

**MAT 535, ALGEBRA II, SPRING 2001
FINAL EXAM**

NAME :

SSN :

**THERE ARE SIX PROBLEMS.
THEY DO NOT HAVE EQUAL VALUE.
SHOW YOUR WORK!!!**

YOU MAY USE ANY RESULT DISCUSSED IN CLASS, IN THE HOMEWORKS OR ANY THEOREM FROM ARTIN, HUNGERFORD OR THE NOTES I HAVE DISTRIBUTED. HOWEVER, PLEASE SAY WHICH RESULT(S) YOU ARE USING (FOR EXAMPLE “BY THE STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER A P.I.D.” UNLESS IT IS OBVIOUS.

WORK ALONE. DO NOT USE OR CONSULT ANY OTHER TEXT OR PERSON. ANY VIOLATION OF THESE SIMPLE RULES IS CHEATING.

PLEASE:
HAND-IN A READABLE SET OF SOLUTIONS! THE TEST IS POSTED ON THE WEB : YOU CAN MAKE A COPY IF YOU NEED. USE ONLY THE SPACE GIVEN (FRONT PAGES ONLY!).

THIS IS A TAKE-HOME TEST. RETURN IT IN PERSON TO MY OFFICE, MATH TOWER ROOM 3-115 **ON MONDAY MAY 14, 12 NOON**. NO EXCEPTIONS. IF YOU CANNOT RETURN IT TO ME AT 12 NOON, YOU STILL HAVE TO HAND-IN THE TEST BY THAT TIME AND DAY; IN THIS CASE MAKE AND KEEP A COPY, SLIDE THE ORIGINAL UNDER THE DOOR AND E-MAIL (*mde@math.sunysb.edu*) ME IMMEDIATELY THAT YOU HAVE DONE SO.

1. Prove that every element of a finite field E can be written as the sum of two squares of elements in E .

Hints: There are several ways to solve this problem. The following hints point to one solution.

1) Do first the case of $\text{char } E = 2$.

2) Study the group homomorphism $s : E^* \rightarrow E^*$, $s(a) = a^2$; consider $E^*/s(E^*)$ and how E^* gets subdivided into cosets; consider what happens to these subdivisions if you multiply by elements in E^* .

3) Consider $f : E \rightarrow E$ given by $f(b) = 1 - b$.

Let $p := \text{char } E$.

If $p = 2$, since E is finite, Frobenius, $c \rightarrow c^2$, is bijective and every element is a square, $a = b^2$, and we are done $a = b^2 + 0^2$.

Let $p \neq 2$.

Let $s : E^* \rightarrow E^*$ be defined as $s(a) = a^2$. It is a group homomorphism with kernel $\{1, -1\}$. Let $S := s(E^*) \subset E^*$ be the image, i.e. the set of squares. $[E^* : S] = 2$. Let $T = E^* \setminus S$. We have $|S| = |T|$.

The following can be checked immediately:

1) if $b \in S$, then $bS = S$ and $bT = T$;

2) if $b \in T$, then $bS = T$ and, by cardinality reasons, $bT = S$.

Let $E^{**} = E \setminus \{0, 1\}$.

Define $S^* = S \setminus \{1\}$.

$E^{**} = S^* \amalg T$.

Let $f : E^{**} \simeq E^{**}$ be the bijection $u \mapsto 1 - u$.

Since $|S^*| = |T| - 1$, $f(T) \cap T \neq \emptyset$.

Let $v \in f(T) \cap T$.

Now we can solve the problem.

Let $a \in S$. Then we are done.

Let $a \in T$. Then by 2) above, $va \in S$ and $(1 - v)a \in S$.

Clearly $a = va + (1 - v)a$ and we are done.

Remark. In reality the above can be summarized by first realizing that in char 2 the problem is trivial and in the other characteristics squaring is a group homomorphism with image of index two and this suggests trying to find the solution by some parity argument.

2. Let G be a group. Let H and K be subgroups. We consider right cosets only.

a) Prove that K acts by right translation on G/H and that there is a natural bijection between the set of K -orbits $(G/H)/K$ and the set of H -orbits $(G/K)/H$.

b) Prove that G acts on the set $G/H \times G/K$ by right translation and find a bijection

$$(G/H \times G/K)/G \longrightarrow (G/H)/K$$

between the set of orbits G -orbits in $G/H \times G/K$ and $(G/H)/K$.

c) Let $H = K$. Determine the fixed points of the H -action on G/H , i.e. the right cosets Hg such that $(Hg)h = Hg, \forall h \in H$.

a) As to the K -action, the only real thing to check is that $(Hg)k := Hgk$ is well defined. Since $Hg = Hg'$ iff $gg'^{-1} \in H$ iff $gk(g'k)^{-1} \in H$ iff $Hgk = Hg'k$.

