrow (a-b)+(X) = 0+(X) \Rightarrow a-b \in (X)$

$\Rightarrow a-b = 0 \Rightarrow a=b$. so ϕ 1-1.

Let $a+(X) \in R[X]/(X)$

choose $a \in R$, s.t. $\phi(a) = a+(X)$

thus ϕ is surjective.

thus ϕ is an isomorphism. //

Rush

2004 (October).

Part A.

1. Let R be a UFD in which each nonzero prime ideal is maximal. Show that
   (a) if $a, b \in R$ and $(a, b) = 1$, then $ax + by = 1$ for some $x, y \in R$.
   (b) Show that each ideal of R that is generated by two elements is principal.

2. (a) Let G be a finite group and H a normal subgroup of G. Show that if H and G/H are solvable, then G is solvable also.
   (b) Show that if H and K are solvable normal subgroups of G with $HK = G$ and $H \cap K = \{e\}$, then G is solvable.

3. Let S be a multiplicative subset of the commutative ring R and let I be an ideal of R. Show that $S^{-1}\,\mathrm{Rad}(I) = \mathrm{Rad}(S^{-1}I)$, where $\mathrm{Rad}(J) = \{x \in R : x^n \in J \text{ for some positive integer } n\}$.

4. Let p be a prime integer and let G be a finite p-group. Show that G has a nonzero center.

5. Let G be a finite simple group having a subgroup H of index n. Show that G is isomorphic to a subgroup of S_n.

Fall 2003

2004 (Oct) A5

Let G be a finite simple group having a subgroup H of index n. Show that G is $\simeq$ to a subgp of S_n.

Pf:

Let G be simple and $[G:H]=n$.

Consider, $\phi : G \times gH \longrightarrow g'H$

$(g'', gH) \longmapsto g''gH$

which is a well-defined group action.

ϕ induces a map

$\psi : G \longrightarrow S_n$

since G is simple, $\ker \phi = \{e\}$

$\Rightarrow \psi$ injective

Thus there is an isomorphism between G and $\psi(G) \leq S_n$. //

2004 (April).

Part A.

1. Let $G = \mathbf{Q}/\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{Z}$ being considered as additive groups. Prove that for any positive integer n, G has a unique subgroup $G(n)$ of order n, and that $G(n)$ is cyclic.

2. Let G be a group. Prove that if the group of automorphisms $\mathrm{Aut}(G)$ of G is cyclic, then G is abelian.

3. Let G be a finite group and $H \lhd G$ a normal subgroup of prime order p. Prove that H is contained in each Sylow p-subgroup of G.

4. Let $H < G$ be a proper subgroup of finite index in a group G. Prove that G does not equal the union of all subgroups of G conjugate to H.

5. Prove that a group of order 40 has a normal Sylow subgroup.

6. Let G be a finite group. Describe all group homomorphisms $\varphi : G \to F_2$, where F_2 denotes the free group on two elements.

2004 A 2 (Apr)

Let G be a group. Prove that if $\mathrm{Aut}\, G$ is cyclic, then G is abelian.

Pf:

Let $\mathrm{Inn}\, G < \mathrm{Aut}\, G$ be the subgroup of all inner automorphisms of G. By assumption $\mathrm{Inn}\, G$ is cyclic.

Consider the natural homom,

$\tau : G \longrightarrow \mathrm{Inn}\, G$ given by

$g \longmapsto (x \mapsto gxg^{-1})$.

Need to show $\ker \tau = Z(G)$.

Let $a \in \ker \tau$.

So $\tau(a) = id_G$

So for every $g \in G$, $g = aga^{-1}$.

Thus $ga = ag$. So $a \in Z(G)$ (b/c it commutes w/ any $g \in G$).

So $\ker \tau \subset Z(G)$.

Let $b \in Z(G)$.

Then for every $g \in G$, $gb = bg$.

Thus $g = bgb^{-1}$

So $\tau(b) = id_G$ and $b \in \ker \tau$.

So $Z(G) \subset \ker \tau$.

Thus $\ker \tau = Z(G)$.

So $G/Z(G) \cong \mathrm{Inn}\, G$ by the first isomorphism Thm

So $G/Z(G)$ is cyclic.

By $G/Z(G)$ Thm G is abelian. //

Penkov, Ivan

2003.

Part A.

1. Prove that a group cannot be the union of two proper subgroups.

2. Let $\mathbf{Q}$ be the additive group of rational numbers. Prove that any subgroup of $\mathbf{Q}$ generated by two distinct elements is isomorphic to $\mathbf{Z}$. Use this to prove that $\mathbf{Q}$ is not isomorphic to $\mathbf{Q} \times \mathbf{Q}$.

3. Let G_1 and G_2 be two non-trivial non-isomorphic simple groups. Prove that any proper non-trivial normal subgroup of $G_1 \times G_2$ coincides with G_1 or G_2.

4. Prove that a free group that is abelian is either trivial or is isomorphic to $\mathbf{Z}$.

5. Describe up to isomorphism all groups of order 121. Prove your answer.

6. Prove that if S is a Sylow subgroup of a finite group G, then $N_G(N_G(S)) = N_G(S)$.

Fall 2002

2003 A1

Prove that a group cannot be the union of two proper subgroups.

Pf:

atc $A, B \subsetneq G$ and $G = A \cup B$.

so $\exists$ $a \in A$ s.t. $a \notin B$ since $(a \neq e)$

$A \cup B = G$ and $B \neq G$

likewise $\exists$ $b \in B$ s.t. $b \notin A$ $(b \neq e)$

since $b \notin A$, $ab \notin A$

(if it were $ab \in A \Rightarrow a^{-1}ab = b \in A \rightarrow\leftarrow$)

likewise $ab \notin B$ since $a \notin B$.

$\Rightarrow ab \notin G$ since $ab \notin A$ and $ab \notin B$

$\rightarrow\leftarrow$ since $A, B \subsetneq G$ & $a, b \in G$ then $ab \in G$.

Thus G is not the union of two proper subgroups. //

2003 A5

Describe up to isomorphism all groups of order 121.

Pf:

Well, $121 = 11^2$ and we know that every group of order p^2, with p prime is abelian.

Thus any group of order 121 is abelian.

By the fundamental theorem of finite abelian groups any group of order 121 is isomorphic to either $\mathbb{Z}_{121}$ or $\mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$.

//

Rush

2002

Part A.

1. Show that if a positive integer d divides the order n of a finite cyclic group G, then G has a unique subgroup of order d.

2. Show that there are no simple groups of order 200.

3. Let H be a subgroup of a group G with $(G : H) = n$.

   (a) Show H contains a normal K such that $(G : K)$ divides $n!$.

   (b) Show that if G is finite and $n = p$ is the smallest prime dividing $|G|$, then H is normal.

4. Show that each finite p-group is solvable.

5. Show that in a principal ideal domain every non-zero prime ideal is maximal.

6. Let R be a commutative unitary ring. An ideal I of R is said to be *primary* if $a, b \in R$ and $ab \in I$ imply $a \in I$ or $b^n \in I$ for some $n \in \mathbf{N}$. Assume that I is primary and S is a multiplicative subset of R such that $S \cap I = \varnothing$. Show that $S^{-1}I$ is a primary ideal of $S^{-1}R$.

Fall 2001

2002 A 3:

Let G be a group. ← think cosets

1) If $H < G$ and $[G:H] = n$, then $\exists$ $K < H$ s.t.
   a) $K \triangleleft G$
   b) $[G:K]$ divides $n!$ ← think $|S_n|$

2) If $|G| < \infty$ and $n = p$ is the minimal prime divisor of $|G|$, then $H \triangleleft G$.

Pf:

1) G acts on the set $G/H = \{g_1H, \ldots, g_nH\}$ by left multiplication meaning $\exists$ a function

$$G \times G/H \xrightarrow{\alpha} G/H \quad \text{s.t.}$$

$$g \cdot (g' \cdot (aH)) = (gg') \cdot aH \qquad \text{OR}$$

$$\begin{array}{ccc} G \times G \times G/H & \xrightarrow{1_G \times \alpha} & G \times G/H \\ \downarrow{\scriptstyle \text{mult} \times 1_{G/H}} & & \downarrow{\scriptstyle \alpha} \\ G \times G/H & \xrightarrow[\alpha]{} & G/H \end{array} \qquad \text{commutes}$$

observe that for all $g \in G$ and each $i \in \{1, \ldots, n\}$

$g \cdot g_iH = g_jH$ for a unique $j = j(g,i) \in \{1, \ldots, n\}$.

Define $\phi: G \longrightarrow S_n$ by $g \longmapsto (i \longmapsto j(g,i))$

τ_g so $\tau_g(i) = j$ when $g(a_iH) = a_jH$

Verify ϕ is a group homom:

NTS $\tau_{gg'} = \tau_g \tau_{g'}$

Let $\tau_{gg'}(i) = j$ where $gg'(a_iH) = a_jH$ and

$\tau_g \tau_{g'}(i) = K$ where $g \cdot (g' \cdot (a_iH)) = a_kH$

But $g \cdot (g' \cdot (a_i H)) = (gg') \cdot a_i H$
b/c group action axiom.

Thus $a_k H = a_j H$

$\Rightarrow j = k$.

So ϕ is a homom.

Consider $K = \ker \phi$

Note $K \trianglelefteq G$.

Applying the 1st iso thm, we get.

$$G \longrightarrow S_n$$
$$G/K$$

i.e. $|G/K| \mid |S_n|$

b/c $G/K \cong \operatorname{Im} G$, so $G/K < S_n$.

Claim: $K < H$.

Let $g \in \ker \phi = K$
$\Rightarrow$ for the coset H that $gH = H$ iff $g \in H$.

So $K < H$.

Note: $|G/K| = [G:K]$ and $|S_n| = n!$.

Thus $[G:K] \mid |S_n|$.

Thus (a) & (b) hold. //

2) Let K be as before. So $K < H < G$

Let $m = [H:K]$

Recall, $[G:K] = [G:H][H:K] = pm$

From part (1) we know $pm \mid p!$.

so $m \mid (p-1)!$

Thus all prime divisors of m are less than p.

Note: all prime divisors of m are greater than or equal to p, b/c $m \mid |G|$ and p is the minimal prime divisors of $|G|$.

Thus $m = 1$.

Therefore $H = K$ & $K \trianglelefteq G$ (from 1).

Thus $H \trianglelefteq G$.

//

Penkov, Ivan

2001

Part A.

1. Show that the symmetric group S_3 is not isomorphic to a direct product of two of its proper subgroups.

2. Show that a group of order 77 has exactly one subgroup of order 11.

3. Prove that if G is a group and $G/C(G)$ is cyclic, then G is abelian, where $C(G)$ is the center of G.

4. Describe explicitly all free groups which are abelian.

5. Prove that if H is a cyclic normal subgroup of G, then every subgroup of H is normal in G.

6. How many elements of order 7 are there in a simple group of order 168? Prove your answer.

Fall 2000

2001 A3:

If G is a group and $G/Z(G)$ is cyclic, then G is abelian.

Pf:

First note that $Z(G) \trianglelefteq G$

Select $a \in G$ s.t. $aZ(G)$ generates $G/Z(G)$

Remark: $gZ(G) \cdot hZ(G) = (gh)Z(G)$.

Thus $G/Z(G) = \langle aZ(G) \rangle = \{a^i Z(G) \mid i \in \mathbb{Z}\}$

Let $g, h \in G$

So $\exists\ m, n \in \mathbb{Z}$ s.t. $gZ(G) = a^m Z(G)$

and $hZ(G) = a^n Z(G)$.

Thus $g = a^m z$ and $h = a^n z'$ for $z, z' \in Z(G)$.

So $gh = a^m z\, a^n z' = a^m a^n z z' = a^{m+n} zz'$

($z \in Z(G)$)

$= a^{n+m} zz' = a^n a^m zz' = a^n a^m z'z = a^n z' a^m z = hg$

($z' \in Z(G)$ for the second equality; $z' \in Z(G)$ for the third)

Thus $gh = hg$ and therefore G is abelian.

//

Note:

The G/Z Thm nearly trivializes

1995 A5, 2004 A2, 2003 A5, 1994 A4,

2000 A4, . . .

2000

Part A.

1. (a) Find all subgroups of $\mathbf{Z}_{48}$
   (b) Find all ideals of the ring $\mathbf{Z}_{48}$
   (c) Which ideals in (b) are maximal? Which are prime?

2. Find all normal subgroups of D_{11}.

Prove or disprove the following:

3. A group of order 375 is simple.

4. There is a non-abelian group G such that $|G| = 125$ and $|C(G)| = 25$.

5. $\mathbf{R}[X, Y]$ is a PID, but $\mathbf{Z}[X]$ is not a PID (x, y are indeterminates).

6. $\mathbf{Z}[i]$ is a UFD.

7. Let p be a fixed prime number. Let $R = \{a/b : a, b \in \mathbf{Z}, p \nmid b\}$. Then R is a local ring.

Fall 1999

2000 A4

T/F. ∃ a non-abelian group of order 125 whose center has order 25.

False:

Let G be a group of order 125 and $|C(G)| = 25$

Well, $|G/C(G)| = |G|/|C(G)| = 125/25 = 5$

Thus $|G/C(G)| = 5$ so $G/C(G)$ is cyclic.

Thus G is abelian. //

1999

Parts A and B.

1. Let $K \subseteq H$ be subgroups of the finite group G, which are not necessarily normal. Show $(G : K) = (G : H)(H : K)$, where the notation $(A : B)$ denotes the number of left cosets of B in A.

2. Let the group G operate on the set S, and suppose that $s, t \in S$ are in the same orbit under the operation. Show that the isotropy groups G_s and G_t are conjugate. That is, there exists $g \in G$ such that $g^{-1}G_s g = G_t$. (Recall that $G_s = \{x \in G : gs = s\}$).

3. Show that each group of order p^2, p prime, is abelian.

4. (a) Define *free group* $F(X)$ *on a set* X.
   (b) Define *coproduct* $(G, \{\varphi_i\}_{i \in I})$ *of a family* $\{G_i : i \in I\}$ of groups.
   (c) Show that if $(G, \varphi_1, \varphi_2)$ is a coproduct of G_1 and G_2 with G_i isomorphic to the additive group of integers Z, then $G \simeq F(\{a, b\})$.
   (d) Is $F(\{a, b\})$ abelian?

5. Show that the direct sum of an arbitrary family of injective abelian groups is injective. (Hint: Divisible).

6. (a) Determine the units in $\mathrm{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathrm{Z}\}$.
   (b) Show that $1 + \sqrt{-5}$ and 2 are irreducible in $\mathrm{Z}[\sqrt{-5}]$.

7. (a) Give an example of an integral domain R and ideals I and J of R such that $IJ \neq I \cap J$.
   (b) Show that if $I + J = R$ then $IJ = I \cap J$.

8. Give an example of a monomorphism $f : A \to B$ of abelian groups and an abelian group C such that the induced homomorphism $\hom_{\mathrm{Z}}(B, C) \to \hom_{\mathrm{Z}}(A, C)$ is not onto.

Fall/Winter 1998/1999

9. Show that if R is a PID and $M = R/a_1R \oplus R/a_2R \oplus \cdots \oplus R/a_mR$, with $R \neq a_1R \supseteq a_2R \supseteq \cdots \supseteq a_mR$, then M cannot be generated by fewer than m-elements.

10. Let

$$A = \begin{pmatrix} 2 & & & & & & & \\ & -1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & 1 & 1 & & & \\ & & & & & -1 & & \\ & & & & & & 2 & \\ & & & & & & & -1 \end{pmatrix}.$$

Find the minimal polynomial and the rational canonical form of A.

Fall/ Winter 1998/1999

1998

Part A.

1. (a) Find all subgroups of $\mathbf{Z}_{24}$.
   (b) Find all the ideals in the ring $\mathbf{Z}_{24}$.
   (c) Which of these ideals are maximal and which are prime?

In problems 2-5a, prove or disprove.

2. If $(P, \{\pi_i\})$ and $(Q, \{\psi_i\})$ are both products of the family $\{A_i : i \in I\}$ of objects of a category G, then P and Q are equivalent.

3. A group of order 250 is simple.

4. Let R be an integral domain. Then R is Euclidean iff R is a PID iff R is a UFD.

5. (a) Let $R = \mathbf{Z}_6$, $S_1 = \{1, 3\}$, and $S_2 = \{1, 2, 4\}$. Then $S_i^{-1}R$ is a field.
   (b) How many elements does $S_i^{-1}R$ have?

Fall 1997

1997

Part A.

1. Let $|G| = p^n$. Prove that for each $0 \leqslant k \leqslant n$, G has a normal subgroup of order p^k.

2. Let G be a group containing an element of order different from 1 or 2. Prove that G has a non-identity automorphism.

3. Prove that a commutative ring with identity is local iff for all $r, s \in R$, $r + s = 1_R$ implies r or s is a unit.

4. Prove that $\mathbb{Z}[x]$ is not a principal ideal domain.

5. Prove that in the ring $\mathbb{Z}$ the following conditions are equivalent

   a. I is prime.

   b. I is maximal.

   c. $I = (p)$ with p prime.

6.

Fall 1996

1996

Part A.

1. Let F be a field. Prove that F contains a unique smallest subfield F_0 and that F_0 is isomorphic to either $\mathbf{Q}$ or to $\mathbf{Z}_p$ for some prime p.

2. Let R be a commutative ring with identity. Prove that a polynomial ring in more than one variable is not a principal ideal domain.

3. Let P be a prime ideal in a commutative ring with 1 and let D be the set $R \backslash P$. Show that the ring of fractions $D^{-1}R$ is defined and that it has a unique maximal ideal.

4. Let $\varphi : R \to S$ be a homomorphism of rings. Prove that the inverse image in R of a prime ideal in S is either R or a prime ideal.

5. Let A and B be finite groups. Prove that the number of Sylow-p subgroups in $A \times B$ is the product of the number of Sylow-p subgroups in A and B.

6. Let G be a cyclic group of order n and assume that k is prime to n. Prove that the map $x \mapsto x^k$ is surjective. Now prove that the same result holds for any finite group G of order n and for k prime to n.

7. Let C be a normal subgroup of A and D a normal subgroup of B. Prove that $C \times D$ is a normal subgroup of $A \times B$ and that the corresponding quotient group is isomorphic to $A/C \times B/D$.

Fall 1995

M-201C

2) Give an example of a field of char $p>0$ that is perfect and one that is not perfect. Justify.

Def a field K is perfect if $K^p = K$.

Perfect:
any finite field is perfect

- Pf: Let F be finite.
  Let $\phi: F \to F$ be defined by $\phi(x) = x^p$.
  We will show ϕ an automorphism (of fields)
  Let $a, b \in F$.
  Well $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$.
  $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$ blc char $= p > 0$ & freshmans dream.
  Since $x^p \neq 0$ when $x \neq 0$ then $\ker \phi = \{0\}$.
  So ϕ is injective.
  Since F is finite and ϕ injective then ϕ is surjective.
  Thus ϕ an automorphism. Therefore $F = F^p$.
  Hence F is perfect //

specific ex: take $F = \mathbb{Z}_2$, $\mathbb{Z}_2$ finite $\Rightarrow$ $\mathbb{Z}_2$ perfect.

Not Perfect: Let F_p be a field of char p and let t be the transcendentals in F_p.

Claim: $F = F_p(t)$ is not perfect.

Pf: aTC $F = F_p(t)$ is perfect.
Let E be the splitting field of $f(x) = \text{irr}(\alpha, F, x) = x^p - t$.

$\Rightarrow f(\alpha) = \alpha^p - t = 0 \Rightarrow \alpha^p = t$.

$\Rightarrow f(x) = x^p - t = x^p - \alpha^p = (x-\alpha)^p$ $\rightarrow\leftarrow$

blc this irred. poly. is not sep

thus $F = F_p(t)$ is not perfect. //

M-201C

3) Let $k \subseteq F \subseteq E$ be a tower of fields with E/k normal.

(a) Show E/F is normal.

Pf

Let E/k be normal.

Observe that if $\sigma: E \to \overline{F}$ is an F-embedding then σ is a k-embedding as well b/c $k \subseteq F$ so $\overline{F} = \overline{k}$ so $\sigma: E \to \overline{k}$

Since E/k is normal then $\sigma(E) = E$

$\Rightarrow$ E/F is normal as well. //

Def an ext K of k is said to be normal if K/k is alg and $K \subseteq \overline{k}$

Then:

1) Every k-embedding $\sigma: K \to \overline{k}$ is an automorphism of K that is $\sigma K = K$
2) K is the splitting field of a family $\{f_i\}_{i \in I} \subseteq k[x]$
3) Every irred. $f \in k[x] \setminus k$ which has a root in K splits into linear factors in K.

E | $*$ | F | $*$ | k — normal $\Rightarrow$ $*$ nor.

(b) Show that F/k may not be normal

Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq K$ w/ K = splitting field of $x^3 - 2$

Well, $K/\mathbb{Q}$ is normal by how we defined K.

NTS $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

Well $x^3 - 2 \in \mathbb{Q}[x]$ and has a root in $\mathbb{Q}(\sqrt[3]{2})$ & is irred.

but does not split in $\mathbb{Q}(\sqrt[3]{2})$ (b/c other 2 roots are complex)

Thus it cannot be normal.

//

M-201C

4) Let F_2 be the field with 2 elmts.

a) Are the rings $F_2[x]/(x^3+x+1)$ and $F_2[x]/(x^3+x^2+1)$ fields? Explain.

If $p(x)$ is monic irred poly, then $(p(x))$ is prime ideal.
since $p(x)$ is a prime ideal in a PID then it is max.
Thus $F_2[x]/(p(x))$ is a field.

so it suffices to show x^3+x+1 and x^3+x^2+1 are irreducible in $F_2[x]$.
We will show they do not have linear factors & hence no quadratic factors

Take $x=0$,
$0^3+0+1=1$ and $0^3+0^2+1=1$
$\Rightarrow$ 0 is not a root of either

Take $x=1$,
$1^3+1+1=1$ and $1^3+1^2+1=1$
$\Rightarrow$ 1 is not a root of either.

Thus x^3+x+1 and x^3+x^2+1 have no linear factors
Thus they are irreducible.
Hence $F_2[x]/(x^3+x+1)$ and $F_2[x]/(x^3+x^2+1)$ are fields. //

b) are they isomorphic? Explain.

Since they are both fields and since the irred. poly have the same degrees, then the dim of the extension will be the same, which implies there is an isomaphism between the fields.

M-201C

5) Factor $X^8 - X = X^{2^3} - X$ into a product of monic irred. elmts in $F_2[X]$.

Well,

$$X^8 - X = X^8 + X \text{ in } F_2[X]$$

So $X^8 - X = X(X^7+1)$

$= X(X+1)(X^6+X^5+X^4+X^3+X^2+X+1)$

$= X(X+1)(X^3+X+1)(X^3+X^2+1)$.

(all b/c in $F_2[X]$ so $2 \equiv 0$.)

474
84

Kayla Murray

Math 201C Final

June 13, 2013

Do 7 out of the 8 problems. Indicate which of the 8 that I am not to grade.

1. Let E/K be an algebraic extension and let $\phi : E \to E$ be a K-embedding of E into itself. Show that ϕ is an automorphism of E.

2. Determine the Galois group of $X^3 + 9X + 3$ over the rationals $\mathbb{Q}$.

3. Show that the class of separable extensions is a distinguished class of extensions. Do not grade

4. Let K be a field with $\mathrm{char}(K) = p \neq 0$ and let F be an algebraic extension field of K. Show that if $u \in F$ is separable of K, then $K(u) = K(u^{p^n})$ for all $n \geq 1$.

5. Show that for each prime integer p and each positive integer n there exists an irreducible polynomial $f \in \mathbb{Z}/p\mathbb{Z}[X]$ of degree n.

6. Prove or disprove that each finite extension field K of $\mathbb{Q}$ is a subfield of a cyclotomic extension of $\mathbb{Q}$.

7. (a) Define the norm N_K^E of a finite extension E/K of fields.

(b) State Hilbert's Theorem 90.

(c) What did we use Hilbert's Theorem 90 for?

8. (a) Factor the polynomial $X^9 - 1$ over $\mathbb{Q}$.

(b) Is $X^6 + X^3 + 1$ irreducible over $\mathbb{Q}$? Explain.

(c) Give the Galois group of $X^6 + X^3 + 1$ over $\mathbb{Q}$? Explain.

see 2005 qual

F-201C

1) Let E/K be an alg. ext and let $\phi : E \to E$ be a K-embedding of E into itself. Show ϕ is an automorphism of E.

Pf:

Since embeddings are injective, it suffices to show ϕ is surjective.

Let $\alpha \in E$, let $p(X) = \text{irr}(\alpha, K, X)$

Let E' be the subfield of E generated by all the roots of $p(X)$ which lie in E.

($\exists$ at least one generator since $\alpha \in E$ is a root)

$\Rightarrow \sigma E' \subseteq E'$ (since a root of $p(X)$ is mapped to a root of $p(X)$)

Note that $[E' : K]$ is finite since E' is finitely generated and hence a finite ext of K.

Since ϕ is 1-1, $\sigma E'$ is a subspace of E' having the same dim as $[E' : K]$

$\Rightarrow \phi E' = E'$

Since $\alpha \in E' \Rightarrow \alpha$ is in the image of ϕ

thus ϕ is surjective.

thus ϕ is an automorphism. //

F-201C

2) Determine the Galois group of X^3+9X+3 over the rationals $\mathbb{Q}$.

Pf:

By Eistenstein X^3+9X+3 is irred. over $\mathbb{Q}$ b/c $3 \nmid 1$, $3 \mid 9$, $3 \mid 3$ and $3^2 \nmid 3$.

The discriminant is

$$\begin{aligned}\Delta &= -4a^3 - 27b^2 \\ &= -4(9)^3 - 27(3)^2 \\ &= -4(9)^3 - 3(9)^2 \\ &= 9^2(-4(9)-3) \\ &= 9^2(-36-3) \\ &= 9^2(-39)\end{aligned}$$

Since $\sqrt{9^2(-39)} \notin \mathbb{Q}$.

Then the Galois group of X^3+9X+3 over $\mathbb{Q}$ is S_3. //

F-201C

3) Show that the class of separable extensions is a distinguished class of ext.

Pf:

(1)

($\Rightarrow$) Let $K \subseteq F \subseteq E$ subfields and E/K sep. Every elmt of E is sep over F and every elmt F is an elmt of E so sep over K.

$\Rightarrow$ E/F and F/K sep.

($\Leftarrow$)

Let E/F and F/K be sep.

If E/K is finite then we are done. by L. Cor 4.2

If E/K is infinite, let $\alpha \in E$.

Then α is sep over F.

Let $f(x) = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X_n = \text{irr}(\alpha, F, X)$

So we have $K \subseteq K(a_0, \dots, a_{n-1}) \subseteq K(a_0, \dots, a_{n-1}, \alpha)$ and each step is seperable since

$\rightarrow$ $K(a_0, \dots, a_{n-1})$ is sep over K since F/K is sep. $\forall\, a_i \in F$.

$\rightarrow$ α is sep over $K(a_0, \dots, a_{n-1})$ b/c α is sep over F $\forall\, a_i \in F$.

Then $K(a_0, \dots, a_{n-1}, \alpha)$ is sep over K.

Hence α is sep over K. Thus since α arbitrary $\forall\, \alpha \in E$ then E/K is sep. //

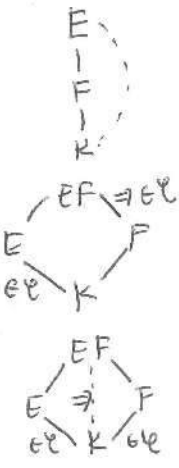
(2)

Let E/K be sep and F/K arbitrary where $E, F \subseteq L$.

Note EF is generated by E over F and the elmt of E are sep over F since E/K is sep $\forall$ $K \subset F$

Then by Thm 4.4, since EF is generated by sep elmt of E over F, then EF/F is sep. //

Def Let $\mathcal{C}$ be a certain class of ext fields $F \subset E$. $\mathcal{C}$ is distinguished iff



(1) Let $K \subset F \subset E$.

$E/K \in \mathcal{C}$ iff $F/K, E/F \in \mathcal{C}$

(2) If $E/K \in \mathcal{C}$, F/K any and $E, F \subseteq L$ (field) then $EF/F \in \mathcal{C}$. (lifting property)

(3) If $F/K, E/K \in \mathcal{C}$ and $F, E \subseteq L$ then $FE/K \in \mathcal{C}$.

note (1) $\forall$ (2) $\Rightarrow$ (3)

F-201C

4) Let K be a field with $\text{char}(K) = p \neq 0$ and let F/K be alg.

Show that $u \in F$ sep over K iff $K(u) = K(u^{p^n})$ $\forall\, n \geq 1$.

Pf:

sidenote: $(K(u))^{p^n} = K^{p^n}(u^{p^n})$ by Freshmans dream $\because \text{char } K = p$ (*)

($\Rightarrow$)

Consider, $K(K(u))^p = K(K^p(u^p))$ by (*)

$= KK^p(u^p)$

$= K(u^p)$ bc $K^p \subseteq K$.

Now since u is sep over $K \Rightarrow K(u)$ is sep (by def)

By cor 6.10 ~ [(3) $\Rightarrow$ (1)]

since $K(u)/K$ is sep $\Rightarrow K(u)^p K = K(u)$

so $KK(u)^p = K(u)$ but $KK(u)^p = K(u^p)$

$\Rightarrow K(u) = K(u^p)$

Since $K(u)$ is sep and $K(u) = K(u^p)$ then $K(u^p)$ is sep.

$\Rightarrow u^p$ is sep. (by def)

Since u was arbitrary take u to be u^p, so we get

$K(u) = K(u^p) = K((u^p)^p) = K(u^{p^2}) = \ldots$

Thus $K(u) = K(u^{p^n})$ $\forall$ $n \geq 1$. //

($\Leftarrow$) let $K(u) = K(u^{p^n})$ $\forall\, n \geq 1$

consider, $K(K(u))^{p^n} = KK^{p^n}(u^{p^n})$ by (*)

$= K(u^{p^n})$ bc $K^{p^n} \subseteq K$

$= K(u)$ by assumption.

so by cor 6.10 ~ [(2) $\Rightarrow$ (3)]

$\Rightarrow K(u)/K$ is sep $\Rightarrow u$ is ~~de~~ sep by def. //

F-201C

5) Show that for each prime integer p and each positive integer n $\exists$ an irred. poly $f \in \mathbb{Z}/p\mathbb{Z}[x]$ of deg n.

Pf:

Let F be the ext field of $\mathbb{Z}/\mathbb{Z}p = \mathbb{Z}p$ with order p^n.

So $[F : \mathbb{Z}p] = n$.

By the primitive elmt thm, $F = \mathbb{Z}p(\alpha)$ for some $\alpha \in F$
(since finite ext of finite fields)

Let $f = \text{irr}(\alpha, \mathbb{Z}p, x)$

So $n = [F : \mathbb{Z}p] = \deg(\text{irr}(\alpha, \mathbb{Z}p, x)) = \deg(f)$.

Thus $\deg f = n$.

F-201C

(e) Prove or disprove that each finite ext field K of $\mathbb{Q}$ is a subfield of a cyclotomic ext of $\mathbb{Q}$.

Fake,

counter example.

Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq B$ where B is a cyclotomic ext of $\mathbb{Q}$.

Since $B/\mathbb{Q}$ cyclotomic, then $G(B/\mathbb{Q})$ is abelian.

$\Rightarrow \exists\ H \subseteq G(B/\mathbb{Q})$ s.t. H is normal in $G(B/\mathbb{Q})$

where H is the Galois group associated with

$B/\mathbb{Q}(\sqrt[3]{2})$

$\Rightarrow \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is normal.

$\rightarrow\leftarrow$ b/c x^3-2 irred in $\mathbb{Q}$, and has a root in $\mathbb{Q}(\sqrt[3]{2})$ but x^3-2 does not split into linear factors in $\mathbb{Q}(\sqrt[3]{2})$.

Thus it cannot be normal.

Thus $\exists$ a finite ext field K of $\mathbb{Q}$ s.t. K is not a subfield of a cyclotomic ext of $\mathbb{Q}$.

//

F-201C

7)

(a) Define the norm N_K^E of a finite ext E/K of fields

Let E/K be a finite ext. Let $\sigma_1, \ldots, \sigma_n$ be the K-embeddings from E to $\bar{K}$ (assume $E \subseteq \bar{K}$). Let $p^m = [E:K]_i$ then for $\alpha \in E$ the norm of α from E to K is defined as $N_K^E(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)^{p^m}$.

(b) State Hilberts thm 90

Let E/K be cyclic ext of degree n with Galois group G. Let σ be a generator of G. Let $\beta \in E$ then the norm $N_K^E(\beta) = 1$ iff $\exists$ an $\alpha \neq 0$ in E s.t. $\beta = \alpha/\sigma\alpha$.

(c) What did we use Hilberts thm 90 for?

Given enough roots of unity in our base field, we can use Hilberts thm 90 to determine if we have cyclic exts.

//

Chari

2012 Part C

Algebra Qualifying Examination, ~~2012, Part A, C~~

Each question is worth 10 points. Answer any 4. Please remember, all answers need justification.

1. Let K be a field and let $K[x]$ be a polynomial ring in one variable and $K(x)$ the corresponding quotient field. Give an example of a monomorphism $\sigma : K(x) \to K(x)$ which is the identity on K but is not onto. (You must explain why your example is a homomorphism of fields and why it is a monomomorphism). Use this to deduce the following statement. Suppose that F is an extension field of K such that for every intermediate field E every monomorphism $\sigma : E \to E$ which is the identity on K is an automorphism. Then F is an algebraic extension of K.

2. Suppose that F is a field extension of K. Define the Galois group of F over K and the notion of F being Galois over K. Suppose that $E \supset L$ are intermediate fields of the extension such that $[E : L] = 2$. Prove that the Galois group of F over E is a subgroup of the Galois group of F over L of index at most 2. (You should prove the statement explicitly in this simple example and not just refer to the statement of the appropriate theorem).

3. Suppose that F is a finite–dimensional Galois extension of K and assume that the Galois group is the direct product $S_3 \times Z_2$.

(i) If E is an intermediate extension, what are the possible values of $[E : K]$.
(ii) Prove that there exists two distinct intermediate fields L_1 and L_2 such that $[L_j : K] = 6$, and L_j is Galois over K, $j = 1, 2$. Are there any others with these properties?

4. Let F_7 be the cyclotomic extension of $\mathbb{Q}$ of order seven. If ζ is a primitive seventh root of unity, what is the irreducible polynomial over $\mathbb{Q}$ of $\zeta + \zeta^{-1}$. You must justify your answer.

5. Let F be a finite field of characteristic p. Prove that F is a separable extension of Z_p. Suppose now that E is a finite–dimensional extension of F. Prove that E is separable over F. Now prove that any algebraic closure of F is algebraic and Galois over F.

6. Let $f \in \mathbb{K}[x]$ be a cubic whose discrminant is a square in K. If $charK \neq 2$ prove that f is either irreducible or factors completely in K. What happens if $charK = 2$?

Spring 2012

2011 Chang

Part C.

1. Find a polynomial $f(x) \in \mathbf{Q}[x]$ with $\deg(f) = 101$ and f is not solvable by radicals. Justify your answer.

2. Give an example of an infinite field K with $\mathrm{char}K = 5$ and a polynomial $f(x) \in K[x]$ such that the splitting field of f over K has degree 20 and is a cyclic extension of K. Justify your answer.

3. Let F be a cyclotomic extension of $\mathbf{Q}$ of order 24. Determine all intermediate fields and give the diagram of subfields of F. Among all these extensions which one(s) are normal? separable? radical? Justify your answer.

4. Let $F > E > K$ be fields. Prove or disprove each of the following statements.

   (a). If F is Galois over E and E is Galois over K, then F is Galois over K.

   (b). If F is purely inseparable over E and E is purely inseparable over K, then F is purely inseparable over K.

   (c). If F is normal over E and E is normal over K, then F is normal over K.

Spring 2011

2010

Dolgushev, Vasiliy

Part C.

1. Prove that every finite field K is perfect.

2. Let E be a splitting field of the polynomial $f(x) = x^5 - 4x + 2$ over $\mathbf{Q}$. Show that this polynomial is irreducible in $\mathbf{Q}[x]$. Prove that the Galois group $\mathrm{Aut}_{\mathbf{Q}}(E)$ is isomorphic to S_5. Is it possible to find a radical extension F of $\mathbf{Q}$ such that $F \supset E$?

3. Let F be a field with p^n elements (here p is prime). Prove that F contains a primitive d-th root of unity for every divisor d of the number $p^n - 1$.

4. Let $K(x_1, x_2, \ldots, x_n)$ be the field of rational functions in n determinates. Show that $\{x_1, x_2, \ldots, x_n\}$ is a transcendence basis of $K(x_1, x_2, \ldots, x_n)$ over K.

Spring 2010

2009

RVSH

Do 4 out of 5 problems only

Part C.

1. Let K be a field of characteristic zero. Let $f \in K[x]$ be a cubic whose discriminant is a square in K. Show that either f is irreducible over K or factors completely over K.

2. Let G be a finite group of automorphisms of an integral domain A. Let $R = \{a \in A : \sigma(a) = a \text{ for each } \sigma \in G\}$. Show that each $a \in A$ satisfies a monic $f \in R[X]$. Further, if E and F are the quotient fields of A and R respectively, then E/F is separable.

3. Let $g_n(X)$ be the n-th cyclotomic polynomial over $\mathbf{Q}$, let p be a prime integer not dividing n, let $F = \mathbf{Z}/p\mathbf{Z}$. Suppose the canonical image $\overline{g}_n(X)$ of $g_n(X)$ in $F[X]$ remains irreducible in $F[X]$ and let $E = F[X]/(\overline{g}_n(X))$. Show that the Galois group $G(E/F)$ is isomorphic to the group of units $(\mathbf{Z}/n\mathbf{Z})^*$ of $\mathbf{Z}/n\mathbf{Z}$.

4. Show that if $f \in \mathbf{Z}/p\mathbf{Z}[X]$ is irreducible of degree n, then f divides $X^{p^n} - X$ in $\mathbf{Z}/p\mathbf{Z}[X]$.

5. (a) Define what it means for $f \in \mathbf{Q}[X]$ to be solvable by radicals.
   (b) Show that $X^5 - 6X + 3$ is not solvable by radicals over $\mathbf{Q}$.

Spring 2009

2009 C1:

Let K be a field of char 0. Let $f \in K[x]$ be a cubic whose discriminant is a square in K. Show that either f is irred in K or factors completely over K.

Pf:

Note that by def of discriminant, since we have a discriminant, D w/ $D \neq 0$ the roots of f are distinct.

Let F be the splitting field of f and $G = Aut_K F$

Let $D = \Delta^2$

Since $\Delta \in K$ then by Cor 4.6.

$K(\Delta) = K$ (b/c $\Delta \in K$) corresponds to $G \cap A_3$

So $G \subseteq A_3$.

If f is irreducible we are done and $G \cong A_3$ by Cor 4.7

If f is reducible then $G \subsetneq A_3$

However $A_3 \cong \mathbb{Z}_3$ and $\mathbb{Z}_3$ has no proper subgroups

Thus: $G = \{e\}$

$\Rightarrow K = F$ and thus f factors completely in K. //

2009 C2:

Let G be a finite group of automorphisms of an integral domain A. Let $R = \{a \in A \mid \sigma(a) = a \text{ for each } \sigma \in G\}$. Show that each $a \in A$ satisfies a monic $f \in R[X]$. Further, if E and F are the quotient fields of A and R resp, then E/F is separable.

PF:

Let $G = \{\sigma_1, \dots, \sigma_n\}$ and $a \in A$.

Since G is a group, $\exists\ \sigma_i \in G$ s.t. $\sigma_i(a) = a$.

So a is a root of the polynomial

$$f = (X - \sigma_1(a)) \cdots (X - \sigma_n(a)) \qquad (*)$$
$$= X^n - f_1 X^{n-1} + \dots + (-1)^{n-1} f_{n-1} X + (-1)^n f_n$$

where f_i are the elementary symmetric function.

(each $f_i \in R$ since $\sigma_j \in G$ just permutes the roots (and we use the roots to construct each f_i).

Thus $f \in R[X]$ and is monic.

Lets show $F = E^G$,

$F \subseteq E^G$ is trivial.

Let $X \in E^G$ so $X = \frac{a}{b}$ for some $a, b \in R$, $(a,b) = 1$.

$$\Rightarrow \sigma(X) = \sigma\left(\frac{a}{b}\right) = \frac{\sigma(a)}{\sigma(b)} = \frac{a}{b}$$

$$\Rightarrow b\sigma(a) = a\sigma(b)$$

$\Rightarrow a \mid \sigma(a)$ and $b \mid \sigma(b)$ since $(a,b) = 1$.

since $b\sigma(a) = a\sigma(b)$, $a = k\sigma(a)$, $b = k\sigma(b)$

but $(a,b) = 1$ so $k = 1$

Thus $\sigma(a) = a$ and $\sigma(b) = b$.

So $X = \frac{a}{b} \in F$

So $E^G \subseteq F$

Thus $E^G = F$.

Next we will show E/F is normal.

Define K to be the splitting field of $\{f_a\}$ over F where f_a is of the form $(*)$

$K = F(X)$, $X = \{\sigma_i(a)\}_{1 \le i \le n}^{a \in A}$

$F \subseteq E$, $X \subseteq A \subseteq E \Rightarrow K \subseteq E$

$A \subseteq K \Rightarrow F \subseteq K$

$\Rightarrow K = E$

$\Rightarrow E/F$ is normal.

need this to use thm

Let G' be the group of automorphisms of E

$\Rightarrow G \subseteq G' \Rightarrow E^{G'} \subseteq E^G$

Since $E^G = F$, it follows that $E^{G'} \subseteq E^G = F \subseteq E$.

By prop 6.11 (Lang), $E/E^{G'}$ is sep.

Since separable ext are distinguished,

$\Rightarrow E/F$ is separable. //

2009 C3:

Let $q_n(x)$ be the n-th cyclotomic poly over $\mathbb{Q}$, let p be a prime integer not dividing n, let $F = \mathbb{Z}_p$. Suppose the canonical image $\bar{q}_n(x)$ of $q_n(x)$ in $F[x]$ remains irred in $F[x]$ and let $E = F[x]/(\bar{q}_n(x))$. Show that the Galois group $G(E/F)$ is $\simeq$ to the group of units $(\mathbb{Z}_n)^*$ of $\mathbb{Z}_n$.

Pf:

Note E is a field of char p and E/F is a cyclotomic ext of order n. also $p \nmid n$.

So $G(E/F)$ is isomorphic to a subgrp of $(\mathbb{Z}/n\mathbb{Z})^*$ (Thm V 8.1. (iii)

but $|E| = |\mathbb{Z}_p[x]/(\bar{q}_n(x))| = p^{\deg(\bar{q}_n(x))}$

So $[E:F] = \deg(\bar{q}_n(x)) = \deg(q_n(x)) = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$

canonical map

So $|G(E/F)| = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Thus since $|G(E/F)| = |(\mathbb{Z}/n\mathbb{Z})^*|$ and since $G(E/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ then

$G(E/F) \cong (\mathbb{Z}/n\mathbb{Z})^*$. //

2009 C4

4) Show that if $f \in \mathbb{Z}/p\mathbb{Z}[x]$ is irred. of deg n, then f divides $x^{p^n} - x$ in $\mathbb{Z}/p\mathbb{Z}[x]$.

Pf:

Let $f \in \mathbb{Z}_p[x]$ be irred of deg n.

Then we know that $\exists$ a root $\alpha \in \mathbb{Z}_p(\alpha)$ of deg n over $\mathbb{Z}_p$.

This means $\mathbb{Z}_p(\alpha)$ has p^n elmt (by R4 (1)⇒(2))

So all elmts in $\mathbb{Z}_p(\alpha)$ satisfy $x^{p^n} - x = 0$ (R4 (2)⇒(4))

therefore $f(x) = \text{irr}(\alpha, \mathbb{Z}_p, x)$ must divide $x^{p^n} - x$ by uniqueness of the irred poly for α over $\mathbb{Z}_p$. //

2009 C5

(a) Define what it means for $f \in \mathbb{Q}[x]$ to be solvable by radicals.

Let L be a field. We say $f \in L[x]$ is <u>solvable by radicals</u> if its splitting field is contained in a radical ext of L.

(b) Shows that $x^5 - 6x + 3$ is not solvable by radicals over $\mathbb{Q}$.

Let $f(x) = x^5 - 6x + 3$

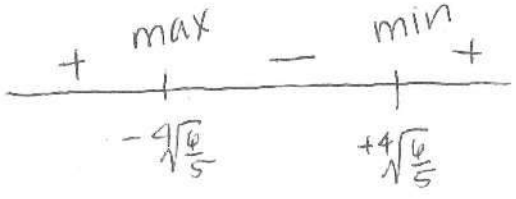
Using Eistein with $p = 3$
we see that $f(x)$ is irred in $\mathbb{Q}$.
b/c $3 \nmid 1$, $3 \mid -6$, $3 \mid 3$, and $3^2 \nmid 3$.

NTS $f(x)$ has exactly two nonreal roots.

well $f'(x) = 5x^4 - 6$

$= 5(x^4 - \frac{6}{5}) = 5(x^2 - \sqrt{\frac{6}{5}})(x^2 + \sqrt{\frac{6}{5}})$

$= 5(x - \sqrt[4]{\frac{6}{5}})(x + \sqrt[4]{\frac{6}{5}})(x^2 + \sqrt{\frac{6}{5}})$



$x = 0$, $f'(0) = -6$

$x = \pm 2$: $f'(\pm 2)^4$

$= 5(2)^4 - 6 > 0$

NTS $f(-\sqrt[4]{\frac{6}{5}}) > 0$ & $f(\sqrt[4]{\frac{6}{5}}) < 0$

$f(-\sqrt[4]{\frac{6}{5}}) = (-\sqrt[4]{\frac{6}{5}})^5 - 6(-\sqrt[4]{\frac{6}{5}}) + 3$

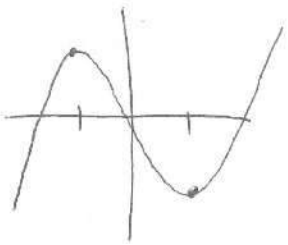
$= -\frac{6}{5}\sqrt[4]{\frac{6}{5}} + 6\sqrt[4]{\frac{6}{5}} + 3 > 0$

$f(\sqrt[4]{\frac{6}{5}}) = (\sqrt[4]{\frac{6}{5}})^5 - 6(\sqrt[4]{\frac{6}{5}}) + 3$

$= \frac{6}{5}(\sqrt[4]{\frac{6}{5}}) - 6\sqrt[4]{\frac{6}{5}} + 3 = -\frac{24}{5}\sqrt[4]{\frac{6}{5}} + 3 < 0$

Thus exact 3 real roots

$\Rightarrow$ exactly 2 non real roots



So by Thm 4.12 (H)

Galois group is S_5

But S_5 is not solvable.

Thus f is not solvable by radicals. //

(Thm from notes 4/7)

2008

Ran

Part C.

1. Let $f(x) = x^5 - x + 1 \in \mathbf{F}_5[x]$.
   (a) Prove that f has no root in $\mathbf{F}_{25}$ (Hint: what polynomial identity holds for any element of $\mathbf{F}_{25}$?).
   (b) Determine the splitting field and the full Galois correspondence for the polynomial $x^5 - x + 1$
      (i) over $\mathbf{F}_5$;
      (ii) over $\mathbf{F}_{25}$;
      (iii) over $\mathbf{F}_{125}$.

2. Let F be a splitting field of $f \in K[x]$ over K. Prove that if an irreducible polynomial $g \in K[x]$ has a root in F, then g splits in linear factors over F. (This result is part of a theorem characterizing normal extensions and you may not, of course, quote this theorem or its corollaries).

3. Disprove (by example) or prove the following: If $K \to F$ is an extension (not necessarily Galois) with $[F : K] = 6$ and $\mathrm{Aut}_K(F)$ isomorphic to the symmetric group S_3, then F is the splitting field of an irreducible cubic in $K[x]$.

4. If $\mathbf{Z}_p \to F$ is a field extension of degree n then $x \mapsto x^p$ is a $\mathbf{Z}_p$-automorphism of F of order exactly n whose fixed field is $\mathbf{Z}_p$.

Spring 2008

2007 chari

Part C.

1. Consider the polynomial $x^5 - ax - 1 \in \mathbf{Z}[x]$. Find all possible values of $a \in \mathbf{Z}$ for which the polynomial is irreducible in $\mathbf{Z}[x]$.

2. Prove that $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$.

3. Let F be a Galois extension of a field K of degree 27. Prove that there exist Galois extensions of K contained in F of degree 3 and 9.

4. Prove that if the Galois group of the splitting field of a cubic over the rational numbers is $\mathbf{Z}_3$ then all roots of the cubic are real.

5. Prove that a finite dimensional extension of a finite field is Galois.

6. Prove that in a finite field of characteristic p every element has a unique p-th root. Give an example to show that the condition that the field be finite is necessary.

Spring 2007

2007 C2:

Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Prove in general for any two distinct nonsquares $a, b \in \mathbb{R}$

Pf:

Well $\mathbb{Q}(\sqrt{a}+\sqrt{b}) \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$ clearly.

Since $\mathbb{Q}(\sqrt{a}+\sqrt{b})$ is a field, then

$$\frac{1}{\sqrt{a}+\sqrt{b}} \in \mathbb{Q}(\sqrt{a}+\sqrt{b}).$$

but $$\frac{1}{\sqrt{a}+\sqrt{b}} \cdot \frac{(\sqrt{a}-\sqrt{b})}{(\sqrt{a}-\sqrt{b})} = \frac{\sqrt{a}-\sqrt{b}}{a-b}$$

so $\frac{\sqrt{a}-\sqrt{b}}{a-b} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$ so $(\sqrt{a}-\sqrt{b}) \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$

so $$\sqrt{a} = \frac{(\sqrt{a}+\sqrt{b})+(\sqrt{a}-\sqrt{b})}{2} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$$

Likewise $\sqrt{b} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$.

Hence $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subset \mathbb{Q}(\sqrt{a}+\sqrt{b})$.

Thus, $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$.

//

2006

Ran

Part C.

1. Let $K \subseteq F$ be a finite-dimensional extension.

   (i) Define what it means for F to be separable over K.

   (ii) Prove from scratch that if K is a finite field then F is separable over K.

   (iii) Prove that if K is of characteristic zero then F is separable over K.

   (iv) Give an example of a non-separable finite-dimensional extension.

2. Let K be a field with 9 elements. Prove from scratch that K has an extension of degree 2 and that any two such are isomorphic over K.

3. Let $u = \sqrt{3+\sqrt{2}}$.

   (i) Determine the minimal polynomial of u over $\mathbf{Q}$.

   (ii) Prove that $F = \mathbf{Q}(u)$ is a splitting field of f over $\mathbf{Q}$.

   (iii) Prove that $\sqrt{7} \in F$.

   (iv) Determine the Galois group of F over $\mathbf{Q}$.

2005

Rush

Do 4 out of 5 only

Part C.

1. Let p be a prime integer and let $\mathbf{F}_{p^n}$ denote the field with p^n elements in a fixed algebraic closure $\mathbf{F}_p$.
   (a) Show that $\mathbf{F}_{p^n} \subseteq \mathbf{F}_{p^m}$ if and only if $n|m$.
   (b) Let q be another prime integer and let $E = \cup_{i=1}^{\infty} \mathbf{F}_{p^{q^i}}$. Show that E is an infinite extension of $\mathbf{F}_p$ which is not algebraically closed.

2. (a) Factor the polynomial $X^9 - 1$ over $\mathbf{Q}$.
   (b) Is $X^6 + X^3 + 1$ irreducible over $\mathbf{Q}$? Explain.
   (c) Give the Galois group of $X^6 + X^3 + 1$ over $\mathbf{Q}$. Explain.

> 2013 Final

3. (a) Define what it means for a polynomial $f \in \mathbf{Q}[x]$ to be solvable by radicals over $\mathbf{Q}$.
   (b) Show that $X^5 - 4X + 2$ is not solvable by radicals over $\mathbf{Q}$.

4. Give an example of a finite extension E/F of fields with infinitely many intermediate fields and explain why your example works.

5. Define the symmetric algebra $S(M)$ of a k-module M and state the universal property it satisfies.

Spring 2005

2005 C1

Let p be a prime integer and let F_{p^n} denote the field w/ p^n elmts in a fixed algebraic closure F_p.

(a) show that $F_{p^n} \subseteq F_{p^m}$ iff $n|m$.

($\Rightarrow$) $F_p \subseteq F_{p^n} \subseteq F_{p^m}$

$\Rightarrow [F_{p^m} : F_p] = [F_{p^m} : F_{p^n}][F_{p^n} : F_p]$

$m = [F_{p^m} : F_{p^n}]n \quad \Rightarrow n|m.$

($\Leftarrow$) let $n|m$. So $m = kn$.

Let $\alpha \in F_{p^n}$ s.t. α is a root of $X^{p^n} - X$

$\Rightarrow \alpha^{p^n} = \alpha$

since $m = kn$, $p^m = (p^n)^k$

So $\alpha^{p^m} = \alpha^{(p^n)^k} = \alpha$

So α is also a root of $X^{p^m} - X \Rightarrow \alpha \in F_{p^m}$

Thus $F_{p^n} \subseteq F_{p^m}$

(b) Let q be another prime integer and let $E = \bigcup_{i=1}^{\infty} F_{p^{q^i}}$. Show that E is an infinite extension of F_p which is not algebraically closed.

Let $E = \bigcup_{i=1}^{\infty} F_{p^{q^i}}$ where q is prime and $q \neq p$. by part (a)

by part (a): $F_p \subsetneq F_{p^q} \subsetneq F_{p^{q^2}} \subsetneq \cdots$

Thus E is an infinite extension of F_p.

Consider $f = X^{p^m} - X \in F_p[X]$ where $(m, q) = 1$, $m > 1$.

If E is algebraically closed, then E must contain a splitting field of f over F_p.

So $F_{p^m} \subseteq E$.

By def of E, there must $\exists$ some $i \in \mathbb{N}$ s.t. $F_{p^m} \subseteq F_{p^{q^i}}$

$\Rightarrow$ (by part a) $m | q^i$ $\rightarrow\leftarrow$ since $(m, q) = 1$. Thus E is not alg. closed. //

2005 C2

(a) Factor the poly x^9-1 over $\mathbb{Q}$.

$$x^9-1 = (x^3)^3-1 = (x^3-1)(x^6+x^3+1)$$
$$= (x-1)(x^2+x+1)(x^6+x^3+1)$$

(b) Is x^6+x^3+1 irred over $\mathbb{Q}$? Explain.

cyclotomic poly

divisors of 9 are 1, 3, 9

$$g_1(x) = (x-1)$$
$$g_3(x) = \frac{x^3-1}{g_1(x)} = \frac{x^3-1}{x-1} = x^2+x+1$$
$$g_9(x) = \frac{x^9-1}{g_1(x)\,g_3(x)} = \frac{x^9-1}{(x-1)(x^2+x+1)} = x^6+x^3+1$$

since $g_9(x)$ is 9th cyclotomic poly over $\mathbb{Q}$, it must be irreducible in $\mathbb{Q}[x]$.

(c) Give the Galois grp of x^6+x^3+1 over $\mathbb{Q}$. Explain

Let F be a cyclotomic ext of $\mathbb{Q}$ of order 9.

So if ξ is a primitive root of unity (ie a root of $g_9(x)$)

$$F = \mathbb{Q}(\xi)$$

so $g_9(x)$ splits in F and has distinct roots

$\Rightarrow F/\mathbb{Q}$ galois

so $G(F/\mathbb{Q}) = Aut_{\mathbb{Q}} F \cong \mathbb{Z}_9^{\times}$ since F is the splitting field of the 9th cyclotomic poly over $\mathbb{Q}$.

($\mathbb{Z}_9^{\times}$: set of all units in $\mathbb{Z}_9 = \{1,2,4,5,7,8\}$)

2005 C3

(a) Define what it means ~~beeee~~ for a poly $f \in \mathbb{Q}[x]$ to be solvable by radicals over $\mathbb{Q}$.

Let L be a field. a poly $f \in L[x]$ is solvable by radicals if its splitting field is contained in a radical extension of L.

(b) Show that $x^5 - 4x + 2$ is not solvable by radicals over $\mathbb{Q}$.

Let $f(x) = x^5 - 4x + 2$

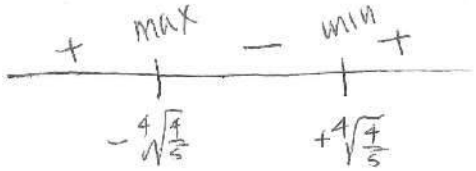
using Eistein w/ $p = 2$,
we see that $f(x)$ is irred in $\mathbb{Q}$
blc $2 \nmid 1$, $2 \mid -4$, $2 \mid 2$, $2^2 \nmid 2$.

NTS $f(x)$ has exactly two complex roots.

well $f'(x) = 5x^4 - 4$

$= 5(x^4 - \frac{4}{5}) = 5\left(x^2 - \sqrt{\frac{4}{5}}\right)\left(x^2 + \sqrt{\frac{4}{5}}\right)$

$= 5\left(x - \sqrt[4]{\frac{4}{5}}\right)\left(x + \sqrt[4]{\frac{4}{5}}\right)\left(x^2 + \sqrt{\frac{4}{5}}\right)$



$x = 0$, $f'(0) = -4$

$x = \pm 2$, $f'(\pm 2) = 5(2)^4 - 4 > 0$

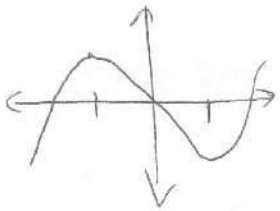
NTS $f(-\sqrt[4]{\frac{4}{5}}) > 0$ & $f(\sqrt[4]{\frac{4}{5}}) < 0$

$f(-\sqrt[4]{\frac{4}{5}}) = (-\sqrt[4]{\frac{4}{5}})^5 - 4(-\sqrt[4]{\frac{4}{5}}) + 2$

$= -\frac{4}{5}\left(\sqrt[4]{\frac{4}{5}}\right) + 4\left(\sqrt[4]{\frac{4}{5}}\right) + 2 > 0$

$f(\sqrt[4]{\frac{4}{5}}) = \left(\sqrt[4]{\frac{4}{5}}\right)^5 - 4\left(\sqrt[4]{\frac{4}{5}}\right) + 2$

$= \frac{4}{5}\sqrt[4]{\frac{4}{5}} - 4\left(\sqrt[4]{\frac{4}{5}}\right) + 2 = \left(\frac{4}{5} - \frac{20}{5}\right)\sqrt[4]{\frac{4}{5}} + 2 = -\frac{16}{5}\sqrt[4]{\frac{4}{5}} + 2 < 0$

Thus 

$f(x)$ has exactly 3 real roots
so it has exactly 2 complex roots.

So by thm 4.12 H
Galois group is S_5.

But S_5 is not solvable

thus f is not solvable by radicals.
(thm notes 4/7).

2005 C4

Give an example of a finite extension E/F of fields with infinitely many intermediate fields and explain why your example works.

Let $E = \mathbb{Z}_2(x^2, y^2)$ and $F = \mathbb{Z}_2(x, y)$, so $E \subset F$

NTS $[F:E] = 4$.

consider $E \subset \mathbb{Z}_2(x^2, y) \subset F$

$\Rightarrow [F:E] = [F : \mathbb{Z}_2(x^2, y)][\mathbb{Z}_2(x^2, y) : E]$

$\{1, y\}$ is a basis for $\mathbb{Z}_2(x^2, y)/E$ and

$\{1, x\}$ is a basis for $F/\mathbb{Z}_2(x^2, y)$.

THUS $[F:E] = 2 \cdot 2 = 4$.

NTS F/E is not simple.

ATC F/E is simple, so $\exists\ w \in F$ s.t. $F = E(w)$

So $w^2 \in E$ consider $w = ax + by + 1$

$w^2 = a^2x^2 + b^2y^2 + 1 \in E$ (since $\text{char } E = 2$)

So w is a root of $f(z) = z^2 - w^2 \in E[z]$

Since $w \notin E$, f is irred over E

$\Rightarrow [F:E] = 2 \neq 4$ $\rightarrow\leftarrow$

THUS F/E is not simple.

Therefore by primitive elmt thm there exist infinitely many intermediate fields.

2004 (Oct)

Chang

Part C.

1. Let F be a splitting field over $\mathbf{Q}$ of the polynomial $x^4 - 4x^2 - 1$. Let $g(x) = x^3 + 6x^2 - 12x - 12$. Does $g(x)$ have a root in F? Prove your answer.

2. Let F be a splitting field over $\mathbf{Q}$ of the polynomial $x^4 - 5$. Find all the intermediate fields of F over $\mathbf{Q}$. Indicate the ones which are Galois over $\mathbf{Q}$. Prove your answer.

3. Let $\mathbf{F}_{12}$ be a cyclotomic extension of $\mathbf{Q}$ of order 12. Determine $\mathrm{Aut}_{\mathbf{Q}}\,\mathbf{F}_{12}$ and all intermediate fields.

4. Construct a field with 49 elements and give the rules for its addition and multiplication. If a is a generator, what is the multiplicative inverse of $1 + a$ in terms of your set of *minimal* generator(s)?

5. Let a, b be nonzero in some extension field of K. Assume that a is separable over K and b is purely inseparable over K. Prove that $K(a, b) = K(ab) = K(a + b)$.

Spring 2004

2004(Apr)

~~Charg~~? Char?

Part C.

1. Suppose that F is an extension field of K. Let $u, v \in F$ be algebraic over K and assume that the degree of u is prime to the degree of v over K. What is the degree of the extension $K(u, v)$ over K? You must provide a proof for you answer.

2. (a) Let F be an extension field of K. Define the Galois group of F over K. Suppose that L is a subfield of F containing K. When do we say that L is closed? Let G be the Galois group of F over K. Let H be a subgroup of G. When do we say that H is closed?

   (b) Prove that if H is a subgroup of G then its fixed field is closed.

3. Prove that a field F generated by an infinite set of separable elements is separable.

4. Suppose that K is the field of rational numbers and let f be an irreducible polynomial of degree 3 and discriminant D. Suppose $D \neq 0$. Prove that $D > 0$ iff f has three real roots. What conclusion can you draw if $D < 0$?

5. Suppose that $f \in K[x]$ is a monic polynomial whose roots are distinct and form a field. Prove that $\mathrm{char} K \neq 0$. What can you say about f in this case?

6. Define a cyclotomic extension of order n of a field K. Define the n-th cyclotomic polynomial over K. Suppose that F_8 is a cyclotomic extension of order 8 over the field $\mathbf{Q}$ of rational numbers. Determine the Galois group of F_8 over $\mathbf{Q}$.

Spring 2003?

2003

Chari

Part C.

1. A complex number is said to be an algebraic number if it is algebraic over $\mathbf{Q}$ and an algebraic integer if it is a root of a monic polynomial in $\mathbf{Z}[x]$.