A bijection is given by $\overline{Hg} \rightarrow \overline{Kg^{-1}}$, where we denote by $\overline{Hg} \in (G/H)/K$ the K -orbit of Hg . etc. Well defined: Kg^{-1} and $K(hgk)^{-1}$ are in the same H -orbit for every $h \in H$ and $k \in K$. Surjectivity is obvious. Injectivity: follows from $g = htk$ for some $h \in H$ and some $k \in K$ iff $g^{-1} = k't^{-1}h'$ for some $k' \in K$ and some $h' \in H$.

b) A bijection is given by

$$\overline{(Ha, Kb)} \longrightarrow \overline{Hab^{-1}}.$$

You argue as above.

c) $(Hg)h = Hg, \forall h \in H$ iff $ghg^{-1} \in H, \forall h \in H$, i.e. iff $g \in N$, the normalizer of H in G . The set of fixed points is $N/H \subseteq G/H$.

3. Compute the Galois group of

$$f = x^3 - x^2 + x + 1$$

a) over \mathbb{Q} ;

b) over $E := \mathbb{Q}(i\sqrt{11})$.

First of all, note that f does not have a rational root: a root $u = c/d$ would have to be either 1 or -1 by Hungerford III, Proposition 6.8 (discussed in class and elementary). Since the degree of f is three, f is irreducible over \mathbb{Q} . Since the characteristic is zero, the roots are all distinct.

a) For $g = x^3 + ax^2 + bx + c$, the discriminant is

$$D(g) = a^2(b^2 - 4ac) - 4a^3 - 27c^2 + 18abc.$$

You can also “complete the cube” and use the shorter formula. $D = D(f) = -44$. D is not a perfect square in \mathbb{Q} . By the general theory, the Galois group G of the splitting field is $G = S_3$.

b) $D = -44 = (2i\sqrt{11})^2$. Note that $\Delta = \Delta(f) = 2i\sqrt{11}$, up to a sign. $E = \mathbb{Q}(\Delta) =$ the field fixed by $A_3 < S_3$ (as discussed in class). The Galois group is A_3 .

4. Let $f : \mathbb{Z}^3 \rightarrow \mathbb{Z}^3$ be the \mathbb{Z} -linear map defined by the matrix A :

$$\begin{bmatrix} 2 & 3 & -4 \\ 2 & 6 & 0 \\ 2 & 6 & -4 \end{bmatrix}$$

i.e. view elements \mathbb{Z}^3 as column vectors, v , of integers and set $f(v) := Av$. Let $K := \text{Ker } f$ and $C = \text{Coker } f$.

Note, but do not prove, that K and C are finitely generated abelian groups, so that they are both isomorphic to a direct sum of finitely many cyclic groups.

a) Compute K and C , i.e. determine the cyclic groups appearing in their direct sum decomposition.

b) Let B be any $n \times n$ matrix of integers and use it to define a \mathbb{Z} -linear map $g : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ as above. Prove that if g has non-zero determinant, then $\text{Coker } g$ is a finite abelian group.

Hint: Consider the operation $- \otimes_{\mathbb{Z}} \mathbb{Q}$.

a) The matrix has non zero determinant. Viewed as a linear map $\mathbb{Q}^3 \rightarrow \mathbb{Q}^3$ the map has no kernel so that it has no kernel: $K = \{0\}$ the trivial cyclic group.

Viewing C as cosets, the elements of C can be described using a row vector of integers modulo elements in the image of f .

We can therefore perform elementary row operations on A like switching rows and adding or subtracting integer multiples of rows to a given row.