   (a) Prove that u is an algebraic number iff there exists an integer n such that nu is an algebraic integer.

   (b) If $r \in \mathbf{Q}$ is an algebraic integer prove that $r \in \mathbf{Z}$.

   (c) If u is an algebraic number prove that $u + n$ is algebraic for all $n \in \mathbf{Z}$.

   (d) Deduce from the above, that the sum and product of two algebraic integers is an algebraic integer.

2. Let F be a field extension of K. Define the Galois group G of F over K. Now define what one means by a stable subfield of this extension. Prove that if E is a stable intermediate field, then the Galois group of F over E is a normal subgroup of G. Conversely, prove that if H is a normal subgroup of G, then the fixed field of H is a stable subfield of the extension $F \supset K$.

3. Let F be an extension field of K. Define the maximal algebraic extension of K in F. Suppose that for every extension $F \supset K$, the maximal extension is K, prove that K is algebraically closed. Now suppose that K is algebraically closed and let F be any extension of K. Prove that the maximal algebraic extension of K in F is K.

4. Let F be a finite dimensional extension of $\mathbf{Z}_3$. Deduce that F is Galois over $\mathbf{Z}_3$. Prove that $\varphi : F \to F$ given by $\varphi(u) = u^3$ is a $\mathbf{Z}_3$-automorphism of F. Show that φ generates the Galois group of F over $\mathbf{Z}_3$.

5. (a) Let $K = \mathbf{Q}(i)$. Let $F \subset \mathbf{C}$ be a field that contains a root of the polynomial $x^4 - 2 \in K[x]$. Prove that F is the splitting field of this polynomial. What is the Galois group of this polynomial? Determine the subfields of this extension.

   (b) Let E be an algebraic extension of a field K. Prove that there exists an extension F of E such that F is normal over K and no proper subfield of F containing E is normal over K.

Spring 2003

2002 Chari

Part C.

1. Prove that if $f \in K[x]$ is a polynomial of degree n, then there exists an extension of K in which f has a root. Consider the example $f(x) = x^3 - 5x - 2 \in \mathbf{Q}[x]$, let u be a root of this polynomial. What is the natural basis of $\mathbf{Q}(u)$ and write the element $x^4 - 3x + 1$ as a linear combination of the basis elements.

2. Let F be a finite-dimensional Galois extension of K and E an intermediate field. Prove that there exists a unique smallest field L between E and F which is Galois over K and prove that

$$\mathrm{Aut}_L F = \cap_\sigma \sigma(\mathrm{Aut}_E F)\sigma^{-1}.$$

3. Prove that F is an algebraic closure of K iff F is algebraic over K and for every algebraic field extension E_1 of another field K_1 and isomorphism of fields $\sigma : K_1 \to K$, σ extends to a monomorphism $E \to F$.

4. (a) Compute the Galois group of $x^3 - 10$ over $\mathbf{Q}(\sqrt{2})$.
   (b) Prove that if F is Galois over E, E is Galois over K and F is a splitting field of polynomials in $K[x]$, then F is Galois over K.

5. Let F be an algebraic closure of $\mathbf{Z}_p$. Prove that
   (a) F is algebraic Galois over $\mathbf{Z}_p$.
   (b) The map $\varphi : F \to F$ given by $u \mapsto u^p$ is a non-identity $\mathbf{Z}_p$-automorphism of F.
   (c) What is the fixed field of the subgroup of $\mathrm{Aut}_{\mathbf{Z}_p} F$ generated by φ.

Spring 2002

2002 C1:

Prove that if $f \in K[X]$ is a polyn. of degree n, then $\exists$ an extension of K in which f has a root.

Pf:

Let $p \in K[X]$ be an irred factor of f, say of degree r. (so $r \leq n$)

It suffices to construct an extension of K in which p has a root.

Since p irred $\iff$ (p) is maximal in set of all principal ideals but in field so all ideals are principal so (p) is max in $K[X]$.

Thus $F = K[X]/(p) = \{ a_0 + a_1 X + \dots + a_{r-1} X^{r-1} + (p) \mid a_i \in K \}$ is a field (Thm 2.20)

Identifying K with its image under the monomorphism $a \longmapsto a + (p)$, it can be assumed that F is an extension of K.

Let $u = X + (p)$

Then, writing $p(x) = \sum_{i=1}^{r} b_i x^i$ the i^{th} term in the expression of $p(u)$ has the form

$$b_i \left(\sum_{j=1}^{i} \binom{i}{j} X^i (p)^{i-j} \right) = b_i X^i + (p).$$

Thus $p(u) = p(X) + (p) = 0 + (p)$. //

Consider the example $f(x) = x^3 - 5x - 2 \in \mathbb{Q}[x]$.

Let u be a root of this polyn.

What is the natural basis of $\mathbb{Q}(u)$ and write the elmt $x^4 - 3x + 1$ as a linear combination of the basis elmts.

as a vector space over $\mathbb{Q}$

$$\mathbb{Q}(u) = \{ a_0 + a_1 u + a_2 u^2 \mid a_i \in \mathbb{Q},\ f(u) = 0 \}$$

(since $K(u) \cong K[x]/(f)$ since f 3rd degree it kills everything above 3rd deg)

This is the natural basis $u_i := x^i + (f)$ of Thm VI.6

polynomial division gives

$$x^4 - 3x + 1 = x f(x) + 5x^2 - x + 1.$$

$$= x(x^3 - 5x - 2) + 5x^2 - x + 1$$

$$= x^4 - 5x^2 - 2x + 5x^2 - x + 1$$

$$= x^4 - 3x + 1 \quad \checkmark$$

so that in $\mathbb{Q}(u)$,

$$u^4 - 3u + 1 = 5u^2 - u + 1.$$

//

2001

Chari

Part C.

1. (a) Suppose that $F = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbf{Q}$ for $i = 1, 2, \ldots, n$. Prove that $\sqrt[3]{2} \notin \mathbf{Q}$.
   (b) Determine the degree of the extension of $\mathbf{Q}(\sqrt{32\sqrt{2}})$ over $\mathbf{Q}$.

2. (a) Determine the splitting field and its degree over $\mathbf{Q}$ for $x^6 - 4$.
   (b) Prove that the polynomial $x^{p^n} - x$ over $\mathbf{Z}_p$ is separable.

3. For any integer $r \geqslant 1$, let $\mathbf{F}_{p^r}$ be a finite field of cardinality p^r. Prove that $\mathbf{F}_{p^r} \subset \mathbf{F}_{p^s}$ if and only if r divides s. (Hint: First prove that r divides s if and only if $x^r - 1$ divides $x^s - 1$).

4. Determine the Galois group of $(x^3 - 2)(x^3 - 3)$ over $\mathbf{Q}$. Determine the subfields which contain $\mathbf{Q}(\rho)$ where ρ is a primitive cube root of unity.

5. Determine the splitting field of $x^p - x - 1$ over $\mathbf{Z}_p$ and prove explicitly that the Galois group is cyclic.

6. Determine the Galois group of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ and let $F/\mathbf{Q}$ be the splitting field of this polynomial. Determine all subfields $L \subset F$ which are galois over $\mathbf{Q}$.

Spring 2001

2000

Part C.

1. Let K be a field containing a primitive n-th root of 1, ζ, where the characteristic of K is either 0 or does not divide n, and let F be a field extension of degree n over K.

   (i) Prove that if $n = 2$ then F is cyclic Galois over K.

   (ii) Assume F is cyclic Galois over K (any n), and let σ be a generator of $\mathrm{Gal}(F/K)$, considered as an endomorphism of F as K-vector space. Show that ζ is an eigenvalue of σ.

   (iii) Conclude from (ii) or prove otherwise that, with assumptions as in (ii), F is a radical extension of K.

2. Let G be a finite group. Prove that there exists a finite Galois field extension $K \subseteq F$ with Galois group G.

3. Let $K \subseteq F$ be a field extension. Prove or disprove the following

   (i) If $\mathrm{Gal}(F/K) \simeq S_3$ then F is a splitting field over K of some cubic polynomial.

   (ii) Ditto, assuming in addition that F is Galois over K.

4. Let $f(x) = x^{11} + 5x^3 + 10 \in \mathbf{Q}[x]$ and let α be a root of f in $\mathbf{C}$. Let $g(x) = x^{19} + 6x^5 - 12$. Does g have a root in $\mathbf{Q}(\alpha)$? Prove your answer.

5. Find with proof a transcendence base over $\mathbf{Q}$ of

$$\mathbf{Q}(x^5, x^2 + y^5, x^3 + y^4).$$

Spring 2000

1999 Do 4 out of 6 only rush?

Part C.

1. Let F be a splitting field of $X^{18} - 1$ over $\mathbf{Q}$. Determine all intermediate fields $F \supseteq \mathbf{Q}$. How many of them are Galois over $\mathbf{Q}$?

2. Find all roots of unity in $\mathbf{Q}(\sqrt{11})$.

Prove or disprove.

3. The polynomial $X^{625} - X - 1$ is irreducible over $\mathbf{Z}_5$.

4. Let F be a degree 4 extension of $\mathbf{Q}$. If any proper subfield of F is Galois over $\mathbf{Q}$, then F is Galois over $\mathbf{Q}$.

5. For field extensions, being separable (respectively, purely inseparable) is transitive.

6. Let $F > k$ be fields.

   (i) $[F : k] = \infty \implies \text{tr. d.}_k F > 0$.

   (ii) $[F : k] < +\infty \implies \text{tr. d.}_k F = 0$.

   (iii) $\text{tr. d.}_k F < +\infty \implies \text{tr. d.}_k F = [F : k]$.

Spring 1999

1999 C1

1) Let F be a splitting field of $X^{18}-1$ over $\mathbb{Q}$?
Determine all intermediate fields $F \geq \mathbb{Q}$.
How many of them are Galois over $\mathbb{Q}$?

Note:
$X^{18}=1$
$X^{18}=e^{2\pi i k}$

$X^{18/18} = e^{\frac{2\pi i k}{18}}$
$X^{1} = e^{\frac{\pi i k}{9}}$

Pf:
Note: $F = \mathbb{Q}(e^{\frac{\pi i}{9}})$

Intermediate fields:
note: we know $X = e^{\frac{\pi i k}{9}}$ is a root of $X^{18}-1$
for $k = \{1, \ldots, 18\}$

~~if $K \neq \mathbb{Q}$ and $K \neq F$ then $K = \mathbb{Q}(e^{\frac{\pi i k}{9}})$~~

let $E_k = \mathbb{Q}(e^{\frac{\pi i k}{9}})$

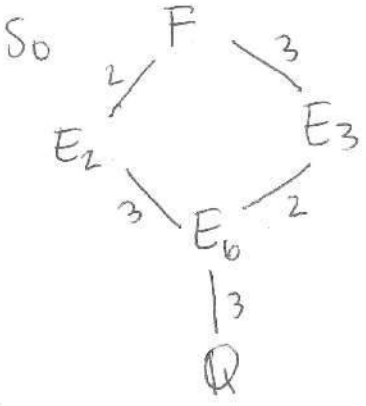
Well, $F = E_1 = E_5 = E_7 = E_{11} = E_{13} = E_{17}$ b/c generate all since odd relatively prime to 9

$E_2 = E_4 = E_8 = E_{10} = E_{14} = E_{16}$ b/c even relatively prime to 9.

$E_3 = E_{15}$ common prime w/ 9 odd

$E_6 = E_{12}$ " even

$\mathbb{Q} = E_9 = E_{18}$



So the intermediate fields are E_2, E_3, E_6

note that $F/\mathbb{Q}$ is Galois.
E_K is the splitting field for $X^{18/K}-1$ $(K=2,3,6)$
(so $E_K/\mathbb{Q}$ normal)
and $E_K/\mathbb{Q}$ is sep since $\mathrm{Char}\,\mathbb{Q}=0$.
thus $E_K/\mathbb{Q}$ is Galois for $K=2,3,6$?

1999 C2

2) Find all roots of unity in $\mathbb{Q}(\sqrt{11})$

Well,

$1^n = 1$ is a n^{th} root of unity

$(-1)^{2n} = 1$ is a $2n^{th}$ root of unity

We will now show $\nexists$ any more in any of these fields.

Let $a, b \in \mathbb{Q}$. ATC $\exists$ a n^{th} root of unity.

So $(a+b\sqrt{11})^n = 1$ $(b \neq 0)$

$\Rightarrow (a+b\sqrt{11}) = 1$

$\Rightarrow \sqrt{11} = \frac{1-a}{b}$ $\rightarrow\leftarrow$

If $b=0$ then $(a)^n = 1$ only true for $a = \pm 1$.

$\therefore \nexists$ any more roots of unity in $\mathbb{Q}(\sqrt{11})$.

//

1999 C3

Prove or disprove.

The polynomial $X^{625} - X - 1$ is irreducible over $\mathbb{Z}_5$.

False.

Suppose $X^{5^4} - X - 1$ is irreducible.

Let α be a root of $f(X) = X^{5^4} - X - 1$

(Lang pg 246) Frobenius mapping — we know $\phi(X) = X^5$ generates the Galois group of $\overline{\mathbb{Z}_5}$ (which is the splitting field of f)

Since the Galois group permutes roots, pick β to be another root of f.

so $\beta = \phi^k(\alpha) = \alpha^{5^k}$

Since α is a root of f

$$\alpha^{5^4} - \alpha - 1 = 0$$

so $\alpha^{5^4} = \alpha + 1$.

raising both sides to 5^4 we get

$$\alpha^{5^4 \cdot 2} = (\alpha+1)^{5^4} = \alpha^{5^4} + 1 = \alpha + 2$$

Likewise,

$$\alpha^{5^4 \cdot 3} = \alpha + 3$$

$$\alpha^{5^4 \cdot 4} = \alpha + 4$$

$$\alpha^{5^4 \cdot 5} = \alpha$$

$\Rightarrow$ f has at most $5(4) = 20$ roots $\rightarrow\leftarrow$ since $20 < 625$

Thus $f = X^{625} - X - 1$ is reducible //

1999 C4

Prove or disprove.

4) Let F be a degree 4 ext of $\mathbb{Q}$. If any proper subfield of F is Galois over $\mathbb{Q}$, then F is Galois over $\mathbb{Q}$.

False

disprove:

consider $F = \mathbb{Q}(\sqrt[4]{2})$ and $E = \mathbb{Q}(\sqrt{2})$

$E/\mathbb{Q}$ is Galois b/c

E is the splitting field for $X^2 - 2$ (normal) and roots are distinct (separable)

But $F/\mathbb{Q}$ is not Galois b/c

It fails to be a normal ext since $X^4 - 2 \in \mathbb{Q}[X]$ is irred over $\mathbb{Q}$ and F contains a root of $X^4 - 2$ but $X^4 - 2$ does not split in F (since $\exists$ complex roots).

//

1999 C5

prove/disprove

5) For field ext, being separable (resp p.i) is transitive. (ie 

$\Rightarrow$ ✓.

True:

Pf:

Let $K \subseteq F \subseteq E$.

separable:

Let E/F and F/K be separable.

If E/K is finite then we are done by L. Cor 4.2

If E/K is infinite, Let $\alpha \in E$.

Then α is sep over F.

Let $f(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + X_n = \text{irr}(\alpha, F, X)$.

So we have $K \subseteq K(a_0, \ldots, a_{n-1}) \subseteq K(a_0, \ldots, a_{n-1}, \alpha)$

and each step is sep since.

$\rightarrow K(a_0, \ldots, a_{n-1})$ is sep over K since F/K is sep and $a_i \in F$.

$\rightarrow \alpha$ is sep over $K(a_0, \ldots, a_{n-1})$ b/c α is sep over F & $a_i \in F$.

Then $K(a_0, \ldots, a_{n-1}, \alpha)$ is sep over K.

Hence α is sep over K. This since α arbitrary and $\alpha \in E$ then E/K is sep.

p.i:

Let E/F and F/K be p.i.

$\Rightarrow [E:F]_s = 1$ and $[F:K]_s = 1$

$\Rightarrow [E:K]_s = [E:F]_s [F:K]_s = 1$

$\Rightarrow E/K$ is p.i. //

1998

Part C.

F will always denote an extension field of K.

1. (a) Let $u \in F$ be an element of odd degree over K, prove that $K(u) = K(u^2)$.
   (b) Compute the Galois group of $x^3 - x - 1$ over $\mathbf{Q}$.
   (c) If $f \in K[x]$ has degree n and F is its splitting field prove that $[F : K]$ divides $n!$.

2. Prove that $\mathrm{Aut}_K K(x)$ is finite. Deduce that if K is finite then $K(x)$ is not a Galois extension. Determine the closed subgroups of $\mathrm{Aut}_K K(x)$ when K is infinite.

3. Prove that in a finite field of characteristic p, every element has a unique p-th root in it. If F is a finite extension of a finite field K of characteristic p, prove that $\mathrm{Aut}_K F$ is cyclic.

4. Let F be an algebraically closed extension of K of finite transcendence degree, prove that every K-monomorphism of F to itself is actually an automorphism. Give an example of a field extension which is transcendental of finite degree and give an example of a field extension of infinite transcendental degree.

spring 1998

1997

Part C.

1. (i) Define separable extension, perfect field.
   (ii) Give an example of an imperfect field.
   (iii) Prove that every finite field is perfect.

2. Prove from scratch that every finite field admits algebraic extensions of arbitrarily large degree.

3. State and prove the theorem on the primitive element.

4. Let $K \subset E \subset F$ be fields. Prove or disprove.
   (i) If F is Galois over K, then F is Galois over E.
   (ii) If F is Galois over K, then E is Galois over K.
   (iii) If F is Galois over E and E is Galois over K, then F is Galois over K.

5. Compute the Galois group of $X^4 - 5$ over $\mathbf{Q}$.

Spring 1997

1996

Part C.

1. Suppose E is a Galois extension field of degree 7 over F. What can you say about a group of automorphisms of E whose elements fix each element of F? Prove your answer.

2. Let E be the field obtained from the rationals $\mathbf{Q}$ be adjoining a cube root of 3. Determine the Galois group of E (over $\mathbf{Q}$).

3. Let f be a polynomial of degree n over F and let E be a splitting field of f over F. Prove that the degree of E over F is at most $n!$.

4. What can you say about the cardinality of an algebraic closure of the field of 3 elements? Sketch a proof of your answer.

5. Let F be a field of 4 elements. Prove that there exists an extension field of degree 2 over F.

spring 1996

1995

Part C.

1. Let $\alpha = \sqrt{2+\sqrt{2}}$.

   (a) Find the minimum polynomial of α over $\mathbf{Q}$. What are its other roots?

   (b) Prove that $\mathbf{Q}(\alpha)$ is the splitting field of α over $\mathbf{Q}$.

   (c) Write down all the automorphisms of $\mathbf{Q}(\alpha)$ over $\mathbf{Q}$.

   (d) Prove that the Galois group of $\mathbf{Q}(\alpha)/\mathbf{Q}$ is cyclic.

   (e) Determine the intermediate fields of the extension $\mathbf{Q} \subset \mathbf{Q}(\alpha)$.

2. (a) Let p be a prime and let $F = \mathbf{Z}_p$. Determine the number of irreducible polynomials of type $x^2 + cx + d$ where $c, d \in F$.

   (b) Let $f(x)$ be one of the polynomials described in (a). Prove that $K = F[x]/(f)$ is a field containing p^2 elements and that the elements of K form $a + b\alpha$ where $a, b \in F$ and α is a root of f in K. Prove also that every such element $a + b\alpha$ with $b \neq 0$ is a root of an irreducible quadratic polynomial in $F[x]$.

   (c) Show that every polynomial of degree 2 in $F[x]$ has a root in K. (Hint: Any two fields containing p^2 elements are isomorphic).

3. Determine the splitting field of the polynomial $f(x) = (x^2 - 2x - 1)(x^2 - 2x - 7)$.

Spring 1995

1994(Feb)

Part C.

1. Let $K \subseteq F$ be fields and $a, b \in F$ algebraic over K.

   (a) State and prove an upper bound for the degree of the product ab over K.

   (b) Give an example showing your bound is sharp.

2. Let F be a field and $\sigma \in \mathrm{Aut}(F)$. Let $K = \{u \in F : \sigma(u) = u\}$.

   (a) Prove that K is a field.

   (b) If $\sigma^n = \mathrm{id}$ and $\sigma^k \neq \mathrm{id}$ for $k < n$, prove $[F : K] = n$.

3. Determine the irreducible factorization and Galois group of the polynomial $X^{16} - X$

   (a) over $\mathbf{F}_4$.

   (b) over $\mathbf{F}_8$.

4. (a) Define Galois extension.

   (b) Let K be a subfield of the complex numbers which is a Galois extension of $\mathbf{Q}$, the rationals. Prove or disprove that complex conjugation takes K onto itself and defines an automorphism of K.

5. Assume π is a transcendental number.

   (a) Show $X^3 + \pi X + 6$ is irreducible over $\mathbf{Q}(\pi)$.

   (b) Determine the Galois group of $X^3 + \pi X + 6$ over $\mathbf{Q}(\pi)$.

1993

Part C.

1. (a) Define: simple algebraic extension F/K of fields.
   (b) Show that if F/K is a simple algebraic extension of degree n then $|\operatorname{Aut}_K(F)| \leqslant n$.
   (c) Give an example of a simple algebraic extension F/K where $|\operatorname{Aut}_K(F)| < n$.

2. Assuming that e is transcendental over the rationals $\mathbf{Q}$, prove that so is $e + \sqrt{2}$.

3. Let F be a finite field and F_1, F_2 subfields of F. State and prove a formula for $|F_1 \cap F_2|$ in terms of $|F_1|$ and $|F_2|$.

4. Compute the Galois group of $X^3 + 3$ over $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{Z}_7$.

5. Prove or disprove that the degree of the splitting field of a polynomial of degree n divides $n!$.

1995

Part A.

1. Define normal subgroup. Give an example of a subgroup that is normal and one that is not.

2. Let G operate on the set S, and suppose that $s, t \in S$ are in the same orbit under the operation. Show that the isotropy groups G_s and G_t are conjugate. That is, there exists $g \in G$ such that $g^{-1}G_s g = G_t$. (Recall that $G_s = \{g \in G : gs = s\}$).

3. Let p be a prime integer and let G be a finite p-group. Show that G has a nonzero center.

4. Let G be a finite group of order $p^n q$, p and q primes with $p > q$. Show that G is not simple.

5. Show that every group of order p^2, p a prime, is abelian.

6. Let p be a prime integer and let $Z(p^\infty)$ be the subgroup of the additive group $\mathbf{Q}/\mathbf{Z}$ generated by the cosets of the form $1/p^i$, $i \in \mathbf{Z}$, $i \geqslant 0$. Let A be a subgroup of a finitely generated group B. Show that any homomorphism $f : A \to Z(p^\infty)$ extends to a homomorphism $g : B \to Z(p^\infty)$.

Fall 1994 2004

1995 A3

If $|G| = p^n$ for some prime p, then the center of G is nontrivial center.

Pf:

Consider the grp action $\phi: G \times G \to G$ by conjugation
$(g, x) \mapsto gxg^{-1}$

This is a grp action b/c

$\phi(e, x) = exe^{-1} = x$

$\phi(g_1 g_2, x) = (g_1 g_2) x (g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1}$
$= g_1 \phi(g_2 x) g_1^{-1}$
$= \phi(g_1, g_2 x)$

Define $X_0 = \{x \in G \mid gxg^{-1} = x \ \forall\ g \in G\} = C(G)$

since $[G : C_G(x_i)] > 1$ and $p \mid |G|$ then we get the class equation:

$$|G| = |C(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$$

So $[G : C_G(x_i)] \geq 2$ and $G : C_G(x_i)] \mid |G|$

but the only prime that divides $|G|$ is p so

$[G : C_G(x_i)] = p^k$ for some $k \geq 0$.

If $k = 0$, then $[G : C_G(x_i)] = 1 \to \leftarrow$

thus $p \mid [G : C_G(x_i)]$.

also recall $p \mid |G|$, so $p \mid |C(G)|$

thus $|C(G)| \neq 1$.

So $C(G)$ contains more then one elmt. //

1995 A5

Every group of order p^2, where p is some prime is abelian.

Pf:

Let $|G| = p^2$

Since $C(G) \leq G$ then by Lagranges thm

$|C(G)| = 1, p, p^2$.

Note, $|G/C(G)| = |G|/|C(G)| =: \frac{p^2}{1}, \frac{p^2}{p}, \frac{p^2}{p^2}$

$=: p^2, p, 1$.

Case 1:

$|G/C(G)| = 1$

so $|C(G)| = p^2 \Rightarrow G = C(G)$

but $C(G)$ abelian $\Rightarrow G$ is abelian.

Case 2:

$|G/C(G)| = p$

so $G/C(G)$ is cyclic $\Rightarrow$ by $G/C(G)$ thm that G is abelian.

Case 3:

$|G/C(G)| = p^2$

$\Rightarrow |C(G)| = 1$ so $C(G) = \{e\}$

$\rightarrow\leftarrow$ b/c the center of a nontrivial finite p-group G contains more than one elmt.

thus G abelian. //

1994 (September)

Part A.

1. Describe all groups G which contain no proper subgroup.

2. Let G be a cyclic group of order n and H a cyclic group of order m. Describe all homomorphisms from G to H.

3. (a) Prove that every subgroup of index 2 is normal.
   (b) Give an example of a subgroup of index 3 in a group G which is not normal. (Hint: Take G to be of order 6).

4. Prove that a group G of order 244 cannot be simple. (Hint Show by counting that if G has more than one Sylow 2-subgroup, then it has only one Sylow 7-subgroup).

5. For which integers $\geqslant 5$ is the cyclic subgroup of the symmetric group S_n generated by $(1,2,3,4,5)$ a normal subgroup of S_n?

1994 (sept) A2

Let G be a cyclic group of order n and H a cyclic group of order m. Describe all homom from G to H.

Pf:
Since $|G|=n$ and G cyclic then $G \cong \mathbb{Z}_n$.
Since $|H|=m$ and H cyclic then $H \cong \mathbb{Z}_m$.
We will show $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_{(n,m)}$.
Let $d=\gcd(m,n)$.

Define $\Phi: \mathbb{Z}_d \longrightarrow \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$

$$k \longmapsto (\phi_k : \mathbb{Z}_n \to \mathbb{Z}_m) \quad (1 \longmapsto k\tfrac{m}{d})$$

note: we can do this bc homom between cyclic groups are determined by where 1 goes.

First we will show Φ is a homom.

Let $k, \ell \in \mathbb{Z}_d$.

So $\Phi(k+\ell) = \phi_{k+\ell} = (k+\ell)\frac{m}{d} = k\frac{m}{d} + \ell\frac{m}{d} = \phi_k + \phi_\ell = \Phi(k)+\Phi(\ell)$

so Φ is a homom.

Next show Φ injective.

Let $\Phi(k_1) = \Phi(k_2)$, so $\phi_{k_1} = \phi_{k_2} \Rightarrow k_1\frac{m}{d} = k_2\frac{m}{d}$

so $(k_1 - k_2)\frac{m}{d} \equiv 0 \bmod m$

$\Rightarrow \frac{k_1-k_2}{d} \in \mathbb{Z} \Rightarrow d \mid k_1 - k_2$

$\Rightarrow k_1 = k_2$ in $\mathbb{Z}_d$. So Φ injective.

Now show Φ surjective.

Let $\psi \in \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ s.t. $\psi(1) = s$.

well, $\psi(0) = 0 \bmod m$ and $\psi(n) = sn$

but $\psi(0) = \psi(n)$ (since working mod n inside)

thus $\psi(0) = \psi(n) = sn \equiv 0 \bmod m$. $\Rightarrow m \mid sn$

So the prime factors of m which don't divide n, are of the form $\frac{m}{d}$, and they must divide s.

Thus $\frac{m}{d} \mid s \Rightarrow s = k\frac{m}{d}$ for some $k \in \mathbb{Z}$.

Thus Φ is surjective.

Therefore Φ is an isomorphism. //

1994 (February)

Part A.

1. Give an example of a polynomial $p(x) \in \mathbf{Z}_{10}[x]$ of degree n for some n which has more than n zeros. Can you give an example of such a polynomial in $\mathbf{Z}_{13}[x]$? Explain your answer.

2. (a) Find all the subgroups of $\mathbf{Z}_{18}$.
   (b) Find all the ideals in the ring $\mathbf{Z}_{18}$.
   (c) Which of these ideals are maximal and which are prime?

3. Prove that every group of order 45 has a normal subgroup of order 9.

4. Let G be a group of order p^n. Assume that the center $Z(G)$ has order $\geqslant p^{n-1}$. Prove that G is abelian.

5. Let G be a finite group and let N be a normal subgroup of G. Let $\varphi : G \to G/N$ be the canonical homomorphism. If H is a subgroup of order G/N prove that $\varphi^{-1}(H)$ is a subgroup of order $|H||N|$.

1994 (Feb) A4

Let G be a group of order p^n for some prime p. Assume that the center of G has order greater than or equal to p^{n-1}. Prove that G is abelian.

Pf:

Let $|G| = p^n$. Let $|C(G)| \geq p^{n-1}$.

since $C(G) \leq G$ then $|C(G)| \mid |G|$

thus $|C(G)| = p^{n-1}$ or $|C(G)| = p^n$.

If $|C(G)| = p^{n-1}$ consider, $|G/C(G)| = |G|/|C(G)| = p^n/p^{n-1} = p$

Since any group of prime order is cyclic then $G/C(G)$ is cyclic thus by the $G/C(G)$ thm G is abelian.

If $|C(G)| = p^n$ then $C(G) = G$ thus G is abelian. //

1993

Part A.

1. Prove that every group of order 15 is cyclic.

2. Recall that the commutator subgroup of a group G is the subgroup G' generated by teh elements $aba^{-1}b^{-1}$ where $a, b \in G$.

   (i) Prove that $G' \trianglelefteq G$ and that G/G' is abelian.

   (ii) If $G = S_4$ prove that $G' = A_4$. Find the commutator subgroup of A_4.

3. Show that the group generated by the two elements a, b with relations $a^3 = 1$, $b^2 = 1$, $ba = a^2b$ is isomorphic to S_3.

4. Find the number of orbits in $\{1, 2, 3, 4, 5, 6, 7, 8\}$ under the action of the subgroup of S_8 generated by $(1, 3)$ and $(2, 4, 7)$.

5. Let R be the ring $\mathbf{Z}_6$ and $S = \{1, 2, 4\}$. Prove that $S^{-1}R$ is a field and identify the field. If $T = \{1, 3\}$, is $T^{-1}R$ a field?

6. Let R be a local ring and $f : R \to R'$ a surjective ring homomorphism. Prove that R' is local.

7. Let R be an integral domain and X an indeterminate over R. Show that for $a, b \in R$, a a unit of R, $X \mapsto aX + b$ extends to an automorphism of $R[X]$ which is the identity on R. Calculate the inverse of this automorphism.

201B CUMULATIVE GREENSTEIN FINAL (2013, 2011, 2007)

(1)

(a) **[2013:i]** Let R be a domain (a commutative unital ring without zero divisors) and let

$$0 \to M \to M' \to M'' \to 0$$

be a short exact sequence of R-modules. Prove that M' is torsion if and only if both M and $M''$are torsion. Which, if any, parts of this statement remains true if "torsion" is replaced with "torsion free"?

(b) **[2013:ii, 2011:i]** Suppose that

$$0 \to M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \to \cdots \xrightarrow{f_{n-1}} M_n \to 0$$

$$0 \to M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots \xrightarrow{f_{r-1}} M_r \to 0,$$

$r > n$, are exact sequences of R-modules for some ring R. Then

$$0 \to M_0 \xrightarrow{f_0} M_1 \to \cdots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_n f_{n-1}} M_{n+1} \xrightarrow{f_{n+1}} \cdots \xrightarrow{f_{r-1}} M_r \to 0$$

is exact (the resulting sequence of length $r+1$ is called the cup product of the sequences of length $n+1$ and $r-n+1$, respectively).

- **[2007:1]** Suppose that $0 \to A \xrightarrow{\iota} B \xrightarrow{f} C \to 0$ and $0 \to C \xrightarrow{g} D \xrightarrow{\pi} E \to 0$ are short exact sequences of modules. Then

$$0 \to A \xrightarrow{\iota} B \xrightarrow{gf} D \xrightarrow{\pi} E \to 0$$

is exact.

(c) **[2013:iii, 2011:iii]** Let

$$0 \to V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} V_2 \to \cdots \xrightarrow{f_{n-1}} V_n \to 0$$

be an exact sequence of finite dimensional vector spaces over a division ring D. Prove that

$$\sum_{k=0}^{n} (-1)^k \dim_D V_k = 0.$$

(d) **[2011:ii]** Cup product is "surjective" in the sense that every sequence of length $r > 2$ can be obtained by taking cup product of two sequences of length $n+1$ and $r-n+1$ for some $1 < n < r$.

(2) **[2013, 2011, 2007]** In these exercises, all proofs must be written in the module- and ring-theoretic language.

(a) **[2013:i, 2011:ii, 2007:iii]** Describe the $\mathbb{Z}$-module dual $\mathbb{Q}^*$ of $\mathbb{Q}$.

(b) **[2013:ii, 2011:iii, 2007:iv]** Use the short exact sequence induced by the canonical inclusion $\mathbb{Z} \to \mathbb{Q}$ to prove that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ as a $\mathbb{Z}$-module.

(c) **[2013:iii, 2011:iv, 2007:v]** Determine, with a proof, whether $\mathbb{Q}$ is projective as a $\mathbb{Z}$-module.

(d) **[2013:iv, 2011:v, 2007:vi]** Let K be a field. Which, if any, of these statements can be modified so that they hold if we replace $\mathbb{Z}$ by the ring $K[x]$ and $\mathbb{Q}$ by its field of fractions $K(x)$?

(e) **[2013:v]** Let M be a right R-module, N be a left R-module and let M' (respectively, N') be a submodule of M (respectively, N). Prove $M/M' \otimes_R N/N' \cong (M \otimes_R N)/(M \otimes_R N' + M' \otimes_R N)$.

(f) **[2013:vi]** Let M, M' be right R-modules, N, N' be left R-modules. Let $f \in \mathrm{Hom}_R(M, M')$, $g \in \mathrm{Hom}_R(N, N')$. Is it always true that $\ker(f \otimes g) = M \otimes_R \ker g + \ker f \otimes_R N$? Prove or provide a counterexample.

(g) **[2011:i, 2007:i]** Determine, with a proof, whether $\mathbb{Q}$ is free as a $\mathbb{Z}$-module.

(h) **[2007:ii]** Prove that $\mathbb{Q}$ is generated by the set $\{p^{-a} : p \text{ prime}, a > 0\}$ as a $\mathbb{Z}$-module.

(3) **[2013, 2011]** Let R be a commutative unital ring. Given $a \in R$, let $\mathrm{ev}_a : R[x] \to R$ be the evaluation homomorphism which is uniquely determined by $\mathrm{ev}_a(r) = r$ for all $r \in R$ and $\mathrm{ev}_a(x) = a$. Recall that a homomorphism of rings $\varphi : R \to S$ extends to a homomorphism of rings $\bar{\varphi} : \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(S)$ defined by $(a_{ij}) \mapsto (\varphi(a_{ij}))$.

- **[2007]** Let R be a commutative unital ring, $\mathrm{ev}_0 : R[x] \to R$ the evaluation homomorphism which is uniquely defined by $\mathrm{ev}_0(r) = r$ for all $r \in R$, $\mathrm{ev}_0(x) = 0$.

(a) **[2013:i]** Let $\Lambda \subset R$ be a multiplicative set (that is, $\lambda_1, \lambda_2 \in \Lambda$ implies $\lambda_1 \lambda_2 \in \Lambda$). Prove that $\Lambda^{-1}M = 0$ if and only if $\mathrm{Ann}_R m \cap \Lambda \neq \emptyset$ for all $m \in M$.

(b) **[2013:ii]** Prove that an epic homomorphism between free R-modules of the same *finite* rank is an isomorphism.

(c) **[2013:iii]** Let $\varphi : R \to S$ be a homomorphism of commutative unital rings. Show that for any $A \in \mathrm{Mat}_n(R)$, $\varphi(\det(A)) = \det(\bar{\varphi}(A))$.

- **[2011:i, 2007:ii]** Show that for all $r \in R$, $D \in \mathrm{Mat}_n(R[x])$, $\mathrm{ev}_r(\det D) = \det(\mathrm{ev}_r(D))$.

(d) **[2013:iv, 2011:iii-iv]** Let $A \in \mathrm{Mat}_n(R)$. Show that $\det(A^a) = \det(A)^{n-1}$ and $(A^a)^a = (\det(A))^{n-2} A$. *The ring R is **not** assumed to be a domain!*

- **[2007:3iv]** Let $A \in \mathrm{Mat}_n(R[x])$. Show that $(A^a)^a = (\det(A))^{n-2} A$.

(e) **[2011:ii, 2007:iii]** Let $A \in \mathrm{Mat}_n(R)$ and set $C = xI_n - A \in \mathrm{Mat}_n(R[x])$. Prove that $A^a = (-1)^{n-1}\mathrm{ev}_0(C^a)$, where A^a is the adjoint matrix of A in $\mathrm{Mat}_n(R)$ and C^a is the adjoint matrix of C in $\mathrm{Mat}_n(R[x])$.

(f) **[2011:v, 2007:v]** Use the identity $CC^a = C^aC = \det(C)I_n$ in $\mathrm{Mat}_n(R[x])$ to prove Cayley-Hamilton theorem ($p_A(A) = 0$) over an arbitrary commutative unital ring R.

(g) **[2007:i]** Prove that ev_0 extends to a homomorphism of rings $\mathrm{Mat}_n(R[x]) \to \mathrm{Mat}_n(R)$.

(4)

(a) **[2013:i, 2011:i, 2007:i]** Find the invariant factors of the matrix

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 0 \\ 3 & 0 & 0 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{Q}).$$

(b) **[2013:ii]** List all possible sets of invariant factors for a matrix $B \in \mathrm{Mat}_6(\mathbb{Q})$ with the *minimal* polynomial $(x-2)^2(x^2+1)$.

(c) **[2013:iii]** List all possible Jordan canonical forms for the matrix $B \in \mathrm{Mat}_6(\mathbb{C})$ with the *characteristic* polynomial $(x-2)^2(x^2+1)^2$ (up to permutations).

- **[2011:iii, 2007:iii]** List all possible Jordan canonical forms for the matrix $B \in \mathrm{Mat}_6(\mathbb{C})$ with the *minimal* polynomial $(x-2)^2(x^2+1)$ (up to permutations).

(d) **[2013:iv, 2011:iv]** Let K be a field. Show that $K[x]/(x^2)$ is an indecomposable $K[x]$-module while $K[x]/(x^2-1)$ is a direct sum of two indecomposable modules (which are isomorphic as K-vector spaces but not as $K[x]$-modules).

(e) **[2011:ii, 2007:ii]** List all possible rational canonical forms for a matrix $B \in \mathrm{Mat}_6(\mathbb{Q})$ with the minimal polynomial $(x-2)^2(x^2+1)$ (up to permutations).

(5) **[2013, 2011]** Let R be a ring, M be an R-module. Then $\mathrm{End}_R M$ is a unital ring (a priori, non-commutative). Note that if S is a subring of R and M is an R-module, $\mathrm{End}_R M$ is a subring of $\mathrm{End}_S M$.

(a) **[2013:i 2011:i]** Describe the natural $\mathrm{End}_R M$-module structure on M.

(b) **[2013:ii, 2011:iii]** Suppose that if $f \in \mathrm{End}_R M$ is not invertible, then $1_M - f$ is invertible. Then M is indecomposable.

(c) **[2013:iii, 2011:iv]** If D is a division ring and V is a (left) D-vector space, prove that V is simple as a module over the ring $S = \mathrm{End}_D V$. Does this remain true for a free module M over a unital ring R?

(d) **[2013:iv]** Let D be a division ring, V be a left D-vector space and $R = \mathrm{End}_D V$. Then $\mathrm{End}_R V \cong D$.

- **[2011:v]** Let D be a division ring, V be a finite dimensional left D-vector space and $R = \mathrm{End}_D V$. Then $\mathrm{End}_R V$ is isomorphic to the center of D. [*Hint.* Identify $\mathrm{End}_R V$ with a subring of R and recall that $R \cong \mathrm{Mat}_n(D^{op})$]

(e) **[2011:ii, 2007:iii]** M is decomposable if and only if $\mathrm{End}_R M$ contains a non-trivial idempotent (that is, there exists $f \in \mathrm{End}_R M$, $f \neq 0, 1_M$ such that $f^2 = f$).

(6) **[2007:5]** Let R be a ring, M be a finite length R-module. Then $\mathrm{End}_R M$ is a ring (a priori, non-commutative).

(a) **[2007:5i]** Prove that M is a finite direct sum of indecomposable modules. [*Hint.* Use induction on length.]

(b) **[2007:5ii]** Prove that if M is indecomposable then $\mathrm{End}_R M$ is a local ring, that is, has a unique maximal ideal. You may use the part of Fitting Lemma proved in class.

(c) **[2007:5iii]** ~~Prove that M is decomposable if and only if $\mathrm{End}_R M$ contains a non-trivial idempotent (that is, there exists $f \in \mathrm{End}_R M$, $f \neq 0, 1_M$ such that $f^2 = f$).~~ **[See 5e]**

(d) **[2007:5iv]** Prove the converse of the statement in (ii) [*Hint.* If $f \in \mathrm{End}_R M$ is a non-trivial idempotent, then so is $1_M - f$].

(e) **[2007:5v]** Do we need M to be finite length in (iii) and (iv)?

(7) **[2007:6]** Given a ring S, denote its center by $Z(S)$ (that is, $Z(S) = \{a \in R : ar = ra \ \forall\, r \in R\}$). Prove that $Z(\mathrm{Mat}_n(R)) \cong Z(R)$.

F-201B

(1)

(a) Let R be a domain (a commutative unital ring w/o zero divisors) and let $0 \to M \xrightarrow{f} M' \xrightarrow{g} M'' \to 0$ be a short exact sequence of R-modules. Prove that M' is torsion if and only if both M and M'' are torsion. Which if any parts of this statement can be replaced with "torsion free"?

Pf:

Torsion:

($\Rightarrow$) Let M' be torsion. Since f is ~~injective~~ monic, we know M is isomorphic to a submodule of M'.
Since a submodule of a torsion module is torsion $\Rightarrow$ M is torsion.
Let $m'' \in M''$, since g is ~~surjective~~ epic, $\exists\ m' \in M'$ s.t. $g(m') = m''$
if $r \in \mathrm{Ann}_R m'$
$\Rightarrow r m'' = r g(m') = g(rm') = g(0) = 0$
$\Rightarrow 0 \neq \mathrm{Ann}_R m' \subseteq \mathrm{Ann}_R m''$ Thus M'' is torsion.

($\Leftarrow$) Suppose M and M'' are torsion.
Let $m' \in M' \setminus \{0\}$.
if $g(m') = 0 \Rightarrow m' \in \ker g = \mathrm{Im} f$
otherwise $\exists$ a $r \in R \setminus \{0\}$ s.t. $0 = r\, g(m') = g(rm')$
In both cases, $sm' \in \mathrm{Im} f$ for $s \in R \setminus \{0\}$
$\Rightarrow sm' = f(m)$ for some $m \in M$.
Since m is torsion, $\exists\ 0 \neq s' \in \mathrm{Ann}_R m$
$\Rightarrow s'sm' = s' f(m) = f(s'm) = f(0) = 0$
Thus $s's \in \mathrm{Ann}_R m'$
Since R is a domain, $s, s' \neq 0 \Rightarrow ss' \neq 0$
$\Rightarrow \mathrm{Ann}_R m' \neq 0$
Thus M' is torsion. //

Torsion Free

If M and M'' are torsion free then M' is torsion free.

Pf:

Let $m' \in M'$ and suppose $rm' = 0$ for $r \in R \setminus \{0\}$

so $g(rm') = g(0) = 0$ but $g(rm') = rg(m')$

s.o $0 = rg(m')$

Since M'' is torsion free $\Rightarrow g(m') = 0$

$\Rightarrow m' \in \ker g = \text{Im } f$

$\Rightarrow \exists \ m \in M$ s.t. $f(m) = m'$

Now $0 = rm' = r f(m) = f(rm)$

Since f is monic, $rm = 0 \Rightarrow m = 0$ since M is torsion free

$\Rightarrow f(m) = f(0) = 0 = m'$.

thus M' is torsion free. //

If M' is torsion free then M is torsion free.

(relays on f being ~~injective~~ monic)

similar to proof of torsion $\Leftrightarrow$

However M'' does not need to be torsion free

ex: Let $I \subseteq R$ be an ideal

$$0 \to I \xrightarrow{f} R \xrightarrow{g} R/I \to 0$$

this is an example where R & I are torsion free, but R/I is torsion

//

(b) Suppose that $0 \to M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \to \cdots \xrightarrow{f_{n-1}} M_n \to 0$ and

$0 \to M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots \xrightarrow{f_{r-1}} M_r \to 0 \quad r > n$

are exact sequences of R-modules for some ring R.

Then $0 \to M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_n f_{n-1}} M_{n+1} \xrightarrow{f_{n+1}} \cdots \xrightarrow{f_{r-1}} M_r \to 0$

is exact.

Pf:

NTS $\operatorname{Im} f_{n-2} = \ker f_n f_{n-1}$ and $\operatorname{Im} f_n f_{n-1} = \ker f_{n+1}$

Since f_n is injective then $\ker f_n = 0$

$\Rightarrow \ker f_n f_{n-1} = \ker f_{n-1}$

$= \operatorname{Im} f_{n-2}$ by exactness of first sequence

Since f_{n-1} is surjective then $\operatorname{Im} f_{n-1} = M_n$

$\Rightarrow \operatorname{Im} f_n f_{n-1} = \operatorname{Im} f_n$

$= \ker f_{n+1}$ by exactness of 2nd sequence

//

note:

Similar argument for

suppose that $0 \to A \xrightarrow{i} B \xrightarrow{f} C \to D$ and

$0 \to \overset{C}{\underset{D}{\bullet}} \xrightarrow{g} B \xrightarrow{\pi} E \to 0$ are short exact sequence

of modules. Then $0 \to A \xrightarrow{i} B \xrightarrow{gf} D \xrightarrow{\pi} E \to 0$

is exact.

c) Let $0 \to V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} V_n \to 0$ be an exact sequence of f.d. v.s. over a division ring D. Prove $\sum_{k=0}^{n} (-1)^k \dim_D V_k = 0$.

Pf:

Note: $\dim_D V_k = \dim_D \ker f_k + \dim_D \operatorname{Im} f_k$

Thus,

$$\sum_{k=0}^{n} (-1)^k \dim_D V_k = \sum_{k=0}^{n} (-1)^k \left(\dim_D \ker f_k + \dim_D \operatorname{Im} f_k \right)$$

$$= \sum_{k=0}^{n} (-1)^k \dim_D \ker f_k + \sum_{k=0}^{n} (-1)^k \dim_D \operatorname{Im} f_k$$

by exactness $\ker f_0 = 0$ and $\operatorname{Im} f_n = 0$, so

$$= \sum_{k=1}^{n} (-1)^k \dim_D \ker f_k + \sum_{k=0}^{n-1} (-1)^k \dim_D \operatorname{Im} f_k$$

$$= \sum_{k=0}^{n-1} (-1)^{k+1} \dim_D \ker f_{k+1} + \sum_{k=0}^{n-1} (-1)^k \dim_D \operatorname{Im} f_k$$

by exactness $\operatorname{Im} f_k = \ker f_{k+1}$

$$= \sum_{k=0}^{n-1} (-1)^{k+1} \dim_D \ker f_{k+1} + \sum_{k=0}^{n-1} (-1)^k \dim_D \ker f_{k+1}$$

$$= (-1) \sum_{k=0}^{n-1} (-1)^k \dim_D \ker f_{k+1} + \sum_{k=0}^{n-1} (-1)^k \dim_D \ker f_{k+1}$$

$$= 0.$$

//

(d) Cup product is surjective in the sense that every sequence of length $r>2$ can be obtained by taking cup products of two sequences of length $n+1$ and $r-n+1$ for some $1<n<r$.

Pf:

Let $0 \to M_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{r-1}} M_r \to 0$ be exact.

Consider $0 \to M_1 \xrightarrow{f_1} \cdots \to M_{n-1} \xrightarrow{\overline{f_{n-1}}} \operatorname{Im} f_{n-1} \to 0$ and

$0 \to \operatorname{Im} f_{n-1} \xrightarrow{i} M_n \xrightarrow{f_n} \cdots \xrightarrow{f_{r-1}} M_r \to 0$

where i is the natural inclusion.

Clearly, $\operatorname{Im} i = \ker f_n$ due to exactness ($\ker f_n = \operatorname{Im} f_{n-1}$)

also $f_{n-1} : M_{n-1} \to M_n$ gives a surjective morphism

$\overline{f_{n-1}} : M_{n-1} \to \operatorname{Im} f_{n-1}$.

Finally, $i \circ \overline{f_{n-1}} = f_{n-1}$ and so the cup product of the above sequence is equal to the original sequence. //

F-201B

(2)

(a) Describe the $\mathbb{Z}$-module dual $\mathbb{Q}^*$ of $\mathbb{Q}$.

Recall $\mathbb{Q}^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$

Pf: claim $\mathbb{Q}^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$ (zero map).

ATC $f \in \mathbb{Q}^*$ s.t. $f(x) \neq 0$ for some $x \in \mathbb{Q}$.

Let $p \in \mathbb{Z}$ be prime s.t. $p \nmid f(x)$.

So $f(x) = f\left(\frac{px}{p}\right) = pf\left(\frac{x}{p}\right)$ (b/c $p \in \mathbb{Z}$ & $\mathbb{Z}$-mod)

$\Rightarrow p \mid f(x)$ $\rightarrow\leftarrow$

Thus $f = 0$

Hence $\mathbb{Q}^* = 0$. //

(b) Use the short exact sequence induced by the canonical inclusion $\mathbb{Z} \to \mathbb{Q}$ to prove that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$ as a $\mathbb{Z}$-module.

Pf:

Consider the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

Since $\mathbb{Q}$ is flat (preserves 1-1 & surjectivity) as a $\mathbb{Z}$-module, we get the following exact sequence.

tensoring gives right exactness so preserves surjectivity

$$0 \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow 0$$

so flat preserves exactness

note: tensoring preserves surjectivity (so w/ flat we have an exact sequence still)

If we show $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, then we would have

$$0 \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to 0 \to 0$$

So $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.

But $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$ (Thm)

Thus $\mathbb{Q} \simeq \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Thus it suffices to show $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$

But this is a special case of the following statement.

If A is a torsion $\mathbb{Z}$-module then $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$

Pf: Let $a \in A$, $x \in \mathbb{Q}$.

Since A is torsion, $\exists\ k \in \mathbb{Z} \setminus \{0\}$ s.t. $ka = 0$.

$$\to a \otimes x = a \otimes \left(\frac{kx}{k}\right) = ka \otimes \frac{x}{k} = 0 \otimes \frac{x}{k} = 0.$$

$$\Rightarrow A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$$

Therefore since $\mathbb{Q}/\mathbb{Z}$ is a torsion $\mathbb{Z}$-module,

$\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, hence $\mathbb{Q} \simeq \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$. //

(c) Determine, with a proof, whether $\mathbb{Q}$ is projective as a $\mathbb{Z}$-module.

Pf:

Since $\mathbb{Z}$ is a PID, then $\mathbb{Q}$ is projective iff it is free.

But $\mathbb{Q}$ is not free by (g) so $\mathbb{Q}$ is not projective. //

(d) Let K be a field. Which, if any, of these statements can be modified so that they hold if we replace $\mathbb{Z}$ by the ring $K[x]$ and $\mathbb{Q}$ by its field of fractions $K(x)$?

all of these statements hold for $K[x]$ and $K(x)$ since it is possible to only use the fact that $\mathbb{Z}$ is a UFD w/ infinitely many equivalence classes of irreducibles. //

(e) Let M be a right R-module, N be a left R-module and let M' (resp N') be a submod of M (resp N). Prove,

$$M/M' \otimes_R N/N' \cong (M \otimes_R N)/(M \otimes_R N' + M' \otimes_R N)$$

Pf:

Let $\pi_M : M \to M/M'$ and $\pi_N : N \to N/N'$ be canonical proj.

then $\pi_M \otimes \pi_N : M \otimes_R N \to M/M' \otimes_R N/N'$ is a canonical proj.

Note, since $M' = \ker \pi_M$ and $N' = \ker \pi_N$

$\Rightarrow K = M \otimes_R N' + M' \otimes_R N \subset \ker(\pi_M \otimes \pi_N)$.

Thus we have a well-defined epimorphism of ab. grps

$$f : (M \otimes_R N)/K \longrightarrow M/M' \otimes_R N/N'$$

$$m \otimes n + K \longmapsto (m+M') \otimes (n+N')$$

Conversely,

define $g : M/M' \times N/N' \longrightarrow (M \otimes_R N)/K$

$$(m+M', n+N') \longmapsto m \otimes n + K$$

g is well-defined since $(M', n+N')$ and $(m+M', N')$ get mapped to zero

Since g is middle R-linear, it induces a canonical homom of abelian grp

$$\bar{g} : M/M' \otimes_R N/N' \longrightarrow (M \otimes_R N)/K$$

$$(m+M') \otimes (n+N') \longmapsto m \otimes n + K$$

Since $\bar{g} f = 1_{(M \otimes N)/K} \Rightarrow f$ is monic. (left inverses gives 1-1)

Thus f is an isomorphism. //

(f) Let M, M' be right R-mod, N, N' be left R-mod. Let $f \in \mathrm{Hom}_R(M, M')$, $g \in \mathrm{Hom}_R(N, N')$. Is it always true that $\ker(f \otimes g) = M \otimes_R \ker g + \ker f \otimes_R N$? Prove or give counterexample? (6)

Counterexample:

Let R be a UFD and $p \in R$ be prime.

Let $f : R/(p) \longrightarrow R/(p)$ be the identity map.

and let $g : R/(p) \to R/(p^i)$ where $i \geq 2$ (note: g is uniquely determined by $1+(p)$)

$$1+(p) \longmapsto p^{i-1}+(p^i)$$

(note g: monomorphism)

Consider the induced homom. $f \otimes g = R/(p) \otimes_R R/(p) \to R/(p) \otimes R/(p^i)$

since $(1+(p)) \otimes (1+(p)) \in R/(p) \otimes_R R/(p)$,

$$\begin{aligned}(f \otimes g)\{(1+(p)) \otimes (1+(p))\} &= (1+(p)) \otimes (p^{i-1}+(p^i)) \\ &= (p^{i-1}+(p)) \otimes (1+(p^i)) \quad \text{since } i \geq 2 \\ &= 0 \otimes (1+(p^i)) \\ &= 0\end{aligned}$$

Thus $f \otimes g = 0$

$\Rightarrow \ker(f \otimes g) = R/(p) \otimes R/(p)$ ($= M \otimes_R N$ from original prob)

but $M \otimes_R \ker g + \ker f \otimes_R N = R/(p) \otimes (p) + (p) \otimes R/(p)$

$= 0$

$\to\leftarrow$ (b/c $R/(p) \otimes R/(p) \neq 0$)

(g) Determine, with a proof, whether $\mathbb{Q}$ is a free $\mathbb{Z}$-module. (2)

Claim: $\mathbb{Q}$ is not free

Pf: first we will show $\mathbb{Q}$ is not cyclic.

Suppose $\mathbb{Q} = \langle m/n \rangle$ for some $m, n \in \mathbb{Z} \setminus \{0\}$

let $k \neq \pm 1$ $k \in \mathbb{Z}$

Suppose $\frac{m}{nk} = \frac{rm}{n}$ for some $r \in \mathbb{Z}$. (can do b/c we are assuming $\mathbb{Q}$ cyclic)

$\Rightarrow nm = rmnk = rknm$

$\Rightarrow rk = 1$ since $\mathbb{Z}$ ID.

$\Rightarrow k$ is a unit $\rightarrow\leftarrow$ b/c $k \neq \pm 1$.

thus $\mathbb{Q}$ cannot have a basis consisting of one elmt.

Now suppose $x_1, x_2 \in \mathbb{Q}$ form a basis for $\mathbb{Q}$.

let $x_i = \frac{a_i}{b_i}$ for $i = 1, 2$. $a_i, b_i \in \mathbb{Z} \setminus \{0\}$.

Consider, $r_1 x_1 + r_2 x_2 = r_1\left(\frac{a_1}{b_1}\right) + r_2\left(\frac{a_2}{b_2}\right)$

since $\mathbb{Z}$ is ID

suppose we let $r_1 = a_2 b_1$ and $r_2 = -a_1 b_2$

since $\mathbb{Z}$ is ID. $r_1, r_2 \neq 0$.

$\Rightarrow r_1 x_1 + r_2 x_2 = r_1\left(\frac{a_1}{b_1}\right) + r_2\left(\frac{a_2}{b_2}\right) = a_2 b_1\left(\frac{a_1}{b_1}\right) + (-a_1 b_2)\left(\frac{a_2}{b_2}\right)$

$= a_1 a_2 - a_1 a_2 = 0$

$\Rightarrow x_1, x_2$ are not linearly independent.

$\Rightarrow \mathbb{Q}$ does not have a basis containing two element.

$\Rightarrow \mathbb{Q}$ is not free. //

(h) Prove that $\mathbb{Q}$ is generated by the set $\{p^{-a} \mid p \text{ prime}, a>0\}$ as a $\mathbb{Z}$-module. (8)

Pf:

Note $\mathbb{Q}$ is generated by $\{\frac{1}{n} \mid n \in \mathbb{Z} \setminus \{0, \pm 1\}\}$

Let $m, n \in \mathbb{Z}$ s.t. $(m,n) = 1$.

Choose $x, y \in \mathbb{Z}$ s.t. $xm + yn = 1$.

$$\Rightarrow \frac{y}{m} + \frac{x}{n} = \frac{1}{mn}$$

$\Rightarrow \frac{1}{mn}$ is contained in the $\mathbb{Z}$-submodule of $\mathbb{Q}$ generated by $\frac{1}{m}$ & $\frac{1}{n}$

Since $\mathbb{Z}$ is a UFD, $\{p^{-a} \mid p \text{ prime}, a>0\}$ generates $\mathbb{Q}$. //

F-201B

(3) Let R be a commutative unital ring. Given $a \in R$. Let $ev_a : R[x] \to R$ be the evaluation homom which is uniquely determined by $ev_a(r) = r \ \forall r \in R$ and $ev_a(x) = a$. Recall that a homom of rings $\phi : R \to S$ extends to a homom of rings $\overline{\phi} : Mat_n(R) \to Mat_n(S)$ defined by $(a_{ij}) \longmapsto (\phi(a_{ij}))$.

[2007] Let R be a comm. unital rng, $ev_0 : R[x] \to R$ the eval. homom which is uniq. ~~determined~~ defined by $ev_0(r) = r$ $\forall\ r \in R$, $ev_0(x) = 0$.

a) Let $\Lambda \subseteq R$ be a multiplicative set (that is $\lambda_1, \lambda_2 \in \Lambda \Rightarrow \lambda_1 \lambda_2 \in \Lambda$). Prove that $\Lambda^{-1} M = 0$ iff $Ann_R m \neq \phi \ \forall\ m \in M$.

Pf:

Let $x \in \Lambda$, $m \in M$

$\frac{m}{x} = 0$ iff $\exists\ t \in \Lambda$ s.t. $tm = 0$

iff $\Lambda \cap Ann_R m \neq 0$.

(b) Prove that an epic homom between free R-mod of the same finite rank is an isomorphism.

Pf:

Let E, F be free R-modules of rank n.

Let $\psi: E \to F$ be an epic homom.

~~For some $\lambda_{ij} \in R$, let $A = (a_{ij})$ be the matrix~~

Let $\{e_i\}$ be a basis of E and $\{f_i\}$ be a basis of F.

For some $\lambda_{ij} \in R$, let $A = (a_{ij})$ be the matrix of ψ wrt these bases.

Thus $\psi(e_i) = \sum_j a_{ij} f_j$

Since ψ is epic then $f_i = \sum_j \lambda_{ij} \psi(e_j)$

$$= \sum_{jk} \lambda_{ij} a_{jk} f_k$$

Since $\{f_i\}$ is a basis, then $\sum_j \lambda_{ij} a_{jk} = \delta_{i,k} \quad \forall i,k$

Thus $A = (a_{ij})$ is left invertible.

Take $\Lambda = (\lambda_{ij})$ so $\Lambda A = I_n$.

But R is comm ring so $A\Lambda = I_n$.

Thus A is invertible.

$\therefore$ ψ is an ~~isomorphism~~ isomorphism. //

(c) Let $\phi: R \to S$ be a homom of comm rings. Show that for any $A \in Mat_n(R)$, $\phi(\det(A)) = \det(\bar{\phi}(A))$

note: $\bar{\phi}: Mat_n(R) \to Mat_n(S)$
$(a_{ij}) \longmapsto (\phi(a_{ij}))$

Pf:

Let $A = (a_{ij})$

$$\phi(|A|) = \phi\left(\sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}\right)$$

$$= \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\left(\phi(a_{1\sigma(1)}) \cdots \phi(a_{n\sigma(n)})\right)$$

$$= |\bar{\phi}(A)|. \quad //$$

Show that $\forall\, r \in R$, $D \in Mat_n(R[x])$,

$$ev_r(|D|) = |(ev_r(D))|$$

Pf:

same take $\phi = ev_r$.

(d) Let $A \in Mat_n(R)$. Show that $\det(A^a) = \det(A)^{n-1}$ and $(A^a)^a = (\det(A))^{n-2} A$.

The ring R is not assumed to be a domain.

Pf:

Let $A \in Mat_n(R)$. Take $C = XI_n - A \in Mat_n(R[X])$.

Since $|C|$ is a monic poly then $|C|$ is not a zero divisor or zero so we can cancel it.

By a proposition we know $CC^a = |C| I_n$, thus $|C||C^a| = |C|^n$

so $|C||C^a| = |C||C|^{n-1}$, thus $|C^a| = |C|^{n-1}$.

For any comm. unital ring S, $|\lambda B| = \lambda^n |B|$ for $B \in Mat_n(S)$.

First we will show that $A^a = (-1)^{n-1} eV_0(C^a)$

So, $(-1)^{n-1} eV_0(C^a) = (-1)^{n-1} eV_0((-1)^{i+j} |C_{ji}|)$ def of C^a

$= (-1)^{n-1}(-1)^{i+j} |eV_0 C_{ji}|$ by 3C

$= (-1)^{i+j}(-1)^{n-1} |-A_{ji}|$ since $C = XI_n - A$

$= (-1)^{i+j} |A_{ji}|$ by thm $|-A_{ji}| = (-1)^{n-1}|A_{ji}|$

$= A^a$ def of A^a.

Consider, $|A^a| = |(-1)^{n-1} eV_0(C^a)|$

$= (-1)^{n(n-1)} eV_0 |C^a|$ by fact above & 3C.