By doing so, one obtains the matrix B :

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

We can therefore describe the elements of C using three vectors v_1, v_2 and v_3 subject to $2v_1 = 0, 3v_2 = 0$ and $4v_3 = 0$.

$$C \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4.$$

b) Consider the exact sequence:

$$\mathbb{Z}^n \xrightarrow{f} \mathbb{Z}^n \xrightarrow{p} C \rightarrow 0,$$

where p is the natural quotient map. Note that $p \circ f = 0$. By tensoring with \mathbb{Q} we get the sequence

$$\mathbb{Q}^n \xrightarrow{g} \mathbb{Q}^n \xrightarrow{p' := p \otimes Id_{BbbQ}} C \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow 0,$$

with $p' \circ g = 0$ and p' surjective (note that, as discussed in class, tensoring does not destroy surjectivity, only, possibly, injectivity). Since g is an isomorphism by assumption, $p' = 0$. Since p' is surjective and trivial, $C \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. It follows that C , which is a finitely generated abelian group (it is a quotient of \mathbb{Z}^n), has no free summand and is a finite direct sum of finite cyclic groups.

NB: The converse is also true.

5.

a) Let R be a principal ideal ring, i.e. every ideal $I \subseteq R$ is principal. Let $f : R \rightarrow S$ be a surjective ring homomorphism. Prove that S is a principal ideal ring.

b) Let N be a positive integer and

$$f_N(x) := \prod_{n=0}^N (x - n) \in \mathbb{Q}[x].$$

Determine all the ideals of the quotient ring

$$\mathbb{Q}[x]/(f_N(x)).$$

a) Let J be an ideal in S . Since f is surjective, $I := f^{-1}(J)$ is an ideal and it is principal, say $I = (r)$. It is routine to check that $J = (f(r))$.

b) Define a ring homomorphism

$$u : \mathbb{Q}[x]/(f_N(x)) \rightarrow \prod_{n=0}^N \mathbb{Q}[x]/(x - n)$$

by

$$u([f]) \longrightarrow ([f], [f], \dots, [f]).$$

Note that each $\mathbb{Q}[x]/(x - n)$ is isomorphic to \mathbb{Q} : just send an $[f]$ to $f(n)$. It is injective since if $u([f]) = 0$, then (any representative) f is divisible by $x - n$, $\forall n = 0, \dots, N$. By unique factorization, f is divisible by $f_N(x)$ so that $[f] = 0 \in \mathbb{Q}[x]/(f_N(x))$. To prove surjectivity it is enough to find a polynomial with prescribed rational values at $x = 0, \dots, N$. This can be done easily.

By part a) or because the $\mathbb{Q}[x]/(x - n)$ are fields, $\prod_{n=0}^N \mathbb{Q}[x]/(x - n)$ is a principal ideal ring. Each factor in the product is a field and has no proper ideals. The ideals are all of the form $\prod_{n=0}^N I_n$ where $I_n \subseteq \mathbb{Q}[x]/(x - n)$ is either the zero ideal or the whole field.

6. Let $a \in \mathbb{R}$ be such $a^4 = 5$.

- a) Show that $\mathbb{Q}(ia^2)$ is normal over \mathbb{Q} .
- b) Show that $\mathbb{Q}(a + ia)$ is normal over $\mathbb{Q}(ia^2)$.
- c) Prove that $\mathbb{Q}(a + ia)$ is not normal over \mathbb{Q} .

a) ia^2 is a root of $x^2 + 5 = 0$ which is of degree two and irreducible over \mathbb{Q} . It follows that $x^2 + 5$ splits over $\mathbb{Q}(ia^2)$ which is then a splitting field (no smaller one does the job). It follows that $\mathbb{Q}(ia^2)$ is normal over \mathbb{Q} .

b) Same proof as above, just note that $a + ia$ is a root of $x^2 + 2ia^2 = 0$ which is irreducible over $\mathbb{Q}(ia^2)$. We show this below, but even if it were reducible, we would then have the equality of fields $\mathbb{Q}(ia^2) = \mathbb{Q}(a + ia)$ and the trivial extension is normal.

c) It is not normal.

First note that part a) and b) imply that $[\mathbb{Q}(a + ia) : \mathbb{Q}] = 2 \cdot 2 = 4$. Note also that $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(x^4 - 5) = 4$.

We prove it by contradiction. Assume it is normal.

$a + ia$ is a root of $x^4 + 20 = 0$ which is irreducible over \mathbb{Q} . By normality all four roots

$$a + ia, \quad i(a + ia), \quad -(a + ia), \quad -i(a + ia)$$

belong to $\mathbb{Q}(a + ia)$.

It follows that $a = (1/2)[(a + ia) - i(a + ia)] \in \mathbb{Q}(a + ia)$.

It follows that $\mathbb{Q}(a) = \mathbb{Q}(a + ia)$: they have the same dimension, 4, over \mathbb{Q} and one is contained in the other.

It follows that $i \in \mathbb{Q}(a)$, but a is real, contradiction.