$= (-1)^{n(n-1)} eV_0 |C|^{n-1}$ by above

$= (-1)^{n(n-1)} |eV_0 C|^{n-1}$ by 3C

$= (-1)^{n(n-1)} |-A|^{n-1}$ since $C = XI_n - A$

$= (-1)^{n(n-1)}(-1)^{n(n-1)} |A|^{n-1}$ by above

$= |A|^{n-1}$

→

Next we will show $(A^a)^a = |A|^{n-2} A$.

By proposition we know,

$C^a(C^a)^a = |C^a| I_n$ thus $C^a(C^a)^a = |C|^{n-1} I_n$ by previous page. multiplying by C on the left we obtain,

$C\,C^a(C^a)^a = C|C|^{n-1} \implies |C| I_n (C^a)^a = C|C|^{n-1}$ by proposition.

So $|C|(C^a)^a = |C||C|^{n-2} C$ since $|C|$ is not a zero divisor or zero we can cancel it, thus.

$(C^a)^a = |C|^{n-2} C$

So, $(A^a)^a = \left((-1)^{n-1} eV_0(C^a)\right)^a$ by previous arg. for inside part.

$= (-1)^{n-1} eV_0 (C^a)^a$

$= (-1)^{n-1} eV_0 (|C|^{n-2} C)$ by above

$= (-1)^{n-1} eV_0 |C|^{n-2} eV_0 C$

$= (-1)^{n-1} |eV_0 C|^{n-2} eV_0 C$ by 3C

$= (-1)^{n-1} |-A|^{n-2} (-A)$ since $C = xI_n - A$

$= (-1)^{n-1} (-1)^{n(n-2)} |A|^{n-2} (-1) A$ by above

$= (-1)^{n(n-1)} |A|^{n-2} A$

$= |A|^{n-2} A$. //

2007 (e) Let $A \in Mat_n(R)$ and set $C = xI_n - A \in Mat_n(R[x])$. Prove that $A^a = (-1)^{n-1} ev_0(C^a)$, where A^a is the adjoint matrix of A in $Mat_n(R)$ and C^a is the adjoint matrix of C in $Mat_n(R[x])$.

Pf:

Well, $(-1)^{n-1} ev_0(C^a) = (-1)^{n-1} ev_0\left((-1)^{i+j} |C_{ji}|\right)$ def of C^a

$= (-1)^{n-1}(-1)^{i+j} |ev_0 C_{ji}|$ by 3C

$= (-1)^{i+j}(-1)^{n-1} |-A_{ji}|$ since $C = xI_n - A$, $ev_0(C) = ev_0(xI_n - A) = -A$

$= (-1)^{i+j} |A_{ji}|$ by mm $|-A_{ji}| = (-1)^{n-1}|A_{ij}|$

$= A^a$ def of A^a.

//

200x (f) Use the identity $CC^a = C^aC = \det(C) I_n$ in $\mathrm{Mat}_n(R[X])$ to prove Cayley-Hamilton thm ($p_A(A) = 0$) over an arbitrary comm unital ring R.

2007 (g) Prove that ev_0 extends to a homom of rings $Mat_n(R[x]) \to Mat_n(R)$.

$$\phi: Mat_n(R[x]) \longrightarrow Mat_n(R)$$
$$a(x)_{ij} \longmapsto (ev_0\, a(x)_{ij})$$

Pf:

The only part we need to check is that it commutes w/ matrix multiplication (homom holds w/ mult)

Let $A, B \in Mat_n(R[x])$. NTS $\phi(AB) = \phi(A)\phi(B)$.

Let $A = (a(x)_{ij})$ and $B = (b(x)_{ij})$

Let $C = AB$ where $c_{ij} = \sum_{k=1}^{n} a(x)_{ik}\, b(x)_{kj}$

Consider,

$$\phi(AB) = \phi(C) = \phi(c_{ij}) = ev_0\left(\sum_{k=1}^{n} a(x)_{ik}\, b(x)_{kj}\right)$$
$$= \sum_{k=1}^{n} ev_0(a(x)_{ik})\, ev_0(b(x)_{kj})$$
$$= ev_0(a(x)_{ij})\, ev_0(b(x)_{ij})$$
$$= \phi(a(x)_{ij})\, \phi(b(x)_{ij})$$
$$= \phi(A)\,\phi(B). \quad //$$

F-201B

(4)

(a) Find the invariant factors of the matrix

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 0 \\ 3 & 0 & 0 \end{pmatrix} \in Mat_3(\mathbb{Q})$$

Well,

$$XI_n - A = \begin{pmatrix} X & 0 & -1 \\ 0 & X-2 & 0 \\ -3 & 0 & X \end{pmatrix} \xrightarrow{C_1 \leftrightarrow C_3} \begin{pmatrix} -1 & 0 & X \\ 0 & X-2 & 0 \\ X & 0 & -3 \end{pmatrix}$$

$$\xrightarrow{C_1 \mapsto -C_1} \begin{pmatrix} 1 & 0 & X \\ 0 & X-2 & 0 \\ -X & 0 & -3 \end{pmatrix} \xrightarrow{r_3 \mapsto Xr_1 + r_3} \begin{pmatrix} 1 & 0 & X \\ 0 & X-2 & 0 \\ 0 & 0 & X^2-3 \end{pmatrix}$$

$$\xrightarrow{C_3 \mapsto C_3 - XC_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & X^2-3 \end{pmatrix} \xrightarrow{r_2 \mapsto r_2 + r_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & X^2-3 \\ 0 & 0 & X^2-3 \end{pmatrix}$$

$$\xrightarrow{C_3 \mapsto C_3 - (X+2)C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 1 \\ 0 & 0 & X^2-3 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & X-2 \\ 0 & X^2-3 & 0 \end{pmatrix}$$

$X^2-3-(X+2)(X-2)$
X^2-3-X^2+4
1

$$\xrightarrow{r_3 \mapsto (X^2-3)r_2 - r_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & X-2 \\ 0 & 0 & (X^2-3)(X-2) \end{pmatrix} \xrightarrow{C_3 \mapsto C_3 - (X-2)C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X^2-3)(X-2) \end{pmatrix}$$

$(X^2-3)(1) - X^2 - 3$

$X-2-(X-2)$
$=0$

Therefore $(X^2-3)(X-2)$ is the invariant factors of matrix A. //

Note: $(X-2)(X^2-3)$ is minimal poly

(b) List all possible sets of invariant factors ② for a matrix $B \in Mat_6(\mathbb{Q})$ w/ minimal poly. $(X-2)^2(X^2+1)$

minimal poly = bottom one.

elementary divisors $(X-2)$, $(X-2)^2$, (X^2+1)

n_1 $\quad n_2 > 0$ $\quad n_3 > 0$

note: $n_1 + 2n_2 + 2n_3 = 6$.

	n_2	n_3	n_1
①	1	1	2
②	1	2	0
③	2	1	0

① $(X-2)^2 \quad (X^2+1) \to (X-2)^2(X^2+1)$

$(X-2) \to (X-2)$

$(X-2) \to (X-2)$

So $\boxed{(X-2) \mid (X-2) \mid (X-2)^2(X^2+1)}$ I.F.

② $(X-2)^2 \quad (X^2+1) \to (X-2)^2(X^2+1)$

$(X^2+1) \to (X^2+1)$

So $\boxed{(X^2+1) \mid (X-2)^2(X^2+1)}$ I.F.

③ $(X-2)^2 \quad (X^2+1) \to (X-2)^2(X^2+1)$

$(X-2)^2 \to (X-2)^2$

So $\boxed{(X-2)^2 \mid (X-2)^2(X^2+1)}$ I.F.

Note rational canonical matrices associated w/ them

① $\begin{pmatrix} 2 & & & & & \\ & 2 & & & & \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & -4 & 4 & -5 & 4 \end{pmatrix}$

② $\begin{pmatrix} 0 & 1 & & & & \\ -1 & 0 & & & & \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & -4 & 4 & -5 & 4 \end{pmatrix}$

③ $\begin{pmatrix} 0 & 1 & & & & \\ -4 & 4 & & & & \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & -4 & 4 & -5 & 4 \end{pmatrix}$

note:

$(X-2)^2(X^2+1) = X^4 - 4X^3 + 5X^2 - 4X + 4$

$(X-2)^2 = X^2 - 4X + 4$

(c) List all possible Jordan canonical forms for the matrix $B \in Mat_6(\mathbb{C})$ with the characteristic poly $(X-2)^2(X^2+1)^2$ (up to permutation.

| char poly = diag mult.

$$(X-2)^2(X^2+1)^2 = (X-2)^2(X+i)^2(X-i)^2$$

$(X-2)^2$ $(X+i)^2$ $(X-i)^2$ $(X-2)$ $(X+i)$ $(X-i)$

n_1 n_2 n_3 n_4 n_5 n_6

note: $J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \\ 0 & \lambda & 1 & 0 \\ & 0 & \ddots & \ddots \\ & & & \lambda \end{pmatrix}$ λ = root

$J_1(2) = (2)$ $J_2(2) = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$

$J_1(-i) = (-i)$ $J_2(-i) = \begin{pmatrix} -i & 1 \\ 0 & -i \end{pmatrix}$

$J_1(i) = (i)$ $J_2(i) = \begin{pmatrix} i & 1 \\ 0 & i \end{pmatrix}$

	n_1	n_2	n_3	n_4	n_5	n_6
①	1	1	1	0	0	0
②	1	1	0	0	0	2
③	1	0	1	0	2	0
④	0	1	1	2	0	0
⑤	1	0	0	0	2	2
⑥	0	1	0	2	0	2
⑦	0	0	1	2	2	0
⑧	0	0	0	2	2	2

$6 = 2n_1 + 2n_2 + 2n_3 + n_4 + n_5 + n_6$

$2n_1 + n_4 = 2$

$2n_2 + n_5 = 2$

$2n_3 + n_6 = 2$

ex: ① $(X-2)^2(X-i)^2(X+i)^2$

④ $(X-2)(X-i)^2(X+i)^2 \to (X-2)(X-i)^2(X+i)^2$
$(X-2) \to (X-2)$

} invariant factors

⑧ [illegible]

① diag $(J_2(2), J_2(-i), J_2(i))$

② diag $(J_2(2), J_2(-i), J_1(i), J_1(i))$

③ diag $(J_2(2), J_2(i), J_1(-i), J_1(-i))$

④ diag $(J_2(-i), J_2(i), J_1(2), J_1(2))$

⑤ diag $(J_2(2), J_1(-i), J_1(-i), J_1(i), J_1(i))$

⑥ diag $(J_2(-i), J_1(2), J_1(2), J_1(i), J_1(i))$

⑦ diag $(J_2(i), J_1(2), J_1(2), J_1(-i), J_1(-i))$

⑧ diag $(J_1(2), J_1(2), J_1(-i), J_1(-i), J_1(i), J_1(i))$

List all possible Jordan canonical forms for the matrix $B \in Mat_6(\mathbb{C})$ w/ the minimal poly $(x-2)^2(x^2+1)$.

Elementary divisors are: $(x-2)^2$, $(x+i)$, $(x-i)$, $(x-2)$
$n_1 > 0$ $n_2 > 0$ $n_3 > 0$ n_4

$2n_1 + n_2 + n_3 + n_4 = 6$

$n_1 = J_2(2)$ $n_3 = J_1(i)$
$n_2 = J_1(-i)$ $n_4 = J_1(2)$

	n_1	n_2	n_3	n_4
①	1	1	1	2
②	1	2	1	1
③	1	2	2	0
④	1	1	2	1
⑤	1	1	3	0
⑥	1	3	1	0
⑦	2	1	1	0

① diag $(J_2(2), J_1(-i), J_1(i), J_1(2), J_1(2))$

② diag $(J_2(2), J_1(-i), J_1(-i), J_1(i), J_1(2))$

③ diag $(J_2(2), J_1(-i), J_1(-i), J_1(i), J_1(i))$

④ diag $(J_2(2), J_1(-i), J_1(i), J_1(i), J_1(2))$

⑤ diag $(J_2(2), J_1(-i), J_1(i), J_1(i), J_1(i))$

⑥ diag $(J_2(2), J_1(-i), J_1(-i), J_1(-i), J_1(i))$

⑦ diag $(J_2(2), J_2(2), J_1(-i), J_1(i))$.

(d) Let K be a field. Show that $K[X]/(X^2)$ is an indecomposable $K[X]$-module while $K[X]/(X^2-1)$ is a direct sum of two indecomposable modules (which are isomorphic as K-vector spaces but not as $K[X]$-modules) (5)

Pf:

suppose $K[X]/(X^2)$ is decomposable.

$\Rightarrow$ (by lemma 6.11) $K[X]/(X^2) \cong \frac{K[X]}{(p_1^{n_1})} \oplus \cdots \oplus \frac{K[X]}{(p_K^{n_K})}$

where $X^2 = p_1^{n_1} \cdots p_K^{n_K}$

but X is irreducible.

$\Rightarrow$ X is prime

$\Rightarrow$ $p_1 = X$ and $n_1 = 2$, $p_i^{n_i} = 1 \quad \forall i \neq 1$.

Thus $K[X]/(X^2)$ is indecomposable

Consider $X^2-1 = (X+1)(X-1)$

$X-1$ and $X+1$ are irred. in $K[X]$

$\Rightarrow$ $X-1$ and $X+1$ are prime

Thus by lemma 6.11,

$K[X]/(X^2-1) \cong K[X]/(X-1) \oplus K[X]/(X+1)$ //

(e) List all possible rational canonical forms for a matrix $B \in mat_6(\mathbb{Q})$ with the minimal poly $(x-2)^2(x^2+1)$.

elementary divisors $(x-2)^2$, (x^2+1), $(x-2)$

$n_1 \geq 0$ $\quad n_2 \geq 0$ $\quad n_3$

$2n_1 + 2n_2 + n_3 = 6$

	n_1	n_2	n_3
①	1	1	2
②	1	2	0
③	2	1	0

① $(x-2)^2(x^2+1) \rightarrow x^4 - 4x^3 + 5x^2 - 4x + 4$

$(x-2) \rightarrow x-2$

$(x-2) \rightarrow x-2$

$$\begin{pmatrix} 2 & & & & & \\ & 2 & & & & \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & -4 & 4 & -5 & 4 \end{pmatrix}$$

② $(x-2)^2 (x^2+1) \rightarrow x^4 - 4x^3 + 5x^2 - 4x + 4$

$(x^2+1) \rightarrow x^2+1$

$$\begin{pmatrix} 0 & 1 & & & & \\ -1 & 0 & & & & \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & -4 & 4 & -5 & 4 \end{pmatrix}$$

③ $(x-2)^2(x^2+1) \rightarrow x^4 - 4x^3 + 5x^2 - 4x + 4$

$(x-2)^2 \rightarrow x^2 - 4x + 4$

$$\begin{pmatrix} 0 & 1 & & & & \\ -4 & 4 & & & & \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & -4 & 4 & -5 & 4 \end{pmatrix}$$

F-201B

(5) Let R be a ring, M be an R-module.
Then $\mathrm{End}_R M$ is a unital ring (non-comm).
Note that if S is a subring of R and M is an R-mod, $\mathrm{End}_R M$ is a subring of $\mathrm{End}_S M$.

(a) Describe the natural $\mathrm{End}_R M$-module structure on M.

Claim: M is an $\mathrm{End}_R M$-module (and unitary)

Pf:
Let the action be defined as $f \cdot m = f(m)$
$\forall f \in \mathrm{End}_R M$, $m \in M$.
Since addition is defined pt-wise
$(f_1 + f_2) \cdot m = f_1(m) + f_2(m)$.

$$f \cdot (m_1 + m_2) = f(m_1 + m_2)$$
$$= f(m_1) + f(m_2) \quad \text{since } f \in \mathrm{End}_R M$$

$$f \cdot (g \cdot m) = f \cdot (g(m)) = f(g(m))$$
$$= f \circ g(m)$$
$$= (f \circ g)(m)$$

$$1_m \cdot m = m$$

Thus M is a unitary $\mathrm{End}_R M$-module.

//

(b) suppose that if $f \in \mathrm{End}_R M$ is not invertible, ~~Prove M is indecomposable~~. Then $1_M - f$ is invertible. Prove M is indecomposable.

Pf:

By midterm 1, M is indecomposable iff the only idempotents in $\mathrm{End}_R M$ are 0, 1.

atc M is decomposable.

Let $f \in \mathrm{End}_R M$ be a nontrivial idempotent.

Then $1_M - f$ is also a nontrivial idempotent

because $1_M - f \neq 0, 1_M$.

Note, $f^2 = f$

so $f - f^2 = 0$

$f(1-f) = 0 \Rightarrow$ f, 1−f are zero divisors

$\Rightarrow$ f, 1−f are not invertible.

$\rightarrow\leftarrow$ b/c if f is not invertible then $1_M - f$ should be invertible.

Thus M is indecomposable. //

For problems (c) & (d) we need a lemma.

Lemma:

Let R be a unital ring, F be a free R-module. Let B be a basis of F, and $X \subset B$. Then for any R-module M and any function $f: X \to M$ $\exists$ $\overline{f} \in \mathrm{Hom}_R(F, M)$ s.t. $\overline{f}(x) = f(x)$ $\forall$ $x \in X$.

In particular, if D is a division ring, V and W are D-vector spaces and $X \subset V$ is linearly independent then for any function $f: X \to W$ $\exists$ $\overline{f} \in \mathrm{Hom}_D(V, W)$ s.t. $\overline{f}(x) = f(x)$ $\forall$ $x \in X$.

(c) If D is a division ring and V is a (left) D-vector space, prove that V is simple as a module over the ring $S = \mathrm{End}_D V$.

(d) Let D be a division ring, V be a left D-vector space and $R = \mathrm{End}_D V$.
Then $\mathrm{End}_R V \cong D$.

(e) M is decomposable iff $\mathrm{End}_R M$ contains a nontrivial idempotent (that is, $\exists\ f \in \mathrm{End}_R M$, $f \neq 0, 1_M$ s.t. $f^2 = f$).

Pf:

($\Rightarrow$) Let M be decomposable.

So $M = M_1 \oplus M_2$ with $M_1, M_2 \neq 0, M$.

Let $\pi : M \to M_1$ and $i : M_1 \to M$ be the canonical projection and inclusion.

Then $\pi \circ i = 1_{M_1}$.

thus $(i \circ \pi) \circ (i \circ \pi) = i \circ (\pi \circ i) \circ \pi = i \circ \pi$

So $i \circ \pi \in \mathrm{End}_R M$ is idempotent.

Since i is 1-1 and π is onto,

$$\ker i \circ \pi = \ker \pi = M_2.$$

So $i \circ \pi \neq 1_M$ b/c $\ker \neq 0$ then $i \circ \pi$ is not 1-1 so cannot be identity

b/c $\ker i \circ \pi \neq M$ so cannot be zero map. //

($\Leftarrow$)

Let $f \in \mathrm{End}_R M$ that is a nontrivial idempotent, so $f \neq 0, 1$ and $f^2 = f$.

By midterm, $M = \ker f \oplus \mathrm{Im}\, f$.

Note $\mathrm{Im} f \neq 0$ since $f \neq 0$.

also $\ker f \neq 0$ since $m - f(m) \in \ker f$ (b/c $f(m - f(m)) = f(m) - f^2(m) = f(m) - f(m) = 0$)

$\forall m \in M$. and $m - f(m) \neq 0$ b/c if so $f(m) = m \Rightarrow f = 1_M \to\leftarrow$ thus M is decomposable

F-201 B

(6) Let R be a ring, M be a finite length R-module. Then $\mathrm{End}_R M$ is a ring. (non-comm.)

(a) Prove that M is a finite direct sum of indecomposable modules.

Pf:

We are done if M is indecomposable.

Suppose M is decomposable.

We will do induction on length of M, $\ell(M)$

Base case: $\ell(M) = 1$, done by above.

Suppose $\ell(M) > 1$

$\Rightarrow$ then $M = M_1 \oplus M_2$ where M_1 and M_2 are nonzero submodules.

It follows by the properties of length that $\ell(M_i) < \ell(M)$.

Applying the induction hypothesis we conclude that each M_i is a finite direct sum of indecomposables. //

(b) Prove that if M is indecomposable then $\mathrm{End}_R M$ is a local ring, that is, has a unique maximal ideal. You may use the part of Fitting Lemma proved in class.

Fitting lemma – If M has finite length and is indecomposable, then $f \in \mathrm{End}_R M$ is either invertible or nilpotent.

Lemma:
General fact:
Let S be any unital ring. Let $a \in S$ s.t. a is nilpotent.
Let $n \in \mathbb{N}$ s.t. $a^n = 0$. We will show $1-a$ is a unit.
$(1-a)(1+a+\cdots+a^{n-1}) = 1-a^n = 1 = (1+a+\cdots+a^{n-1})(1-a)$

Pf:
Let $\underline{m}$ be the set of all nonunits in $\mathrm{End}_R M$.
By fitting lemma, then $\underline{m}$ is the set of all nilpotent elmts.
We will show $\underline{m}$ is an ideal.
Let $f \in \underline{m}$, since $f \in \mathrm{End}_R M$ and f is nilpotent
(so $\exists\, n$ s.t. $f^n = 0$ and $f \neq 0$) then $\ker f \neq 0$.
So $\forall\, g \in \mathrm{End}_R M$, $\ker gf \neq 0$.
So gf is not 1-1, thus gf is not invertible.
thus $gf \in \underline{m}$.

NTS: $fg \in \underline{m}$. Consider when $g \notin \underline{m}$ (so g is iso)
$\Rightarrow \mathrm{Im}\, g \cap \ker f \neq 0$ (not just zero)
$\Rightarrow \ker fg \neq 0$ (b/c g iso $\ker fg = \ker f$).
$\Rightarrow fg \in \underline{m}$ (so fg is not 1-1 thus fg is not invertible)

Now we will show $\underline{m}$ is an abelian subgrp of $\mathrm{End}_R M$
It is clear that $\underline{m}$ is closed under additive inverse.
Suppose $f, g \in \underline{m}$. AIC $f+g \notin \underline{m}$ $\Rightarrow$ $f+g$ is an iso.
$\Rightarrow \exists\, u \in \mathrm{End}_R M$ s.t. $u(f+g) = 1$ (b/c $f+g \notin \underline{m}$)

$\Rightarrow uf+ug=1$ but $uf \in \underline{m}$ (by previous ideal arg.)

so uf is nilpotent.

So $1-uf=ug$ is a unit by general fact.

But $ug \in \underline{m}$ (by previous ideal arg.

so ug is nilpotent $\longrightarrow\!\!\!\!\longleftarrow$.

Thus $f+g \in \underline{m} \Rightarrow \underline{m}$ is closed under addition.

thus $\underline{m}$ is an ideal.

(and maximal since it contains all nonunits.)

(c) Prove the converse of the statement (b). [Hint: If $f \in \mathrm{End}_R M$ is a non-trivial idempotent, then so is $1_M - f$.]

Converse: If $\mathrm{End}_R M$ is a local ring then M is indecomposable.

Pf:

Note: If S is a local ring then for any $x \in S$, either x or $1-x$ is a unit.

ATC M is decomposable.

Then $\exists$ a nontrivial idempotent $f \in \mathrm{End}_R M$ (by part (c))

Since $(1-f)^2 = (1-f)(1-f) = 1 - f - f + f^2$
$= 1 - f - f + f = 1 - f$

so $1-f$ is idempotent and nontrivial b/c f is nontrivial.

Note, $f^2 = f$
So $f - f^2 = 0$
$f(1-f) = 0$
$\Rightarrow$ f, $1-f$ are zero divisors

$\Rightarrow$ f, $1-f$ are not invertible

hence neither f or $1-f$ is a unit in $\mathrm{End}_R M$

$\rightarrow\leftarrow$ (to note)

Thus M is indecomposable. //

(e) Do we need M to be finite length in 5(e) and 6(d)?

We never used that property in the proof, hence these statements hold for any module.

F-201B

(7) Given a ring S, denote its center by
$Z(S) = \{ a \in R \mid ar = ra \ \forall r \in R \}$.
Prove that $Z(Mat_n(R)) \cong Z(R)$.

Pf:

Claim: $Z(Mat_n(R)) = \{ r I_n \mid r \in Z(R) \}$

Note that $Mat_n(R)$ is generated as an R-module by $E_{i,j}$ where $E_{i,j}$ has 1_R in (i,j) th place and zero everywhere else.

Indeed if $X \in Mat_n(R)$ then $X = \sum_{i,j} x_{i,j} E_{i,j}$

Note that $E_{i,j} E_{k,e} = 0$ if $j \neq k$ and $E_{i,j} E_{k,e} = E_{i,e}$ if $j = k$.

Let $X \in Z(Mat_n(R))$

$\Rightarrow X E_{i,j} = \sum_{r,s} x_{r,s} E_{r,s} E_{i,j} = \sum_{r} x_{r,i} E_{r,j}$ $\left(\begin{smallmatrix} \text{blc } s=i \\ \text{otherwise } 0 \end{smallmatrix} \right)$

$E_{i,j} X = \sum_{r,s} x_{r,s} E_{i,j} E_{r,s} = \sum_{s} x_{j,s} E_{i,s}$ $\left(\begin{smallmatrix} \text{blc } j=r \\ \text{otherwise } 0 \end{smallmatrix} \right)$

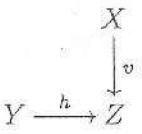
the first matrix has entries only in j^{th} column,
while the second has entries only in the i^{th} row

They can only be equal if $x_{r,i} = 0 \ \forall r \neq i$, $x_{j,s} = 0 \ \forall s \neq j$,
and $x_{i,i} = x_{j,j}$

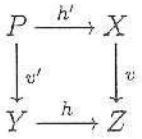
Since this must hold $\forall i,j$ we conclude that X is diagonal and all its diagonal entries are equal.

Observe that $(rI_n)(sI_n) = (sI_n)(rI_n) \ \forall s \in R$ iff $r \in Z(R)$ //

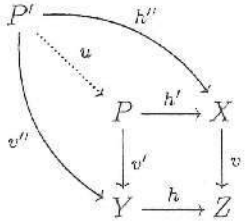
Let $\mathscr{C}$ be a category. A *pullback* of the diagram



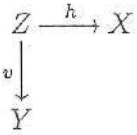
where X, Y, Z are objects in $\mathscr{C}$ and v, h are morphisms between the corresponding objects, is a triple (P, v', h') where P is an object in $\mathscr{C}$, $h' : P \to X$ and $v' : P \to Y$ are morphisms such that the diagram



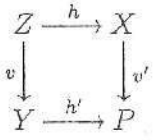
commutes and which is a terminal object in the category of such triples; in other words, if (P', v'', h'') is another such triple then there exists a *unique* morphism $u : P' \to P$ such that the following diagram commutes



The dual concept is called the *pushout*. Thus, a pushout of a diagram

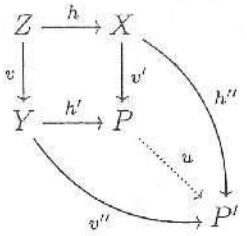


is a triple (P, h', v') such that the diagram



commutes and which is universal with that property, that is for any such triple (P', h'', v'') there is a unique morphism $u : P \to P'$ such

that the diagram



commutes. The usual arguments show that pullbacks and pushouts, when exist, are unique up to an isomorphism.

(a) Show that pullback preserves monomorphisms, pushout preserves epimorphisms and both preserve isomorphisms (that is, if $v : X \to Z$ in the pullback diagram is a monomorphism, then so is $v' : P \to Y$; similarly, if $h : Z \to X$ in the pushout diagram is an epimorphism then so is $h' : Y \to P$).

(b) Let $\mathscr{C} = \mathsf{Set}$ (the category of sets). Define $X \times_Z Y = \{(x, y) \in X \times Y : f(x) = g(y)\}$. Then $(X \times_Z Y, i, j)$, where i, j are the natural functions $X \times_Z Y \to X$, $X \times_Z Y \to Y$, is the pullback of $X \xrightarrow{f} Z \xleftarrow{g} Y$ in Set. Thus, in the category Set every pair of morphisms with the same target object has a pullback.

(c) Show that in the category $R-$Mod every pair of morphisms with the same target object has a pullback. [*Hint.* Let $P = \{(x, y) \in X \oplus Y : f(x) = g(y)\}$. Check that P is a submodule of $X \oplus Y$ and that restrictions of canonical projections $X \oplus Y$ on X and Y to P provide the morphisms $P \to X$ and $P \to Y$ with the desired property. Do not forget to check the uniqueness!]

(d) Show that in the category $R-$Mod every pair of morphisms with the same source object has a pushout. [*Hint.* Let $Q = (X \oplus Y)/\{(f(z), -g(z)) : z \in Z\}$; define the morphisms $X \to Q$ and $Y \to Q$ by composing the natural morphisms $\iota_X : X \to X \oplus Y$ (respectively, $\iota_Y : Y \to X \oplus Y$) with the canonical projection $X \oplus Y \to Q$ show that Q has the desired properties.]

(e) Show that in the category $R-$Mod pullbacks and pushouts preserve monomorphisms and epimorphisms.

Remark. The above constructions work in any abelian category (in particular, in the category of abelian groups). The second construction does not work in the category of rings because the abelian subgroup $\{(f(z), -g(z)) : z \in Z\}$ need not be an ideal of $X \oplus Y$.

Consider two extensions

$$\varepsilon : 0 \to N \xrightarrow{f} E \xrightarrow{g} M \to 0, \qquad \varepsilon' : 0 \to N \xrightarrow{f'} E' \xrightarrow{g'} M \to 0.$$

Consider the pullback of $E \xrightarrow{g} M \xleftarrow{g'} E'$ and let Γ be the corresponding module (that is, $\Gamma = \{(e, e') \in E \oplus E' : g(e) = g'(e')\}$). Inside Γ we have a submodule

$$Y = \{(f(n), -f'(n)) : n \in N\}.$$

Indeed, $gf(n) = 0 = g'f'(n)$. Thus, we can consider the module $E'' = \Gamma/Y$. We have a natural epimorphism $\Gamma \to M$ (pullbacks in this category preserve epimorphisms!) given by $(e, e') \mapsto g(e)$ and, since Y is contained in its kernel, we have an induced homomorphism $g'' : E'' \to M$, $(e, e') + Y \mapsto g(e)$. Furthermore, we have a natural monomomorphism $N \to \Gamma$ given by $n \mapsto (f(n), 0)$ (again, $gf(n) = 0$) so by taking its composition with the canonical projection $\Gamma \to \Gamma/Y$ we obtain a homomorphism $f'' : N \to E''$, $n \mapsto (f(n), 0) + Y = (0, f'(n)) + Y$.

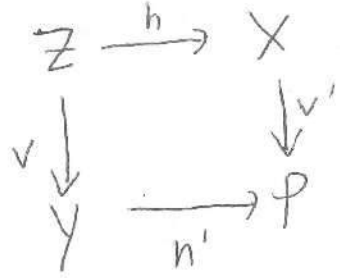
Prove that the sequence

$$0 \to N \xrightarrow{f''} E'' \xrightarrow{g''} M \to 0$$

is short exact. This sequence is called the *Baer sum* of two extensions ε and ε'. Check that this operation is well-defined on equivalence classes of extensions and that for any extension ε its Baer sum with a split extension is equivalent to ε.

Prove pushouts perserve isomorphism

aka: if h is an iso then so is h'
if v is an iso then so is v'.

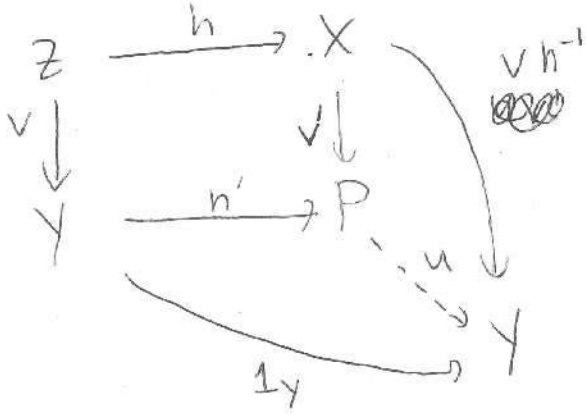


Pf:
Let h be an iso, so $\exists$

$h^{-1}: X \to Z$ s.t. $hh^{-1} = 1_X$ and $h^{-1}h = 1_Z$

we want to find an inverse for h'
ie something say $u: P \to Y$
s.t. $h'u = 1_P$ & $uh' = 1_Y$

Consider,



By universal property (U.P.)
$\exists !\ u: P \to Y$
s.t.
$1_Y = uh'$ and
$vh^{-1} = uv'$

Note we already have $1_Y = uh'$ by U.P.

NTS $h'u = 1_P$.

But to use U.P. NTS that square Z, X, Y, Y commutes (outside one)

aka show $vh^{-1}h = 1_Y v$

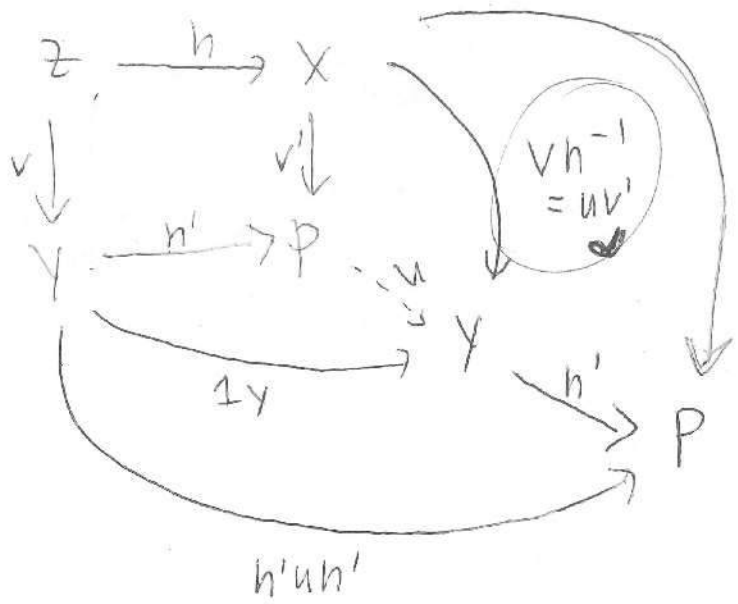
LHS: $vh^{-1}h = v1_Z = v$ = v.

RHS: $1_Y v = v$

so U.P. valid.

NTS $h'u = 1_P$.

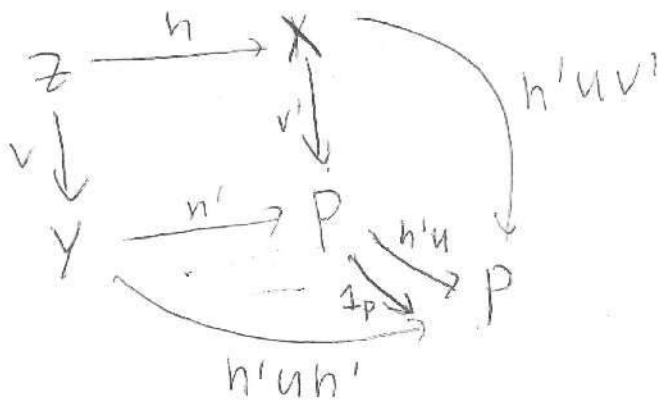
Consider this expanded diagram



Bottom

So pushout preserves ISO.

Now clean this up



~~NTS this~~ ~~sucks~~ u·p.

NTS 1_P & $h'u$ give same u·p

$\Rightarrow 1_P = h'u$.

NTS: $h'u$ solves u·p.

1) NTS: $h'uv' = (h'u)v'$ clear
2) NTS: $h'uh' = (h'u)h'$ clear

} so $h'u$ solves u·p.

NTS: 1_P solves u·p.

1) NTS: $h'uv' = 1_P v'$

Well $h'uv' = h'(uv') = h'(vh^{-1}) = (h'v)h^{-1}$

(by above; by original square)

$= (v'h^0)h^{-1} = v' = 1_P v'$ ✓

2) NTS: $h'uh' = 1_P h'$

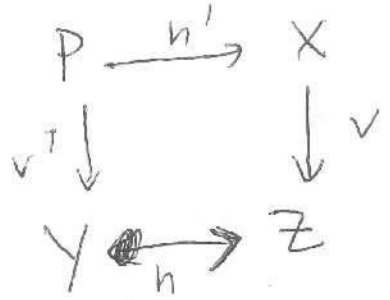
Well $h'uh' = h'(uh') = h'1_Y = h' = 1_P h'$ ✓

So 1_P solves u·p $\Rightarrow$ $1_P = h'u \Rightarrow h'$ is ISO.

Assume for v, h, v'

Prove pullbacks perseve iso

aka: if h is iso then so is h'
if v is an iso then so is v'.



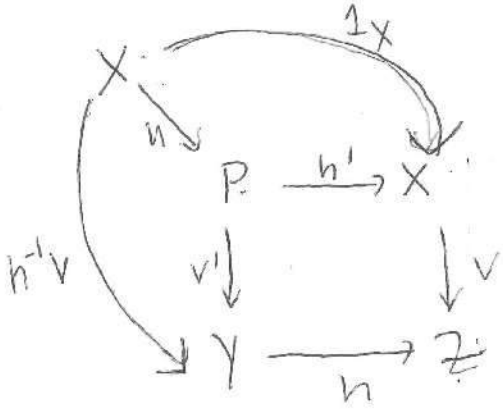
Pf:

let h be an iso, so $\exists$

$h^{-1}: Z \to Y$ s.t. $hh^{-1} = 1_Z$ and $h^{-1}h = 1_Y$

we want to find an inverse for h'
ie something say $u: X \to P$ s.t. $h'u = 1_X$ & $uh' = 1_P$

consider,



By universal property (u.p)

$\exists!\ u: X \to P$

s.t.

$1_X = h'u$ and $h^{-1}v = v'h$

so we already get $h'u = 1_X$ by u.p.

NTS $uh' = 1_P$

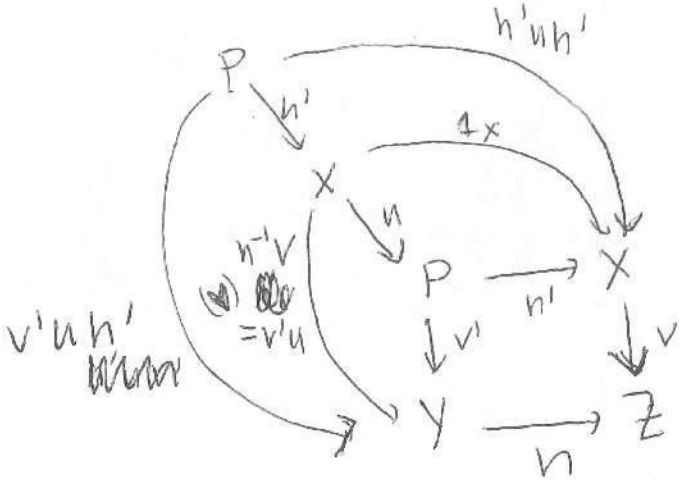
But to use u.p. nts that square X, X, Y, Z (outside) commutes. aka show $v1_X = h(h^{-1}v)$

but $h(h^{-1}v) = hh^{-1}v = v = v1_X$ ✓

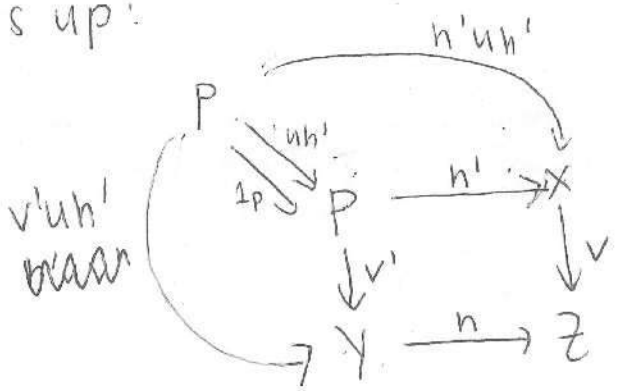
so u.p. valid.

NTS $uh' = 1_P$

Consider the expanded diagram:



Clean this up:



NTS: $1_P \cong uh'$ solve same u.p.

$\Rightarrow 1_P = uh'$

NTS: uh' solves u.p.

NTS: 1) $h'uh' = h'(uh')$ clear

2) ~~$h'Iuv' = h'(uh')$~~ $v'uh' = v'(uh')$ clear.

~~well $v'(uh') = (v'u)h' = h'vh' = h'(vh') = h'v'$~~

So uh' solves u.p.

NTS: 1_P solves u.p.

NTS: 1) $h'uh' = h' 1_P$

well $h'uh' = (h'u)h' = 1_X h' = h' = h' 1_P$ ✓

2) $v'uh' = v' 1_P$

well $v'uh' = (v'u)h' = (h^{-1}v)h' = h^{-1}(vh') = h^{-1}(hv')$ (original square)

$= v' = v' 1_P$ ✓

(above)

So 1_P solves u.p.

By uniqueness $1_P = uh' \Rightarrow h'$ is an isomorphism

Likewise for $v \cong v' \Rightarrow$ pullbacks preserves iso. //

Wed: 12:30 - 3pm

Can do problems through section 4

FITTING LEMMA FOR MODULES

Let R be a ring and M be an R-module. We say that M is Noetherian (respectively, Artinian) if for any chain of submodules $M_1 \subset M_2 \subset \cdots$ (respectively, $\cdots \subset M_2 \subset M_1$) in M there exists $n \geq 1$ such that $M_i = M_n$ for all $i \geq n$.

Lemma (Fitting). *Suppose that M is Noetherian and Artinian. If M is indecomposable, then any $f \in \operatorname{End}_R M$ is either invertible or nilpotent.*

Proof. Let $f \in \operatorname{End}_R M$. Clearly, $\ker(f^n) \subset \ker(f^{n+1})$ and $\operatorname{Im}(f^{n+1}) \subset \operatorname{Im}(f^n)$. Since M is both Noetherian and Artinian, there exists k such that $\ker(f^n) = \ker(f^k)$ and $\operatorname{Im}(f^n) = \operatorname{Im}(f^k)$ for all $n \geq k$. Suppose that $x \in \ker(f^k) \cap \operatorname{Im}(f^k)$. Then $x = f^k(y)$ for some $y \in M$, hence $f^k(x) = f^{2k}(y) = 0$ and $y \in \ker(f^{2k}) = \ker(f^k)$. Therefore, $f^k(y) = x = 0$. Furthermore, given $x \in M$, we have $f^k(x) = f^{2k}(y)$ for some $y \in M$, since $\operatorname{Im}(f^k) = \operatorname{Im}(f^{2k})$. Then $f^k(x - f^k(y)) = 0$ hence $x - f^k(y) \in \ker(f^k)$ and so $M = \operatorname{Im}(f^k) + \ker(f^k)$. Thus, $M = \operatorname{Im}(f^k) \oplus \ker(f^k)$. Since M is indecomposable, either $\operatorname{Im}(f^k) = 0$, or $\ker(f^k) = 0$. In the first case, $f^k = 0$ that is to say f is nilpotent. In the second case, $\ker(f) \subset \ker(f^k) = 0$ and $M = \operatorname{Im}(f^k) \subset \operatorname{Im}(f)$, hence f is injective and surjective. $\Rightarrow$ invertible $\square$

This Lemma can be regarded as a generalization of Schur's lemma. Indecomposable modules for which $\operatorname{End}_R M$ is a division ring are sometimes called bricks (simple modules which are of course indecomposable provide an example of such).

(a) The category of Noetherian (respectively, Artinian) modules is a Serre subcategory of $R-\mathrm{Mod}$ (that is, given a short exact sequence of R-modules $0 \to M \to M' \to M'' \to 0$, M' is Noetherian/Artinian if and only if M and M'' are Noetherian/Artinian).

(b) Suppose that M is both Noetherian and Artinian. Then there exists a chain of submodules $0 = M_l \subset M_{l-1} \subset \cdots \subset M_1 \subset M_0 = M$ such that M_i/M_{i+1} is simple.

Remark. It can be shown that l depends only on M, as well as the set of isomorphism classes of simple modules M_i/M_{i+1}.

(c) Suppose that M is both Noetherian and Artinian. If M is indecomposable then $\operatorname{End}_R M$ is a local ring, that is it has a unique maximal ideal. [*Hint.* Use Fitting lemma to show that the set of non-units in $\operatorname{End}_R M$ is its unique maximal ideal]

If M is not Noetherian and Artinian then $\operatorname{End}_R M$ need not be local.

(d) If $\operatorname{End}_R M$ is local then M is indecomposable [*Hint.* Prove first that a unital ring S is local if and only if the set $S \setminus S^\times$ is an ideal and this happens if and only if for any non-unit $x \in R$, $1_R - x$ is a unit.]

Fitting lemma background

R is a ring and M is an R-mod.

Noetherian (max)

M is Noetherian if for any chain of submod $M_1 \subset M_2 \subset \dots$ in M $\exists\ n \geq 1$ s.t. $M_i = M_n$ $\forall\ i \geq n$.

Artinian (Min)

M is Artinian if for any chain of submod $\dots \subset M_2 \subset M_1$ in M $\exists\ n \geq 1$ s.t. $M_i = M_n$ $\forall\ i \geq n$

EX:

$\mathbb{Z}$ as a $\mathbb{Z}$-mod

Yes Noetherian b/c all ideals, are principle $\Leftrightarrow$ if $(n) \subset (m)$ then $m \mid n$.

So for $(n_1) \subset (n_2) \subset (n_3) \subset \dots$ this stops at some pt b/c only finite # of divisors.

Not artinian b/c for $n > 1$

$(n) \supset (n^2) \supset (n^3) \supset \dots$ union will keep going so not artin.

EX: $\mathbb{Z}/(p^\infty)$ as a $\mathbb{Z}$-mod $\mathbb{Z}[1/p]/\mathbb{Z} \simeq \mathbb{Z}(p^\infty)$

Yes artinian b/c

No Noetherian b/c $\langle 1/p \rangle \subseteq \langle 1/p^2 \rangle \subseteq \langle 1/p^3 \rangle \subseteq \dots$

Lemma (Fitting)

Suppose that M is Noetherian and Artinian. If M is indecomposable, then any $f \in End_R M$ is either invertible or nilpotent.

Pf:

Let $f \in End_R M$

Notice that $\ker f^n \subseteq \ker f^{n+1}$ and $\operatorname{Im} f^{n+1} \subseteq \operatorname{Im} f^n$.

Since M is Noetherian & artinian, $\exists\ k$ s.t.

$\ker f^n = \ker f^k$ and $\operatorname{Im} f^n = \operatorname{Im} f^k$ $\forall\ n \geq k$.

Now we will show $\ker f^k$ and $\operatorname{Im} f^k$ are disjoint, except for 0.

aTC, $\exists\ x \in M$ s.t. $x \neq 0$ and $x \in \ker f^k \cap \operatorname{Im} f^k$.

Since $x \in \operatorname{Im} f^k$, then $\exists\ y \in M$ s.t. $x = f^k(y)$

Since $x \in \ker f^k$, then $0 = f^k(x) = f^k(f^k(y)) = f^{2k}(y)$

So $y \in \ker f^{2k}$

But since M Noetherian $\ker f^{2k} = \ker f^k$, so $y \in \ker f^k$

So $f^k(y) = 0$

But $f^k(y) = x \Rightarrow x = 0$ $\rightarrow\leftarrow$

Thus $\ker f^k$ and $\operatorname{Im} f^k$ are disjoint, except for 0.

Let $x \in M$, since M is artinian then $\operatorname{Im} f^k = \operatorname{Im} f^{2k}$,

so $f^k(x) = f^{2k}(y)$ for some $y \in M$.

so $f^k(x - f^k(y)) = 0$.

$\Rightarrow x - f^k(y) \in \ker f^k$

Thus $x = \underbrace{x - f^k(y)}_{\in \ker f^k} + \underbrace{f^k(y)}_{\in \operatorname{Im} f^k}$

thus $X \in \mathrm{Im} f^k \oplus \ker f^k$

so $M \subset \mathrm{Im} f^k \oplus \ker f^k$.

clearly $\mathrm{Im} f^k \oplus \ker f^k \subset M$

thus $M = \mathrm{Im} f^k \oplus \ker f^k$.

But since M is indecomposable then either

$\mathrm{Im} f^k = 0$ or $\ker f^k = 0$.

If $\mathrm{Im} f^k = 0$,

then f is nilpotent. (since k is the power that kills)

If $\ker f^k = 0$.

so $\ker f \subseteq \ker f^k = 0 \Rightarrow f$ is injective

and $M = \mathrm{Im} f^k \subseteq \mathrm{Im} f \Rightarrow f$ is surjective

thus f is invertible.

//

F.L. (a)

The category of Noetherian (resp. artinian) modules is a serre subcategory of R-mod (that is given a short exact sequence of R-mod, $0 \to M \to M' \to M'' \to 0$, M' is Noetherian/artinian iff $M \& M''$ are as well.

Noetherian

Pf: $0 \to M \xrightarrow{f} M' \xrightarrow{g} M'' \to 0$

($\Rightarrow$) Since f is monic, then M is isomorphic to a submodule of M', call it N (ie $N \subseteq M'$ ($\& M \cong N$)

Since $N \subseteq M'$ and since M' is Noetherian,

N is contained in a chain of Noetherian modules

$\Rightarrow N \cong M$ is Noetherian

Since g is epic, $M'' = \operatorname{Im} g$.

By 1^{st} iso. $M'/\ker g \cong M'' = \operatorname{Im} g$

Since the quotient of a Noetherian module is Noetherian

then $M'/\ker g$ is Noetherian

thus M'' is Noetherian.

($\Leftarrow$) Let $M \& M''$ be Noetherian.

Let $L_1 \subseteq L_2 \subseteq \dots$ be an ascending sequence of submodules of M'. (NTS this sequence stops)

Let $A_i = L_i \cap M$. This is an increasing sequence of submods of M. So for large enough N we have $A_N = A_{N+1} = \dots$

Let $B_i = g(L_i)$ be the image of L_i in M''

Since M'' is Noetherian $\exists$ a large enough N'

s.t. $B_{N'} = B_{N'+1} = \dots$

let $K = \max\{N, N'\}$

So we get the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & A_K & \longrightarrow & L_K & \longrightarrow & B_K \longrightarrow 0 \\ & & \| & & \vdots & & \| \\ 0 & \longrightarrow & A_{K+1} & \longrightarrow & L_{K+1} & \longrightarrow & B_{K+1} \longrightarrow 0 \end{array}$$

Since the rows are exact and the diagram commutes

the map $L_K \longrightarrow L_{K+1}$ is an isomorphism

thus $L_K = L_{K+1}$

Thus our ascending sequence stops & hence M' is Noetherian. //

---

artinian

Pf: $0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{g} M'' \longrightarrow 0$

Let M' be artinian.

Since f is monic, then M is iso to a submodule of M', call it N (ie $N \subseteq M'$, $M \cong N$)

Since $N \subseteq M'$ and since M' is artinian,

N is contained in a chain of artinian modules

$\Rightarrow N \cong M$ is artinian.

Since g is epic, $M'' = \text{Im}\, g$.

By 1st iso $M'/\ker g \cong \text{Im}\, g = M''$ then $M'/\ker g$ is artinian

Since the quotient of a artinian module is ~~artinian~~ so M'' is. //

($\Leftarrow$) Let $M \to M''$ be artinian.

Let $\cdots \subseteq L_2 \subseteq L_1$ be a descending sequence of submodules of M'. (NTS this seq stops).

Let $A_i = L_i \cap M$. This is a decreasing chain of submod of M. So for large enough N we have $A_N = A_{N+1} = \cdots$

Let $B_i = g(L_i)$ be the image of L_i in M''.

Since M'' is artinian $\exists$ large enough N' s.t.

$$B_{N'} = B_{N'+1} = \cdots$$

Let $K = \max\{N, N'\}$.

So we get the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A_K & \longrightarrow & L_K & \longrightarrow & B_K \longrightarrow 0 \\ & & \downarrow = & & \downarrow & & \downarrow = \\ 0 & \longrightarrow & A_{K+1} & \longrightarrow & L_{K+1} & \longrightarrow & B_{K+1} \longrightarrow 0 \end{array}$$

Since the rows are exact & the diagram commutes the map $L_K \to L_{K+1}$ is an isomorphism.

Thus $L_K = L_{K+1}$

Thus our decreasing sequence stops and hence M' is Noetherian.

//

F.L. (b)

Suppose that M is both Noetherian and artinian. Then $\exists$ a chain of submodules $0 = M_e \subset M_{e-1} \subset \dots \subset M_1 \subset M_0 = M$ s.t. M_i/M_{i+1} is simple.

Pf:

Let M be Noetherian and artinian.

Since M is Noetherian, M has a maximal proper submodule, call it M_1.

If $M_1 = 0$ we are done.

Otherwise if $M_1 \neq 0$, then $\exists$ a max proper submod of M_1, call it M_2.

If $M_2 = 0$ we are done.

Otherwise proceed inductively as before.

If $M_n \neq 0$ $\forall n \in \mathbb{N}$ we get an infinite descending chain: $M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots \supsetneq M_n \supsetneq \dots$

$\rightarrow\leftarrow$ since M is artinian.

Thus for some $n \in \mathbb{N}$, we have $M_n = 0$.

So, $0 = M_n \subsetneq \dots \subsetneq M_1 \subsetneq M$.

Each M_i/M_{i+1} is simple.

Thm IV.1.10: If it where not then $\exists$ a submodule inbetween $M_i \supsetneq M_{i+1}$ but $\rightarrow\leftarrow$ since we constructed M_{i+1} to be a max submodule of M_i.

Thus M_i/M_{i+1} is simple.

//

F.L. (c) See Final (6b)

Suppose that M is both Noetherian and Artinian. If M is indecomposable then $\text{End}_R M$ is a local ring, that is it has a unique maximal ideal.

Hint: Use Fittings lemma to show that the set of non-units in $\text{End}_R M$ is its unique max ideal.

Pf:

Let M be Noetherian and Artinian. Let M be indecomposable.
So $\forall f \in \text{End}_R M$ f is either invertible or nilpotent by Fittings Lemma.
Consider the set of nonunits in $\text{End}_R M$, call it I. (so $\forall g \in I$, g is nilpotent)
NTS I is an ideal.
Let $g, f \in I$ s.t. $g^n = 0$, $f^m = 0$ $(n, m \in \mathbb{Z}^+)$

- Well g is a unit iff $-g$ is a unit, hence g is nilpotent iff $-g$ is nilpotent
  Thus $-g \in I$.
- also since $f \in I$, $\ker f$ is nontrivial
  so $\{0\} \neq \ker f \subseteq \ker gf$ so gf is not injective thus gf is not invertible, thus $gf \in I$.
  Likewise $fg \in I$.
- ATC $f+g \notin I$ so $f+g$ is a unit
  so $\exists\ h \in \text{End}_R M$ s.t. $(f+g)h = 1$ so $foh + goh = 1$.
  Since $g \in I$, g is nilpotent
  ATC goh is a unit, so $h'(goh) = 1$
  $h'g = h^{-1}$
  $g = h'^{-1}h^{-1}$
  But $h'^{-1}h^{-1}$ is a unit so g is a unit $\to\leftarrow$
  Thus goh is not invertible, hence goh is nilpotent
  So $(goh)^K = 0$ for $K \in \mathbb{Z}^+$

But $1 = 1 - (goh)^K = (1-(goh))(1+(goh)+(goh)^2+\dots+(goh)^{K-1})$

So $1-(goh)$ is invertible.

→← blc then foh would be invertible
but since $f \in I$ then $foh \in I$ (same reasoning as above)
thus $f+g \in I$ so $f+g$ is nilpotent.

So I is a subring.

let $r \in End_R M \setminus I$ and $f \in I$.

NTS $rf \in I$ and $fr \in I$

OTC rf is a unit so $\exists\ h \in End_R M$ s.t. $rfoh = 1$

so $rf = h^{-1}$

$f = r^{-1}h^{-1}$ can do this blc $r \in End_R M \setminus I$.

since r, h are units then $r^{-1}h^{-1}$ is a unit

so f is a unit →←

thus rf is not a unit, so $rf \in I$.

likewise $fr \in I$.

This ideal I is maximal blc if we were to add another elmt from $End_R M$ then it would be a unit by construction but then we would get the whole ring $(End_R M)$

thus I maximal & unique.

F.L. (d) See final 6(d)

If $\text{End}_R M$ is local, then M is indecomposable.

Hint: Prove first that a unital ring S is local iff the set $S \setminus S^\times$ is an ideal and this happens iff $\forall$ non-unit $x \in R$, $1_R - x$ is a unit.

Pf:

Let $\text{End}_R M$ be local.

NTS: $1_R - x$ is a unit $\forall$ non-units $x \in R$.

aTC $1_R - x = y$ is a non-unit

Well $1 = x + y$, since 1 is a unit then

$x+y$ is a unit.

but x, y are nonunits $\rightarrow\leftarrow$

Thus $1_R - x$ is a unit.

Note: By midterm 1, M is indecomposable iff the only idempotents in $\text{End}_R M$ are $0, 1$.

aTC M is decomposable.

Let $f \in \text{End}_R M$ be a nontrivial idempotent.

Then $1_M - f$ is also nontrivial idempotent.

blc $1_M - f \neq 0, 1_M$.

Note $f^2 = f$

So $f - f^2 = 0$

$f(1-f) = 0 \implies f, 1-f$ are zero divisors.

$\Rightarrow f, 1-f$ are not invertible.

$\rightarrow\leftarrow$ blc if f is not invertible then $1_M - f$ should be invertible. Thus M is indecomposable. //

Why tensoring is not an exact functor

Let $\alpha : \mathbb{Z}_2 \to \mathbb{Z}_4$ be the monomorphism of $\mathbb{Z}$-modules induced by the multiplication by 2. Consider

$$1 \otimes \alpha : \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4.$$

We have $(1 \otimes \alpha)(1 \otimes 1) = 1 \otimes \alpha(1) = 1 \otimes 2 = 0$, hence $\ker(1 \otimes \alpha) \neq 0$.

Localizaion of modules

Let R be a commutative ring, $S \subset R$ be a multiplicative set. Let M be an R-module. Define a relation $\sim$ on $M \times S$ by $(m, s) \sim (m', s')$ if and only if $tsm' = ts'm$ for some $t \in S$. Then $\sim$ is an equivalence relation. The set of equivalence classes is denoted by $S^{-1}M$ or $M[S^{-1}]$ and the class of (m, s) is denoted by m/s.

(a) $S^{-1}M$ is an R-module, with the abelian group structure defined by $(m/s)+(m'/s') = (s'm+sm')/ss'$ and the R-action defined by $r(m/s) = rm/s$. Moreover, $S^{-1}M$ is an $S^{-1}R$-module in the natural way and the R-action coincides with the one induced by the canonical homomorphism $\varphi_S : R \to S^{-1}R$, $r \mapsto rs/s$.

(b) There is a natural morphism of R-modules $\varphi_{M,S} : M \to S^{-1}M$, $m \mapsto sm/s$, $s \in S$.

(c) $\ker \varphi_{M,S} = \{m \in M : \operatorname{Ann}_R m \cap S \neq \emptyset\}$ where $\operatorname{Ann}_R m = \{r \in R : rm = 0\}$ (note that $\operatorname{Ann}_R m$ is always a left ideal).

(d) $S^{-1}M \cong S^{-1}R \otimes_R M$ as $S^{-1}R$-modules.

Define $\alpha_M : S^{-1}R \otimes_R M \to S^{-1}M$, $\alpha_M(r/s \otimes m) = rm/s$, check that α_M is a well-defined homomorphism of $S^{-1}R$-modules. To prove that α_M is an isomorphism, define $\beta_M : S^{-1}M \to S^{-1}R \otimes_R M$ by $\beta_M(m/s) = s/s^2 \otimes m$. Check that β_M is well-defined and show that $\alpha_M \circ \beta_M = 1_{S^{-1}M}$ and $\beta_M \circ \alpha_M = 1_{S^{-1}R \otimes_R M}$.

Let $r \in R$ and define the map $L_r : N \to N$ by $n \mapsto rn$. Then $L_r \in \operatorname{End}_R M$ (for this we need R to be commutative!)

(e) $S^{-1}M$ solves the following universal problem. Let N be an R-module such that for all $s \in S$, L_s is invertible as an endomorphism of N. Let $f \in \operatorname{Hom}_R(M, N)$. Then there exists a unique $\bar{f} : S^{-1}M \to N$ such that $f = \bar{f} \circ \varphi_{M,S}$.

(f) Prove (d) using (e).

(g) $S^{-1}R$ is flat as an R-module.

Suppose that $f \in \operatorname{Hom}_R(M, N)$ is injective. Then $1 \otimes f : S^{-1}R \otimes_R M \to S^{-1}R \otimes_R N$ is injective if and only if $h : S^{-1}M \to S^{-1}N$ defined by $h := \alpha_N \circ (1 \otimes f) \circ \beta_M$ is injective.

(h) If P is a prime ideal and $S = R \setminus P$, we write M_P instead of $(R \setminus P)^{-1}M$.

Let M be an R-module. Show that $\bigcap_{\mathfrak{m} \in \operatorname{Max} R} \ker \varphi_{M,R\setminus\mathfrak{m}} = \{0\}$, where $\operatorname{Max} R$ is the set of all maximal ideals in R. In particular, $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of R.

(i) A morphism of R-modules $M \to N$ is injective (respectively, surjective, an isomorphism) if and only if for each maximal ideal $\mathfrak{m}$ the induced morphism of R-modules $M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (respectively, surjective, an isomorphism).

(j) Let $\mathfrak{m}$ be a maximal ideal in R. Then we have two fields canonically associated with $\mathfrak{m}$, namely $R/\mathfrak{m}$ and $R_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}$ (recall that $R_{\mathfrak{m}}$ is a local ring). What is the relation between these fields? More generally, if M is an R-module, what is the relation between $M_{\mathfrak{m}}$ and $M/\mathfrak{m}M$?

Ran

Part B

2012 RINGS QUALIFIER

Prove all your claims; proofs must be as self-contained as is feasible.

1.[20] Let R be a unitary commutative ring. Prove *from scratch* that R and $R \oplus R$ are not isomorphic as R-modules.

2. [40] In this problem only, advanced theorems may be used.

(i) Determine with proof the number of similarity classes of matrices over the field $\mathbf{C}$ of complex numbers, with characteristic polynomial $(x-1)^2(x-2)^3$

(ii) Determine with proof the number of similarity classes of 8×8 matrices over the field $\mathbf{C}$ of complex numbers, with minimal polynomial $(x-1)^3(x-2)$

(iii) Let k be an algebraically closed field. Let A be an $n \times n$ matrix over k. For $a \in k$, set

$$W_a(A) := \ker((A - aI_n)^n) \subset k^n.$$

A *quasi-eigenvector* for A is a nonzero vector $v \in W_a(A)$ for some $a \in k$. Prove that there exist $a_1, \ldots, a_m \in k$ such that

$$k^n = \bigoplus_{i=1}^{m} W_{a_i}(A).$$

(Hint: You may use the Jordan form theorem).

(iv) Let k be an algebraically closed field. Let A, B be $n \times n$ matrices over k such that $AB = BA$. Prove that there is a basis of k^n whose elements are quasi-eigenvectors for both A and B.

3. [20] Let $R = \mathbb{Z}_{20}, S = \{1, 4, -4\}$.

(i) Prove that the natural map $R \to S^{-1}R$ is surjective and identify its kernel.

(ii) What is the cardinality of $S^{-1}R$?

4. [20] (i) Prove *from scratch* that if R is a PID then R has the property that any submodule of a finitely generated R-module is finitely generated.

(ii) Give an example with proof of a commutative unitary ring R where this property fails.

Winter 2012

2011

Greenstein

each question 10pts, perfect score is 50 pts

Part B.

All rings are assumed to be unital and all modules are assumed to be left and unitary unless specified otherwise.

1. Let I be a two-sided ideal in a ring R and let IM be the abelian subgroup of an R module M generated by all elements of the form xm, $x \in I$, $m \in M$. Show that IM is an R-submodule of M, describe the natural left R-module structure on $R/I \otimes_R M$ and show that $R/I \otimes_R M \simeq M/IM$ as left R-modules.
   2011-M2 #1 a/b 2013-M2 #1 c/d

2. Prove Schur's lemma: if M is a simple module over a ring R then $\mathrm{End}_R M$ is a division ring. Is the converse true (prove or provide a counter example)?
   2011-M1 #2 iii 2013-M1 #3 c

3. Let R be a ring and let M, N be left R-modules. Construct a natural homomorphism of abelian groups $M^* \otimes_R N \to \hom_R(M, N)$. If $R = k$ is a field and M, N are finite dimensional k-vector spaces prove that this natural homomorphism is in fact an isomorphism of k-vector spaces.
   ~2011 M2 #4

4. Let K be a field. We say that a $K[x]$-module M is nilpotent if for every non-unit $p \in K[x]$, $p^n M = 0$ for n sufficiently large. Prove that a finitely generated nilpotent indecomposable $K[x]$-module is isomorphic to $K[x]/(x^k)$ for some $k > 0$.
   Final sheet 4d ~

5. Let R be a ring.

   a. Prove that if a projective R-module P is a homomorphic image of an R-module M, then P is (isomorphic to) a direct summand of M (that is, $M = N \oplus P'$ for some submodules N, P', with $P \simeq P'$). IV.3.4 (i)⇒(iii)

   b. Formulate and prove an analogous statement for injective modules.
   IV 3.13

6. Let R be a ring and M_i, N_i, $i = 1, 2, 3$ be R-modules. Consider a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \psi_2} & & & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \longrightarrow & 0 \end{array}$$

   with exact rows (all maps are homomorphisms of R-modules). Suppose that there exists $\psi_1 \in \hom_R(M_1, N_1)$ such that $g_1\psi_1 = \psi_2 f_1$. Prove that there exists $\psi_3 \in \hom_R(M_3, N_3)$ that makes the diagram commute (that is, satisfies $g_2\psi_2 = \psi_3 f_2$). Which conditions should satisfy ψ_1 and/or ψ_2 to ensure that ψ_3 is surjective?
   short five lemma V.1.17

Winter 2011

7. Let K be a field and $p \in K[x]$ be a monic polynomial and A be its companion matrix. Prove that p is the minimal polynomial of A. Write down the companion matrix $q(x) = x^3 - x^2 + 2x - 1 \in \mathbf{Q}[x]$.

8. Let R be a domain and let A be an $n \times n$ matrix over R. Prove that if a system of linear equations $Ax = 0$ has a non-zero solution then $\det A = 0$. Is the converse true? both quals

2011 B 1

Let I be a two-sided ideal in a ring R and let IM be the abelian subgroup of an R-module M generated by all elmt of the form xm, $x \in I$, $m \in M$.

a) show that IM is an R-submodule of M.

b) Describe the natural left R-module structure on $R/I \otimes_R M$.

c) show that $R/I \otimes_R M \cong M/IM$ as left R-mod.

Pf:

a) Given IM is an abelian subgroup of M (R-mod)

NTS $rb \in IM$ $\forall$ $r \in R$ & $b \in IM$.

It suffices to show that the generators of IM satisfy this property.

Let $r \in R$, $xm \in IM$ (so $x \in I$, $m \in M$)

Consider rxm. Since $r \in R$ & $x \in I$ (two-sided ideal)

$\Rightarrow rx \in I$

$\Rightarrow rxm \in IM$

Thus IM is a R-submodule of M.

b) The left R-mod structure on $R/I \otimes_R M$ is defined by

$$r \cdot (r'+I) \otimes M = (r'+I)\, r \otimes M$$

$$= (r'r + I) \otimes M.$$

c) Consider the short exact sequence

$$0 \to I \xrightarrow{i} R \xrightarrow{\pi} R/I \to 0$$

Note, $-\otimes_R M$ is a right exact functor so

$$I \otimes_R M \xrightarrow{i\otimes 1_M} R \otimes_R M \xrightarrow{\pi \otimes 1_M} R/I \otimes_R M \longrightarrow 0$$

is a right exact sequence.

Since M is an R-mod, $R \otimes_R M \cong M$ (*)

Since right exact sequence then $\operatorname{Im}(i\otimes 1_M) = \ker(\pi \otimes 1_M)$ (♥)

Claim: $\operatorname{Im}(i \otimes 1_M) \cong IM$

We know $f: R \otimes_R M \longrightarrow M$, $r \otimes m \longmapsto rm$ is a well-defined isomorphism.

Since f is well-defined $\Rightarrow I \otimes M \subseteq R \otimes M$, then

$g: I \otimes M \longrightarrow M$, $x \otimes m \longmapsto xm$ is a well-defined monomorphism.

Since IM is generated by elmts of the form xm, where $x \in I$, $m \in M$, then $\operatorname{Im} g = IM$

$$\Rightarrow I \otimes M \cong \operatorname{Im} g = IM$$

also by def of i, $I \otimes M \cong \operatorname{Im}(i \otimes 1_M)$

$$\Rightarrow \operatorname{Im}(i \otimes 1_M) \cong IM. \quad (♥)$$

So, $R/I \otimes_R M \cong (R \otimes M)/\ker(\pi \otimes 1_M)$ (by 1st iso $\Rightarrow$ sequence) ↓ ♥

$$\cong R \otimes M / IM$$

↓ (*)

$$\cong M/IM$$

2011 B2:

Prove Schur's lemma: If M is a simple module over a ring R then $\mathrm{End}_R M$ is a division ring.

Pf:

Note $1_M \in \mathrm{End}_R M$.

Let $f \in \mathrm{End}_R M$, $f \neq 0$.

Then $\ker f \neq M$ and $\mathrm{Im} f \neq 0$

Since M is simple and both $\ker f$, $\mathrm{Im} f$ are submodules of M,

we have $\ker f = 0 \Rightarrow f$ monic

$\mathrm{Im} f = M \Rightarrow f$ epic

Thus f is isomorphism.

Therefore invertible.

Hence $\mathrm{End}_R M$ is a division ring. //

Is the converse true?

False, counterexample:

Consider $\mathbb{Z}_4$ as a $\mathbb{Z}$-mod.

Since $\mathbb{Z}_4$ is cyclic, any $f \in \mathrm{End}_{\mathbb{Z}} \mathbb{Z}_4$ is uniquely determined by where 1 goes. Thus the only $\mathbb{Z}$-mod homom are 0, 1_M, $f_{1,3}$ where $f_{1,3}$: $0 \to 0$, $1 \to 3$, $2 \to 2$, $3 \to 1$

Since 1 and $f_{1,3}$ are their own inverses

Then $\mathrm{End}_{\mathbb{Z}} \mathbb{Z}_4$ is a division ring.

However, $\mathbb{Z}_4$ is not a simple module.

Let $R = \mathbb{Z}$, $M = \mathbb{Q}$

every abelian group is a $\mathbb{Z}$-mod so, $\mathbb{Q}$ is a $\mathbb{Z}$-mod.

$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}) \cong \mathbb{Q}$ well

$\mathbb{Q}$ division ring but is simple //

2011 B3

Let R be a ring and let M, N be left R-mod. Construct a natural homom of abelian groups $M^* \otimes_R N \longrightarrow \mathrm{Hom}_R(M, N)$.

Pf:

Let R be a ring and M, N left R-mod.

Thus $M^* = \mathrm{Hom}_R(M, R)$ is a right R-mod.

Let $\phi : M^* \times N \longrightarrow \mathrm{Hom}_R(M, N)$

$$(f, n) \longmapsto (m \longmapsto f(m)\, n)$$

NTS ϕ is middle linear.

Let $f, f_1, f_2 \in M^*$, $n, n_1, n_2 \in N$, $r \in R$

$$\begin{aligned}
\phi(f_1 + f_2, n) &= (m \longmapsto (f_1 + f_2)(m) n) \\
&= (m \longmapsto (f_1(m) + f_2(m))\, n) \\
&= (m \longmapsto f_1(m)\, n + f_2(m) n) \\
&= (m \longmapsto f_1(m) n) + (m \longmapsto f_2(m) n) \\
&= \phi(f_1, n) + \phi(f_2, n).
\end{aligned}$$

By a similar argument $\phi(f, n_1 + n_2) = \phi(f, n_1) + \phi(f, n_2)$

$$\begin{aligned}
\phi(fr, n) &= (m \longmapsto (f(m) r)\, n) \\
&= (m \longmapsto f(m)(rn)) \\
&= \phi(f, rn).
\end{aligned}$$

Thus ϕ is middle linear so it induces the homom,

$\overline{\phi} : M^* \otimes_R N \longrightarrow \mathrm{Hom}_R(M, N)$. //

Now if $R=K$ is a field and M, N are finite dimensional K-vector spaces prove that this natural homom is in fact an isomorphism of K-vector spaces.

Pf:

Let $R=K$ be a field and M, N be finite-dim K-vector spaces.

Let $\dim(M)=m$ and $\dim(N)=n$.

Since every homom of vector spaces has a matrix representation we know $\mathrm{Hom}_R(M,N)$ identifies with $\mathrm{Mat}(m\times n, K)$, call this matrix A.

Let $\Psi: \mathrm{Hom}_R(M,N) \longrightarrow M^* \otimes N$

$$A \longmapsto \sum_{ij} a_{ij} f_i \otimes v_j$$

where $\{u_i\}$ is an ordered basis for M

$\{v_j\}$ is an ordered basis for N

$$f_i(u_j) = \delta_{ij}$$

So $\{f_i\}$ is an ordered basis for M^* (Thm IV 4.11)

NTS, $\bar{\Phi}\circ\Psi = 1_{\mathrm{Hom}_R(M,N)}$ and $\Psi\circ\bar{\Phi} = 1_{M^*\otimes N}$.

It suffices to show $\bar{\Phi}\circ\Psi = 1_{\mathrm{Hom}_R(M,N)} \Rightarrow \Psi$ is injective then show Ψ is surjective.

NTS: $\bar{\Phi}\circ\Psi = 1_{\mathrm{Hom}_R(M,N)}$

well, $(\bar{\Phi}\circ\Psi)(A)(\vec{x})$

$$= \left(\bar{\Phi}\left(\sum_{ij} a_{ij}(f_i\otimes v_j)\right)\right)(\vec{x})$$

$$= \sum_{ij} a_{ij}\left(f_i(\vec{x})\, v_j\right)$$

if $\vec{x} = \sum_{k=1}^{m} b_k u_k$, then $f_i(\vec{x}) = b_i$.

$$= \sum_{ij} a_{ij} b_i v_j = A(\vec{x})$$

Thus $\bar{\Phi}\circ\Psi = 1_{\mathrm{Hom}_R(M,N)}$

so Ψ is injective.

NTS Ψ is surjective,

it suffices to just consider basis elmts.

For $A \in \mathrm{Hom}(M,N)$ define

$A: M \to N$

$u_i \mapsto v_j$

$u_k \mapsto 0$ (if $k \neq i$)

So $\Psi(A) = f_i \otimes v_j$

thus Ψ is surjective. //

2011 B4

Let K be a field. We say that a $K[X]$-module M is nilpotent if for every non-unit $p \in K[X]$, $p^n M = 0$ for n sufficiently large. Prove that a finitely generated nilpotent indecomposable $K[X]$-module is isomorphic to $K[X]/(X^k)$ for some $k > 0$.

Pf:

Since K is a field, $K[X]$ is a PID.

Note: $X \in K[X]$ is irred $\Rightarrow$ prime (b/c PID)

(we always have prime $\Rightarrow$ irred in I.D)

So $X^n M = 0 \Rightarrow \forall\ m \in M\ \exists\ k \geq 0$ s.t. $X^k m = 0$ and $X^{k-1} m \neq 0$.

Thus $X^k \in \mathrm{Ann}_{K[X]}(m)$

$\Rightarrow (X^k) \subseteq \mathrm{Ann}_{K[X]}(m)$

By Thm IV 6.4(iv)

$\Rightarrow \mathrm{Ann}_{K[X]}(m) = (X^k)$.

So $M = M(X)$. Note $M(X) = \{ m \in M \mid \mathrm{ann}_{K[X]}(m) = (X^i) \text{ some } i \geq 0 \}$

By Thm IV 6.7 $\Rightarrow M \cong \bigoplus_{i=1}^{r} K[X]/(X^{n_i})$

$n_1 \geq \dots \geq n_r \geq 1$.

But it is indecomposable

So $r = 1$.

Thus $M \cong K[X]/(X^n)$ for some $n > 0$. //

2011 B5:

Let R be a ring.

a) Prove that if a projective R-mod P is a homomorphic image of an R-module M, then P is ($\simeq$ to) a direct summand of M (that is, $M = N \oplus P'$ for some submodules N, P' w/ $P \simeq P'$)

Pf:

Suppose P is a homomorphic image of an R-mod M.

$\Rightarrow \exists$ an R-mod homom $f: M \to P$ s.t. f is onto

$\Rightarrow M/\ker f \cong P$ (1^{st} iso for R-mod)

Since the following sequence is exact (by construction)

$$0 \to \ker f \xrightarrow{\iota} M \xrightarrow{f} P \to 0$$

and since P is projective, the sequence splits (Thm 3.4)

$\Rightarrow M \cong \ker f \oplus P$

$\ker f \subset M$, $\ker f = N$

Thus $\exists$ submodules $N, P' \subseteq M$ s.t.

Since $\operatorname{Im} f = P$, $\exists\ P' \subset M$ submod s.t. $P' \simeq P$.

$\Rightarrow M = N \oplus P$. //

b) Formulate & prove an analogous statement for injective modules

If an injective R-mod J is embedded into an R-mod M, then J is ($\simeq$ to) a direct summand of M (that is $M = N \oplus J'$ for some submod N, J' w/ $J \simeq J'$)

Pf: Since J is embedded into M,

$$0 \to J \hookrightarrow M \xrightarrow{\pi} M/J \to 0 \quad \text{is short exact.}$$

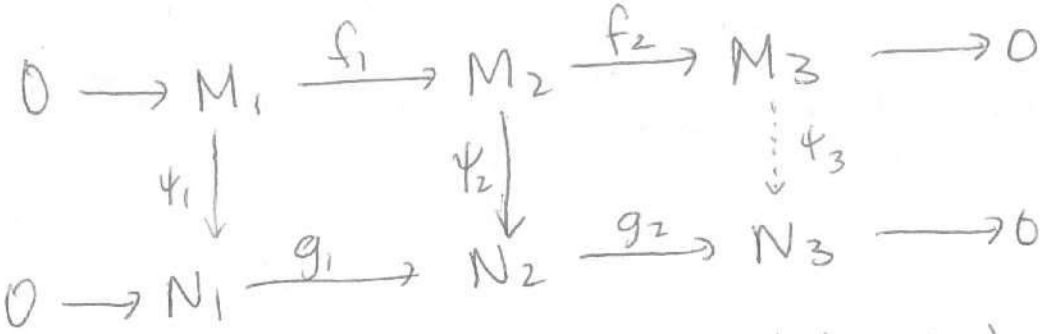
Since J is injective, $M \cong J \oplus M/J$.

$\Rightarrow \exists$ submod $J', N \subseteq M$ s.t. $J' \cong J$ (injective), $M/J \cong N$ (surjective).

$\Rightarrow M \cong N \oplus J'$. //

2011 B6

Let R be a ring and N_i, M_i $i=1,2,3$ be R-mod. Consider the diagram



w/ exact rows (all maps are R-mod homom).

Suppose $\exists\ \psi_1 \in \hom_R(M_1, N_1)$ s.t. $g_1\psi_1 = \psi_2 f_1$.

Prove $\exists\ \psi_3 \in \hom_R(M_3, N_3)$ s.t. $g_2\psi_2 = \psi_3 f_2$.

Pf:

Given $g_1\psi_1 = \psi_2 f_1$.

NTS: $\exists\ \psi_3$ s.t. $g_2\psi_2 = \psi_3 f_2$.

Let $m_3 \in M_3$

$\Rightarrow \exists\ m_2 \in M_2$ s.t. $f_2(m_2) = m_3$ (since f_2 onto)

$\Rightarrow \exists\ n_3 \in N_3$ s.t. $g_2\psi_2(m_2) = n_3$

Define $\psi_3(m_3) = n_3$.

Well-defined:

suppose $\exists\ m_3, m_3'$ s.t. $m_3 = m_3'$

NTS $\psi_3(m_3) = \psi_3(m_3')$.

well, $m_3 = f_2(m_2)$ & $m_3' = f_2(m_2')$

so $f_2(m_2) = f_2(m_2')$

$\Rightarrow f_2(m_2 - m_2') = 0$

$\Rightarrow m_2 - m_2' \in \ker f_2 = \operatorname{Im} f_1$

$\Rightarrow \exists\ m_1 \in M_1$ s.t. $f_1(m_1) = m_2 - m_2'$ (since f_1 1-1)

So $g_1 \psi_1(m_1) = \psi_2 f_1(m_1)$ (by given)

$= \psi_2(m_2 - m_2')$ (by above)

So $\psi_2(m_2 - m_2') \subset \operatorname{Im} g_1 = \ker g_2$.

So $g_2 \psi_2(m_2 - m_2') = 0$

$\Rightarrow g_2 \psi_2(m_2) = g_2 \psi_2(m_2')$

$\Rightarrow \psi_3(m_3) = \psi_3(m_3')$

Thus ψ_3 is well-defined.

By the construction of ψ_3, we have that $g_2 \psi_2 = \psi_3 f_2$

NTS: ψ_3 is a homom. ($\psi_3(rm_3 + m_3') = r\psi_3(m_3) + \psi_3(m_3')$)

Since f_2 is surjective, homom $\exists\ m_2, m_2' \in M_2$

s.t. $f_2(rm_2 + m_2') = rm_3 + m_3'$.

So, $\psi_3(rm_3 + m_3') = \psi_3 f_2(rm_2 + m_2')$

$= g_2 \psi_2(rm_2 + m_2')$

$= r g_2 \psi_2(m_2) + g_2 \psi_2(m_2')$

$= r \psi_3 f_2(m_2) + \psi_3 f_2(m_2')$

$= r \psi_3(m_3) + \psi_3(m_3')$

thus ψ_3 is a homom. //

Which conditions would satisfy ψ_1 and/or ψ_2 to ensure ψ_3 is surjective?

Suppose ψ_2 surjective

let $n_3 \in N_3$

$\Rightarrow \exists\ n_2 \in N_2$ s.t. $g_2(n_2) = n_3$ (since g_2 onto)

$\Rightarrow \exists\ m_2 \in M_2$ s.t. $\psi_2(m_2) = n_2$ (since ψ_2 onto)

so $n_3 = g_2 \psi_2(m_2) = \psi_3 f_2(m_2)$

$\Rightarrow n_3 \in \operatorname{Im} \psi_3$

$\Rightarrow \psi_3$ is surjective.

Thus it suffices to assume ψ_2 is surjective to show that ψ_3 is surjective. //

Side note: ψ_1 epic, ψ_2 iso $\Rightarrow$ ψ_3 is injective ($\Rightarrow$ iso)

2011 B7

Let K be a field and $p \in K[X]$ be a monic polynomial and A be its companion matrix. Prove that p is the minimal polynomial of A.

Pf:

We know $p = \sum_{i=0}^{r} a_i X^i$ with $a_r = 1$ and A is an $r \times r$ matrix given by $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots & & & & 0 \\ 0 & \cdots & & & 1 \\ -a_0 & -a_1 & \cdots & & -a_{r-1} \end{pmatrix}$ the matrix A determines a linear transformation ϕ on the basis of a vector space V with $\dim_K V = r$. Let $\{v_0, \ldots, v_{r-1}\}$ be the basis of V. Then ϕ is given by, $\phi(v_0) = v_1$, $\phi(v_1) = v_2$, $\ldots$, $\phi(v_{r-1}) = -\sum_{i=0}^{r-1} a_i v_i$.

Now we consider $W = K[X]/(p)$ which is a $K[X]$-module. We know $\dim_K W = r$. We define a basis of W by $w_i := X^i + (p)$ for $0 \le i \le r-1$. Now define the map $\Phi : V \to W$ by $v_i \mapsto w_i$. Since W is a $K[X]$-mod, the action of $X \in K[X]$ on the basis elmts w_i determines a map $\psi \in \mathrm{End}_K W$ where ψ acts in the following way $\psi(w_0) = w_1$, $\psi(w_1) = w_2$, $\ldots$, $\psi(w_{r-1}) = -\sum_{i=0}^{r-1} a_i w_i$.

Notice we have the following commutative diagram

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ V & \xrightarrow[\Phi]{} & W \end{array}$$

So $\Phi\phi = \psi\Phi$.

(*) p is minimal poly of A.

Since Φ is an isomorphism Φ^{-1} exists, so we get $\Phi\phi\Phi^{-1} = \psi$. Thus, the matrix of ϕ and ψ are similar. ~~Therefore, the minimal polynomials of the matrices associated with ϕ, ψ are the same.~~ also for any $f \in K[X]$ $\Phi f(\phi) = f\Phi(p)$. Since we have this, the minimal poly. of the matrices of ψ and ϕ are the same. also, we know by construction of W, $p\psi = 0$. If q is another poly s.t. $q\psi = 0$, then we get $p \mid q$ by def of W and p is monic. $\to\leftarrow$ thus, p is the minimal poly of matrix associated w/ $\psi \Rightarrow$ (*)

write down the companion matrix $q(x) = x^3 - x^2 + 2x - 1 \in \mathbb{Q}[x]$.

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & -2 & 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ +1 & -2 & +1 \end{pmatrix}$$

2011 BB:

Let R be a domain and let A be an $n \times n$ matrix over R. Prove that if a system of linear equations $AX = 0$ has a non-zero solution then $\det A = 0$.
Is the converse true.

Pf: (by contrapositive: if $\det A \neq 0$, then $AX = 0$ has only trivial sol)

Let R be a domain, then we can embed R into its field of fraction
Let $F = \text{Frac}(R)$.
Let A be an $n \times n$ matrix over R.
Let $\det A \neq 0$ over R
$\Rightarrow$ $\det A \neq 0$ over F
$\Rightarrow$ A is invertible over F

so $A\vec{x} = \vec{0} \Rightarrow A^{-1}(A\vec{x}) = \vec{0}$
$\Rightarrow \vec{x} = \vec{0}$ is the only solution over F, $R \subset F$

Thus $A\vec{x} = \vec{0}$ only has the trivial solution over R. //

Converse: $\det A = \vec{0} \Rightarrow A\vec{x} = \vec{0}$ has a nonzero solution

The

Pf: Let $|A| = \vec{0}$ over R $\Rightarrow$ $|A| = \vec{0}$ over F.

Note over F, $\vec{0}$ is an eigenvalue iff it is a root of the characteristic poly.

Since characteristic poly $= |xI_n - A|$ and
$|0I_n - A| = |-A| = (-1)^n |A| = 0$

Then it follows that 0 is an eigenvalue.

recall - k is an eigenvalue if $\exists$ a $\vec{u} \neq \vec{0}$ s.t. $A\vec{u} = k\vec{u}$

so for us $k = 0$, so $A\vec{x} = \vec{0}$ has a nontrivial solution over F.

Say $\vec{x} = \begin{pmatrix} x_1/y_1 \\ \vdots \\ x_n/y_n \end{pmatrix}$ so $\vec{x} \in F \Rightarrow x_i \in R$, $y_i \in R$

let $y = \prod_{i=1}^{n} y_i$ then $y \neq 0$ and $(y \in R)$

$$A(y\vec{x}) = y\,A(\vec{x}) = y\,\vec{0} = \vec{0}$$

↑ R is a domain (ie comm)

thus $y\vec{x}$ is a nontrivial solution over R. //

2010

Chari

Part B.

Assume that all rings have identity.

1. Let V be a vector space over a field K of dimension r. Let $f \in \hom_K(V, K)$. Prove that if f is non-zero, then it is surjective and determine the dimension of the kernel of f.

2. (a) Suppose that R and S are commutative rings and that M is a (R, S)-bimodule. This means that M is a left R-module and a right S-module and the actions are compatible, i.e. $r(ms) = (rm)s$, for all $r \in R$, $s \in S$, and $m \in M$. Let N be a left S-module. How does one define a left R-module structure on $M \otimes_S N$. What must you check to see that the action is well-defined. If we assume now in addition, that N is a (S, R)-bimodule what can you say about $M \otimes_S N$?

   (b) Suppose now that K is a field and let V, W, be vector space over K. Use (a) to show that $V \otimes_K W$ is also a vector space over K. What is the most natural way to find a basis for $V \otimes_K W$.

3. (a) Let V, W be vector spaces over a field K. How does one define a vector space structure on $\hom_K(V, W)$? Suppose now that $W = K$. Given a basis for V, how would you produce a natural basis for $V^* = \hom_K(V, K)$? More generally, if $\dim V = r$ and $\dim W = s$ and you are given bases for V and W, find a natural basis for $\hom_K(V, W)$.

   (b) Let W be another vector space over K. Define the natural map of vector spaces $V^* \otimes W \to \hom_K(V, W)$ and prove that it is an isomorphism of vector spaces.

4. Let R be the polynomial ring $\mathbf{C}[t]$ in one variable with coefficients in the complex numbers and let I be the ideal generated by t^2 and let $M = R/I$. Prove that M has a proper non-zero submodule and that M cannot be written as a direct sum of proper non-zero submodules. Suppose now that we take J to be the ideal generated by $t(t-1)$. Prove that the module $N = R/J$ is isomorphic to a direct sum of two proper non-zero submodules.

5. Prove that an $n \times n$-matrix with entries in a field K is invertible iff 0 is not an eigenvalue of the matrix.

6. What is the companion matrix A of the polynomial $q = x^2 - x + 2$. Prove that q is the minimal polynomial of A.

7. Suppose that P_1 and P_2 are R-modules. Prove that $P_1 \oplus P_2$ is projective iff P_1 and P_2 are projective.

8. Let $0 \to L \to M \to N \to 0$ be short exact sequence of R-modules such that we have a short exact sequence

$$0 \to \hom_R(N, L) \to \hom_R(N, M) \to \hom_R(N, N) \to 0.$$

   Prove that the original short exact sequence is split.

Winter 2010

2009 Gan

Part B.

Assume that all rings contain 1, and all modules are unitary, unless stated otherwise.

1. Let U and W be subspaces of a finite dimensional vector space V. Prove that

$$\dim(U+W)+\dim(U\cap W)=\dim(U)+\dim(W).$$

2. Prove that if m and n are coprime integers, then $(\mathbf{Z}/m\mathbf{Z})\otimes_{\mathbf{Z}}(\mathbf{Z}/n\mathbf{Z})\simeq 0$.

3. Let R be a ring. Let M be a finitely generated R-module, and let N be a projective R-module. Prove that if $f: M\to N$ is a surjective homomorphism, then the kernel of f is finitely generated.

4. Let $R=\mathbf{R}[x]$ and $A=Rz_1\oplus Rz_2\oplus Rz_3$, where

$$\operatorname{ann}(z_1)=((x+1)^2(x^2+1)),\quad \operatorname{ann}(z_2)=((x^2+1)^2),\quad \operatorname{ann}(z_3)=(x^4-1).$$

   Find the elementary divisors and the invariant factors of A.

5. Let $A\in \mathrm{Mat}_n(\mathbf{C})$. Prove that A is conjugate to its transpose A^t.

Winter 2009

2008

Gan

Part B.

All rings are assumed to be unital, and all modules are assumed to be unitary left modules unless otherwise stated.

1. Prove that

$$\mathbf{Q}[x]/(x^5 - 4x + 2)$$

is a field. Show, on the other hand, that

$$\mathbf{Z}[x]/(x^5 - 4x + 2)$$

is not a field.

2. Let R be a ring, and let A, B, C be three R-modules such that B is a submodule of A, and $C \simeq A/B$. Prove that if C is a projective R-module, then $A \simeq B \oplus C$.

3. Let R be a commutative ring and I an ideal of R. Let A be a R-module and denote by IA the submodule of A generated by all elements of the form ra with $r \in I$ and $a \in A$. Prove that there is an isomorphism of R-modules

$$(R/I) \otimes_R A \simeq A/IA.$$

4. Let V and W be two vector spaces over a field k, and $f : V \to W$ be a linear map. Prove that f is surjective if and only if its dual map f^* is injective.

5. Find the Jordan normal form of the following matrix over the field of complex numbers:

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Winter 2008

2007 Greenstein

Solve 4 out of 5

Part B.

All rings are assumed to be unital and all modules are assumed to be unitary and left unless specified otherwise.

1. Give an example of a ring R and an R-module M such that

(i) $- \otimes_R M$ is not exact.

(ii) $\hom_R(M, -)$ is not exact.

2. Let R be a ring and M_i, N_i, $i = 1, 2, 3$ be R-modules. Consider a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \psi_2} & & & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \longrightarrow & 0 \end{array}$$

with exact rows (all maps are homomorphisms of R-modules).

(i) Suppose that there exists $\psi \in \hom_R(M_3, N_3)$ such that $g_2\psi_2 = \psi_3 f_2$. Prove that there exists $\psi_1 \in \hom_R(M_1, N_1)$ making the diagram commute. Which conditions should satisfy ψ_2 and/or ψ_3 to ensure that ψ_1 is injective?

(ii) Suppose that there exists $\psi_1 \in \hom_R(M_1, N_1)$ such that $g_1\psi_1 = \psi_2 f_1$. Prove that there exists $\psi_3 \in \hom_R(M_3, N_3)$ making the diagram commute. Which conditions should satisfy ψ_1 and/or ψ_2 to ensure that ψ_3 is surjective? ← 2011 B6 (see other)

short 5 lemma IV.1.17

3. Let K be a field.

(i) Determine, with a proof, whether the field of rational functions $K(x)$ is a projective $K[x]$-module.

(ii) Describe the $K[x]$-module dual of $K(x)$.

(iii) Will the same results remain true if K is replaced by an integral domain R?

4. Let R be a domain, A be an $n \times n$ matrix over R. both equals. (i/ii)

(i) Prove that if the system of linear equations $Ax = 0$ has a non-trivial solution then $\det A = 0$.] see other.

(ii) Prove, or provide a counterexample to, the converse.

(iii) Which, if any, of these statements remain true if we drop the assumption that R is a domain? Prove or provide a counterexample.

5. Let R, S be commutative rings, $\varphi : R \to S$ be a ring homomorphism.

(i) Extend φ to a ring homomorphism $\overline{\varphi} : \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(S)$ and show that $\det(\overline{\varphi}(A)) = \varphi(\det(A))$ for all $A \in \mathrm{Mat}_n(R)$. Final 3c

(ii) Use part (i) to prove that the constant term of the characteristic polynomial of a matrix $A \in \mathrm{Mat}_n(R)$ equals $(-1)^n \det(A)$. VII.5.6

Winter 2007

2007 B1

Give an example of a ring R and an R-mod M s.t.

(i) $- \otimes_R M$ is not exact.

Let $R = \mathbb{Z}$, $M = \mathbb{Z}_2$

Consider the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

which we can tensor with M,

$$0 \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to 0$$

which can be rewritten as

$$0 \to \mathbb{Z}_2 \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to 0$$

since $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2$.

Claim: $\mathbb{Q} \otimes \mathbb{Z}_2$ is zero

This is b/c by tensoring with $\mathbb{Z}_2$, we have made multiplication by 2 identically zero.

By tensoring w/ $\mathbb{Q}$ we have made multiplication by 2 invertible.

$$\frac{a}{b} \otimes 1 = \frac{2a}{2b} \otimes 1 = \frac{a}{2b} \otimes 0 = 0$$

By a similar argument, $\mathbb{Q}/\mathbb{Z} \otimes \mathbb{Z}_2 = 0$.

Thus we get $0 \to \mathbb{Z}_2 \to 0 \to 0 \to 0$

which is not exact.

//

(ii) $\hom_R(M, -)$ is not exact.

Let $R = \mathbb{Z}$, $M = \mathbb{Z}_2$

consider the short exact sequence

$$0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$
$$\parallel$$
$$\mathbb{Z}_2$$

applying $\hom_{\mathbb{Z}}(\mathbb{Z}_2, -)$

$$0 \to \hom_{\mathbb{Z}}(\mathbb{Z}_2, 2\mathbb{Z}) \to \hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) \to \hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \to 0$$

Well, $\hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_2$

$\hom_{\mathbb{Z}}(\mathbb{Z}_2, 2\mathbb{Z}) = 0$

$\hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) = 0$

thus we get

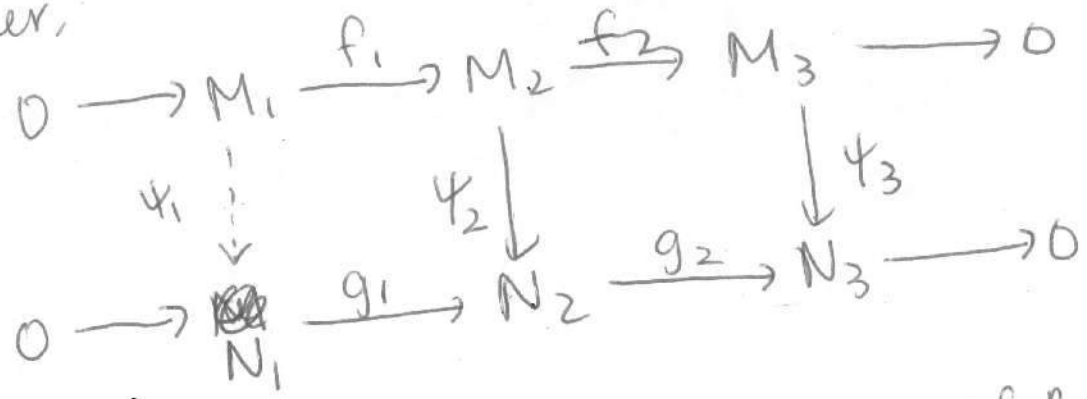
$$0 \to 0 \to 0 \to \mathbb{Z}_2 \to 0$$

which is not exact. //

2007 B2:

Let R be a ring and M_i, N_i $i=1,2,3$ be R-mod.

consider,



with exact rows (all maps are homom of R-mods).

i) suppose $\exists\ \psi_3 \in \mathrm{HOM}_R(M_3, N_3)$ s.t. $g_2\psi_2 = \psi_3 f_2$.

Prove $\exists\ \psi_1 \in \mathrm{HOM}_R(M_1, N_1)$ making the diagram commute. ($g_1\psi_1 = \psi_2 f_1$)

Pf:

Let $m_1 \in M_1$

$\Rightarrow \exists\ m_2 \in M_2$ s.t. $f_1(m_1) = m_2$

note $f_1(m_1) = m_2 \in \mathrm{Im} f_1 = \ker f_2$.

So $g_2\psi_2(m_2) = \psi_3 f_2(m_2) = \psi_3(0) = 0$ (b/c $m_2 \in \ker f_2$)

$\Rightarrow \psi_2(m_2) \in \ker g_2 = \mathrm{Im}\, g_1$

So $\exists\ n_1 \in N_1$ s.t. $g_1(n_1) = \psi_2(m_2) = \psi_2(f_1(m_1))$

Define $\psi_1(m_1) = n_1$

Well-defined:

let $m_1 = m_1'$ where $m_1, m_1' \in M_1$

Since f_1 is a homom. $f_1(m_1) = f_1(m_1') \in \mathrm{Im} f_1 = \ker f_2$

let $m_2 = f_1(m_1)$ and $m_2' = f_1(m_1')$
where $m_2 = m_2'$

So $f_2(m_2) = 0$

$\Rightarrow \psi_3 f_2(m_2) = \psi_3(0) = 0$

so $g_2 \psi_2(m_2) = 0$ (since $g_2 \psi_2 = \psi_3 f_2$)

thus $\psi_2(m_2) \in \ker g_2 = \text{Im } g_1$

so $\exists\ n_1 \in N_1$ s.t. $g_1(n_1) = \psi_2(m_2)$

likewise $\psi_2(m_2') \in \text{Im } g_1$

since $m_2 = m_2'$, and ψ_2 w.d. $\psi_2(m_2) = \psi_2(m_2')$

~~since g_1 is injective etc~~

so $g_1(n_1) = \psi_2(m_2) = \psi_2(m_2')$

$g_1(n_1) = \psi_2(f_1(m_1)) = \psi_2(f_1(m_1'))$

$g_1(n_1) = g_1 \psi_1(m_1) = g_1 \psi_1(m_1')$

since g_1 is injective.

$n_1 = \psi_1(m_1) = \psi_1(m_1')$

thus ψ_1 is well-defined & $\psi_2 f_1 = g_1 \psi_1$

NTS ψ_1 is a homom: ($\psi_1(rm_1 + m_1') = r\psi_1(m_1) + \psi_1(m_1')$)

Well, $g_1 \psi_1(rm_1 + m_1') = \psi_2 f_1(rm_1 + m_1')$

$= r\psi_2 f_1(m_1) + \psi_2 f_1(m_1')$

$= r g_1 \psi_1(m_1) + g_1 \psi_1(m_1')$

$= g_1(r\psi_1(m_1) + \psi_1(m_1'))$

$\Rightarrow \psi_1(rm_1 + m_1') = r\psi_1(m_1) + \psi_1(m_1')$ since g_1 1-1.

$\Rightarrow \psi_1$ is a homom.

which conditions should satisfy ψ_2 and/or ψ_3 to ensure that ψ_1 is injective?

Suppose ψ_2 is injective.

Let $m_1, m_1' \in M_1$ s.t. $\psi_1(m_1) = \psi_1(m_1')$

so $g_1 \psi_1(m_1) = g_1 \psi_1(m_1')$

$\psi_2 f_2(m_1) = \psi_2 f_1(m_1')$ ↓(b/c ψ_2 1-1)

$f_1(m_1) = f_1(m_1')$ ↓(b/c f_1 1-1)

$m_1 = m_1'$

thus ψ_1 is injective. //

for (ii) see 2011 Qual

2007 B5

Let R, S be comm. rings, $\phi: R \to S$ a ring homom.

i) Extend ϕ to a ring homom $\bar{\phi}: Mat_n(R) \to Mat_n(S)$ and show that $\det(\bar{\phi}(A)) = \phi(\det(A))$ $\forall$ $A \in Mat_n(R)$

note: $\det(A) = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ where $A = (a_{ij})$

$$\phi(\det(A)) = \phi\left(\sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}\right)$$

$$= \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\, \bar{\phi}(a_{1\sigma(1)}) \cdots \bar{\phi}(a_{n\sigma(n)})$$

$$= \det(\bar{\phi}(A)).$$

ii) Use part (i) to prove that the constant term of the characteristic poly of a matrix $A \in Mat_n(R)$ equals $(-1)^n \det(A)$.

the characteristic poly $= |xI_n - A| = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$

if we evaluate the characteristic poly at 0, we will be left with the constant term of the characteristic polynomial c_0.

$$c_0 = ev_0|xI_n - A|$$

$$= |ev_0(xI_n - A)| \quad \text{by (i)}$$

$$= |0 \cdot I_n - A|$$

$$= |-A| = (-1)^n |A|.$$

$$= (-1)^n \det(A). \quad //$$

2006 Chari

Part B.

1. (a) Let R be a ring with identity and M a left module for R. Recall that M is indecomposable if M cannot be written as a direct sum of two non-zero submodules. Prove that if $f : M \to M$ is a homomorphism of modules then $f^2 = f$ implies that either $f = 0$ or $f = \mathrm{id}_M$.

   (b) Suppose now that M is decomposable. Prove that there exists $f : M \to M$ a homomorphism of modules such that $f^2 = f$ and f different from zero and the identity.

2. Suppose that R is a ring with identity and $e \in R$ is such that $e^2 = e$.

   (a) Prove that $(1 - e)$ has the same property.

   (b) Prove that $Re \cap R(1 - e) = \{0\}$ and hence $R = Re \oplus R(1 - e)$.

   (c) Prove that the R-module Re is projective.

3. Let R be a ring with identity. Regard R as a right R-module in the usual way and let M be a right R-module. Prove that $\hom_R(R, M) \simeq M$ as abelian groups.

4. Consider the ring $R = \mathbf{C}[x]$ of polynomials in an indeterminate x with coefficients on $\mathbf{C}$.

   (a) Let M be a torsion free module for R with two generators. Prove that M is free of rank at most two.

   (b) Prove that if M is a cyclic R-module and $M \neq R$ then M is torsion. Under what condition on the torsion ideal will M be simple?

5. (a) Prove that if A and B are invertible $n \times n$ matrices with entries in an integral domain R, then $A + rB$ is invertible in the quotient field K for all but finitely many r.

   (b) Prove that the minimal polynomial of a linear transformation of an n-dimensional vector space has degree at most n.

5. Suppose that Φ and Ψ are commuting linear transformation of an n-dimensional vector space E. Prove that if E_1 is a Φ-invariant subspace of E then E_1 is also Ψ-invariant. Use this to prove that if Φ and Ψ both have linear elementary divisors then there exists a basis of E with respect to which the matrix Φ and the matrix Ψ are both diagonal.

Winter 2006

2005 Ran

Part B.

1. Let $\varphi : R \to S$ be a homomorphism of commutative unitary rings, $I < R$, $J < S$ ideals. Prove or disprove each of the following assertions.

   (i) $\varphi(I)$ is an ideal in S.

   (ii) If J is a prime ideal, so is $\varphi^{-1}(J)$.

   (iii) If J is a maximal ideal, so is $\varphi^{-1}(J)$.

2. Let R be a commutative integral domain, $S \subset R$ a multiplicative system and M an R-module. Prove directly from the definitions that

$$S^{-1}M \simeq S^{-1}R \otimes_R M$$

   (isomorphic as R-modules).

3. (i) Determine with proof $\hom_{\mathbf{Z}}(\mathbf{R}, \mathbf{Z})$.

   (ii) Determine with proof whether $\mathbf{R}$ is a projective $\mathbf{Z}$-module.

4. Determine with proof whether the following $\mathbf{Z}$-modules are injective:

   (i) $\mathbf{Q}$,

   (ii) $\mathbf{Z}/12$.

5. (i) Let

$$M = \begin{pmatrix} 0 & 0 & 0 & 4 \\ 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

   Determine with proof the invariant factor and elementary divisor decompositions of the $\mathbf{Q}[x]$-module corresponding to M.

   (ii) Ditto with $\mathbf{Q}$ replaced by $\mathbf{R}$.

   (iii) Let

$$M' = \begin{pmatrix} 0 & 0 & 0 & 3 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{pmatrix}.$$

   Determine with proof whether M and M' are similar as matrices over $\mathbf{Q}$ or $\mathbf{R}$.

   (iv) Ditto with M' replaced by

$$M'' = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 3 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{pmatrix}.$$

2004 (OCT)

Ran 9.

Part B.

1. Let R be a ring.

(i) Prove that if R is unitary, then any left (resp. right, 2-sided) ideal is contained in a maximal left (resp. right, 2-sided) ideal.

(ii) Prove that if R is unitary and commutative, then an ideal I of R is maximal iff R/I is a field.

2. (i) Prove that any nontrivial subgroup of $\mathbf{Z}^2$ is isomorphic to $\mathbf{Z}$ or $\mathbf{Z}^2$ but not to both.

(ii) Let A be a subgroup of $\mathbf{Z}^2$ isomorphic to $\mathbf{Z}^2$. Prove that $\mathbf{Z}^2/A$ is finite.

3. (i) Decompose the following as a direct sum of cyclic groups:

(a) $\mathbf{Z}_{12} \oplus \mathbf{Z}_9$.

(b) $\hom(\mathbf{Z}_{12}, \mathbf{Z}_9)$.

(ii) Let A, B be finitely generated abelian groups. Prove that $\hom(A, B)$ is finitely generated.

4. (i) Let

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Determine with reason the invariant factor and elementary divisor decompositions of the $\mathrm{R}[x]$-module corresponding to M.

(ii) Let M be an $n \times n$ matrix such that $M^2 = M$. Prove that there exists $0 \leqslant r \leqslant n$ such that M is similar to the block matrix

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

WINTER 2004

2004 (Apr)

Rank 2 rush?

Part B.

1. Let I and J be ideals in a commutative unitary ring R such that $I + J = R$ and let A be a left R-module. Show that $A/(I \cap J)A \simeq A/IA \times A/JA$.

2. Let p be a prime integer and let $Z(p^\infty)$ be the subgroup of the additive group $\mathbf{Q}/\mathbf{Z}$ generated by the cosets of the form $1/p^i + \mathbf{Z}$, $i \in \mathbf{Z}$, $i \geqslant 0$. Let A be a subgroup of a finitely generated group B. Show that any homomorphism $f : A \to Z(p^\infty)$ extends to a homomorphism $g : B \to Z(p^\infty)$.

3. Give an example of a monomorphism $f : A \to B$ of abelian groups and an abelian group C such that the induced homomorphism $\hom_{\mathbf{Z}}(B, C) \to \hom_{\mathbf{Z}}(A, C)$ is not onto.

4. (a) Sketch the construction of $A \otimes_R B$.
   (b) State the universal property of $A \otimes_R B$.

5. Let R be a commutative ring with identity and let X be a indeterminate. Let M be a maximal ideal of $R[X]$ such that $M \cap R = P$ is a maximal ideal of R. Show that $M = fR[X] + PR[X]$ for some monic $f \in R[X]$ such that the image of $\overline{f}$ of f in $(R/P)[X]$ is irreducible. ($\overline{f}$ is obtained from f by reducing coefficients mod P).

6. Give an example of an integral domain R which is not a UFD although each element of R factors into irreducibles in R. Justify your assertions.

Winter 2003?

2003

Rush

Part B.

1. Let I and J be ideals of a commutative unitary ring R. Show that $I + J = R$ implies that $I \cap J = IJ$, and if R is a PID, the converse holds.

2. Let A and B be commutative unitary rings. Given that $A \otimes_{\mathbf{Z}} B$ is a commutative unitary ring with multiplication satisfying $(a_1 \otimes_{\mathbf{Z}} b_1)(a_2 \otimes_{\mathbf{Z}} b_2) = (a_1 a_2) \otimes_{\mathbf{Z}} (b_1 b_2)$, for $a_i \in A$, $b_i \in B$, show that the coproduct of A and B exists in the category of commutative unitary rings and unitary ring homomorphisms.

3. Let R be a commutative ring with unique maximal ideal M. Let A be the smallest subring of R containing the multiplicative identity 1 of R. Show that A is a ring isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}/p^n\mathbf{Z}$ for some $p, n \in \mathbf{N}$ with p prime. (Hint: Consider the idempotents of R).

4. Let R be a commutative Noetherian ring. (So each ideal of R is finitely generated). Show that each submodule N of a finitely generated R-module M is finitely generated.

5. Let $O \to A \to B \to C \to 0$ be an exact sequence of R-modules.

   (a) What part of the sequence $0 \to \hom_R(C, D) \to \hom_R(B, D) \to \hom_R(A, D) \to 0$ is exact for every left R-module D? (No proofs required).

   (b) Show that the remaining part is exact if and only if the sequence $0 \to A \to B \to C \to 0$ splits.

6. Let K be a field and let M and N be finitely generated modules over the polynomial ring $K[X]$. Suppose M has invariant factors $(X-1), (X-1)(X-2)^2, (X-1)(X-2)^2(X-3)$, and N has invariant factors $(X-2)(X-3)^2, (X-2)^2(X-3)^2(X-5)$.

   (a) Give the elementary divisors of $M \oplus N$.

   (b) Give the invariant factors of $M \oplus N$.

Winter 2003

2002

Part B.

1. Let

$$A = \begin{pmatrix} 0 & & & & & & & & & \\ & 2 & & & & & & & & \\ & & -1 & & & & & & & \\ & & & 0 & & & & & & \\ & & & & 1 & & & & & \\ & & & & & -1 & & & & \\ & & & & & & 0 & 1 & & \\ & & & & & & & 0 & & \\ & & & & & & & & 0 & 1 & 0 \\ & & & & & & & & & 0 & 1 \\ & & & & & & & & & & 0 \end{pmatrix}.$$

(i) Find the minimal polynomial, the rational canonical form.

(ii) How many independent eigenvectors does A have? (Explain).

2. Let V be a n-dimensional vector space over k.

(i) Define the tensor algebra $T(V)$, the alternating algebra $\Lambda(V)$, and the symmetric algebra $S(V)$, and make them graded k-algebras.

(ii) What are the dimensions of $T^r(V)$, $\Lambda^r(V)$, and $S^r(V)$? (Explain).

(iii) Prove that $\Lambda^r V = 0$ for $r > n$.

Prove or disprove 3 – 9.

3. Let R be any ring, and let A, B, C, D be R-modules. If $0 \to A \to B \to C \to 0$ is a short exact sequence of R-modules, then

(i) $0 \to \hom_R(D, A) \to \hom_R(D, B) \to \hom_R(D, C) \to 0$ is a short exact sequence of R-modules.

(ii) $0 \to \hom_R(C, D) \to \hom_R(B, D) \to \hom_R(A, D) \to 0$ is a short exact sequence of R-modules.

4. Let R, A, B, C, D be as in (3), and $0 \to A \to B \to C \to 0$

(i) $0 \to A \otimes_R D \to B \otimes_R D \to C \otimes_R D \to 0$

(ii) $A \otimes_R B \simeq A \otimes_R C \implies B \simeq C$.

5. (i) A torsion-free module is projective.

(ii) A projective module is torsion-free.

(iii) A torsion-free module is free.

6. (i) A free module is torsion-free.

Winter 2002

(ii) A projective module is free.

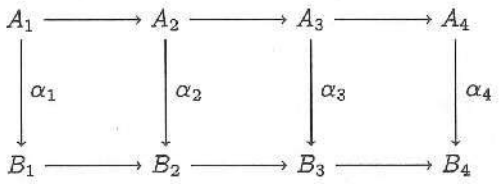
(iii) A free module is projective.

7. (i) A submodule of a free module is free.

(ii) A submodule of a finitely generated module is finitely generated.

8. $x^{10} + \pi x^7 + \pi x + \pi$ is irreducible over $\mathbf{Q}$.

9. Referring to the commutative diagram below: α_4 is one-to-one and α_1, α_3 are onto implies α_2 is onto.



2001 Rush

Part B.

1. Let R be an integral domain. Show that R is a PID if each finitely generated torsion-free R-module is free.

2. Show that if $\hom_R(D, -)$ preserves exactness of $0 \to A \to B \to C \to 0$ for each D, the sequence $0 \to A \to B \to C \to 0$ splits.

3. If X, Y are independent indeterminates over the commutative ring R, show $R[X] \otimes_R R[Y] \simeq R[X, Y]$ as R-algebras.

4. Let B be an abelian group and let A be a subgroup of B. Show that any homomorphism $f : A \to \mathbf{Q}/\mathbf{Z}$ extends to a homomorphism $\overline{f} : B \to \mathbf{Q}/\mathbf{Z}$.

5. Let R be a commutative unitary ring. Show that each injective R-module is divisible.

6. Prove that 3×3 matrices A and B over a field K are similar if they have the same minimal polynomials and the same characteristic polynomials.

Winter 2001

2000

Part B.

1. Give examples of abelian groups A, B satisfying

   (i) $A \otimes B = 0$

   (ii) $A \otimes A \simeq A$.

2. Let R be a ring with identity. Assume that M is a simple module for R. Prove that M is cyclic and that any non-zero R module endomorphism of M is an isomorphism.

3. Prove that a module P over a ring R is projective if and only if P is a summand of a free module.

4. If A is any abelian group, compute $\hom(\mathbf{Z}_m, A)$. What can you say about $\mathbf{Z}_m^*$?

5. Prove that a free module over a pid is torsion free and give an example to show that the converse is false.

6. What are the invariant factors of $\mathbf{Z}_n \oplus \mathbf{Z}_m$, regarded as modules over $\mathbf{Z}$.

7. Prove that if $m > n$, any alternating multilinear form on $(R^n)^m = 0$, here R is any commutative ring.

8. Prove that if q is the minimal polynomial of a linear transformation of vector space E, then $\deg q \leqslant \dim E$.

Winter 2000

1999

Parts A and B.

1. Let $K \subseteq H$ be subgroups of the finite group G, which are not necessarily normal. Show $(G : K) = (G : H)(H : K)$, where the notation $(A : B)$ denotes the number of left cosets of B in A.

2. Let the group G operate on the set S, and suppose that $s, t \in S$ are in the same orbit under the operation. Show that the isotropy groups G_s and G_t are conjugate. That is, there exists $g \in G$ such that $g^{-1}G_s g = G_t$. (Recall that $G_s = \{x \in G : gs = s\}$).

3. Show that each group of order p^2, p prime, is abelian.

4. (a) Define *free group* $F(X)$ *on a set* X.
   (b) Define *coproduct* $(G, \{\varphi_i\}_{i \in I})$ *of a family* $\{G_i : i \in I\}$ of groups.
   (c) Show that if $(G, \varphi_1, \varphi_2)$ is a coproduct of G_1 and G_2 with G_i isomorphic to the additive group of integers $\mathbf{Z}$, then $G \simeq F(\{a, b\})$.
   (d) Is $F(\{a, b\})$ abelian?

5. Show that the direct sum of an arbitrary family of injective abelian groups is injective. (Hint: Divisible).

6. (a) Determine the units in $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\}$.
   (b) Show that $1 + \sqrt{-5}$ and 2 are irreducible in $\mathbf{Z}[\sqrt{-5}]$.

7. (a) Give an example of an integral domain R and ideals I and J of R such that $IJ \neq I \cap J$.
   (b) Show that if $I + J = R$ then $IJ = I \cap J$.

8. Give an example of a monomorphism $f : A \to B$ of abelian groups and an abelian group C such that the induced homomorphism $\hom_{\mathbf{Z}}(B, C) \to \hom_{\mathbf{Z}}(A, C)$ is not onto.

Fall/Winter 1998/1999

9. Show that if R is a PID and $M = R/a_1R \oplus R/a_2R \oplus \cdots \oplus R/a_mR$, with $R \neq a_1R \supseteq a_2R \supseteq \cdots \supseteq a_mR$, then M cannot be generated by fewer than m-elements.

10. Let

$$A = \begin{pmatrix} 2 & & & & & & & \\ & -1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & 1 & 1 & & & \\ & & & & & -1 & & \\ & & & & & & 2 & \\ & & & & & & & -1 \end{pmatrix}.$$

Find the minimal polynomial and the rational canonical form of A.

Fall/ Winter 1998/1999

1998

Part B.

Throughout R denotes a commutative ring with unit element, M a unitary R-module and k a field.

1. (i) Prove that if R is an integral domain with fraction field K and M is a torsion-free R-module, then M is isomorphic to an R-submodule of the K-vector space $M \otimes_R K$.

   (ii) Prove (from scratch) that if R is a principal ideal domain and M a finitely generated torsion-free R-module such that $M \otimes_R K$ is 1-dimensional as K-vector space, then $M \simeq R$ as R-modules (i.e. M is free of rank 1).

   (iii) Give (with proof) an example of two nonzero $\mathbf{Z}$-modules whose tensor product is zero.

   (iv) Prove that if R is an integral domain but not a field then its field of fractions is torsion-free, but is not a submodule of a free R-module.

2. (i) State with proof a correspondence between {pairs (V, L) where V is a finite-dimensional k-vector space and L is a and {finitely generated torsion $k[X]$-modules M}.

   (ii) Determine with proof the pair (V, L) corresponding to a cyclic $k[X]$-module $k[X]/(f)$, $f \in k[X]$ nonzero, and compute the minimal polynomial and the characteristic polynomial of L.

   (iii) In the general case, interpret with proof the minimal polynomial and the characteristic polynomial of a linear transformation L in terms of the corresponding module M.

3. Let V be an n-dimensional k-vector space.

   (i) State the definition of $\Lambda^m(V)$;

   (ii) Prove that if $m > n$ then $\Lambda^m(V) = 3D(0)$.

   (iii) Prove that the dimension of $\Lambda^2(V)$ is $\binom{n}{2}$.

Winter 1998

1997

Part B.

1. Describe all maximal ideals in $\mathbf{Z}[x]/((x-a)^n)$, where $n, a \in \mathbf{Z}$, $n \geqslant 1$. Prove your answer.

2. Let A be a left module over a ring R. Construct a canonical R-module homomorphism

$$\theta : A \to A^{**},$$

where, for any left or right R-module B, $B^* := \hom_R(B, R)$. Give a sufficient condition on R and A for θ to be an isomorphism.

3. Let R be a non-zero commutative ring with unity such that every submodule of any free R-module of finite rank is itself free. Prove that R is a principal ideal domain.

4. Prove that any maximal linearly independent subset X of a (left) vector space V over a division ring D is a basis of V.

Winter 1997

1996

Part B.

1. Describe all maximal ideals in the polynomial ring $\mathbf{C}[x_1, \ldots, x_n]$. Prove your answer.

2. Let R be a ring. A left R-module M is called *simple* iff $M \neq \{0\}$ and M has no proper submodule. Prove that for any simple left R-module the endomorphism ring $\hom_R(M, M)$ is a division ring.

3. Consider the $\mathbf{C}[x]$-module structure on $\mathbf{C}^n$ defined by

$$p(x).v = (p(A))(v),$$

where $v \in \mathbf{C}^n$, $p(x) \in \mathbf{C}[x]$, and A is the $n \times n$-matric

$$\begin{pmatrix} 0 & & & \\ i & 0 & & \\ & \ddots & \ddots & \\ & & i & 0 \end{pmatrix}$$

(where $i^2 = -1$). Decompose $\mathbf{C}^n$ according to the structure theorem for modules over principal ideal domains.

4. Let V be an n-dimensional vector space over $\mathbf{R}$. Establish a canonical isomorphism between $\Lambda^k(V)$ and $\Lambda^{n-k}(V^*) \otimes_{\mathbf{R}} \Lambda^n(V)$, where k is any fixed positive integer less than or equal to n and V^8 is the space dual to V. (A canonical isomorphism between two vector spaces V' and V'' is an isomorphism which does not depend on the choice of bases in V' and V'').

Winter 1996

1995

Part B.

In problems 1,2 and 4, R is a commutative ring with 1, and all R-modules considered are assumed to be unitary.

1. (a) Define: an R-module is *projective*.

(b) Prove that if R is a field then any R-module is projective.

2. (a) Given R-modules M and N, and their tensor product $A = M \otimes_R N$ as an abelian group, state a way of making each element of R act on A so that A becomes an R-module.

(b) Prove that the action you gave in part (a) is well-defined.

3. (a) Suppose F is a given field, and that c and d are two distinct elements of F. Determine the number of similarity classes of matrices (over F) with characteristic polynomial

$$(x-c)^2(x-d)^2.$$

(b) State the result for finite abelian groups which corresponds to your result for part (a).

4. Let M be an R-module, and let H be the set of all m in M such that $rm = 0$ implies $r = 0$ or $m = 0$.

(a) Prove that if R is a principal ideal domain (PID) and M is cyclic then H is a submodule of M.

(b) Is the result in part (a) true if the hypothesis that R is a PID is just deleted? Give a proof or counterexample.

1995
Winter 2008

1994 (Sept)

Part B.

1. Let
$$p(x) = x^2 + x + 1, \qquad q(x) = x^4 + 3x^3 + x^2 + 6x + 10.$$
Find all integers $\geqslant 10$ such that $p(x)$ divides $q(x)$ in $\mathbf{Z}_n[x]$.

2. Let R be a commutative ring and I an ideal of R. Let M be an ideal of R containing I, and let $\overline{M} = M/I$ be the corresponding ideal of R/I. Prove that M is maximal if and only if $\overline{M}$ is maximal.

3. A module M for a ring R is called *simple* if $M \neq \{0\}$ and M has no proper submodule, i.e. if $N \subseteq M$ is a submodule, then $N = \{0\}$ or M. Let M and M' be two simple modules and let $\varphi : M \to M'$ be a module homomorphism. Prove that φ is either zero or an isomorphism.

4. Let I be an ideal in a ring R. Prove that if R/I is a free R-module, then $I = \{0\}$.

5. (a) Prove that a module P over a ring R is projective if and only if for any surjective homomorphism of R-modules
$$\varphi : N \to N',$$
the corresponding homomorphism of abelian groups
$$\hom_R(P, N) \to \hom_R(P, N')$$
is surjective.

   (b) Prove that
$$\mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}_5 = 0.$$

1994 (Feb)

Part B.

1. Find all possible Jordan forms for 8×8 matrices with minimal polynomial $x^2(x-1)^3$.

2. Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of R-modules and homomorphisms such that each row is exact. If two of the vertical maps are injective, what about the third? Consider all three cases.

3. Prove or disprove that every 2×2 matrix over $\mathbf{Z}[X]$ is diagonalizable by row and column operations.

4. Which of the implications: free iff projective iff torsion-free hold? Give proofs or counterexmaples.

5. Compute $\hom_{\mathbf{Z}}(\mathbf{Z}_2, \mathbf{R})$ where $\mathbf{R}$ is the additive group of real numbers.

1993

Part B.

In problems 1-4, give an example and show that your example has the desired properties.

1. A ring that does not have the invariant dimension property.

2. A module D and an exact sequence $0 \to A \to B \to C \to 0$, which shows that neither $\hom_R(-, D)$ nor $\hom_R(D, -)$ is an exact functor.

3. A projective module which is not free.

4. A submodule of a finitely generated module which is not finitely generated.

5. What is $\mathbf{C} \otimes_{\mathbf{Z}} \mathbf{Z}_{10}$, where $\mathbf{C}$ is the complex numbers?

6. Let R be a commutative ring with identity and M be an R-module.
   (a) Outline the construction of the tensor algebra $T(M)$ and the exterior algebra $\Lambda(M)$.
   (b) Give the universal property of $T(M)$.
   (c) Show that if M is free of dimension n and $1 \leqslant k \leqslant n-1$, then $\Lambda^k(M) \simeq \Lambda^{n-k}(M)$.

7. Let

$$A = \begin{pmatrix} -1 & & & & & & & \\ & 2 & & & & & & \\ & & -1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & 1 & & \\ & & & & & 1 & & \\ & & & & & & -1 & \\ & & & & & & & 2 \\ & & & & & & & & -1 \end{pmatrix}.$$

Find the minimal polynomial, the rational canonical form, and all eigenvectors of A.