

Algebra Qual Fall 2015

Problem 1

Statement. Let G be a group containing a subgroup H not equal to G of finite index. Prove that G has a normal subgroup which is contained in every conjugate of H , and which is of finite index.

Solution. Define

$$N = \bigcap_{g \in G} gHg^{-1}$$

i.e. N is the intersection of all conjugate subgroups of $H \leq G$. It is a group being an intersection of subgroups. We claim it is normal and has finite index as well.

Normality 1:

For normality first note that there are finitely many distinct cosets so also finitely many distinct conjugate subgroups thus the above intersection is a finite one

$$N = \bigcap_{i=1}^n g_i H g_i^{-1}.$$

Now conjugation is a bijection so $|gNg^{-1}| = |N|$ so it suffices to check that $gNg^{-1} \subseteq N$. Let $k \in N$. Then k is in every conjugate subgroup, and we want to show gkg^{-1} is as well. First note if $k \in mHm^{-1}$ then $gkg^{-1} \in gmH(gm)^{-1}$. Then consider that k is also in $gmHm^{-1}g^{-1}$ so that $gkg^{-1} \in mHm^{-1}$. Since m was arbitrary we've shown that gkg^{-1} is in every conjugate subgroup as desired.

Normality 2:

Slicker normality. Since conjugation is an automorphism it is a bijection and commutes with intersections. Thus if $k \in G$ is arbitrary

$$\begin{aligned} kNk^{-1} &= k \left(\bigcap_{g \in G} gHg^{-1} \right) k^{-1} = \bigcap_{g \in G} kgHg^{-1}k^{-1} \\ &= \bigcap_{kg \in G} (kg)H(kg)^{-1} = \bigcap_{g \in G} gHg^{-1} \end{aligned}$$

where the last equality follows from the fact that the left multiplication map $m_k : G \rightarrow G$ is a bijection.

Now to show that N is finite index let G act on the cosets of H by left multiplication $g \cdot kH = gkH$. Then we get a homomorphism

$$\phi : G \rightarrow S_{|G/H|}.$$

Then since the target is finite $\ker \phi$ has finite index as a subgroup of G . More formally by the 1st isomorphism theorem

$$G / \ker \phi \cong \phi(G) \subseteq S_{|G/H|}.$$

Then note that

$$\begin{aligned} \ker \phi &= \{g \in G : g \cdot x = x, \text{ for all } x \in G/H\} \\ &= \bigcap_{kH \in G/H} \text{stab}_{kH}. \end{aligned}$$

It suffices to check that

$$\text{stab}_{kH} = kHk^{-1}.$$

Indeed if $khk^{-1} \in kHk^{-1}$ then

$$khk^{-1}kH = khH = kH$$

so $kHk^{-1} \subseteq \text{stab}_{kH}$. Conversely suppose

$$gkH = kH.$$

Then $gk = kh$ which implies $g = khk^{-1} \in kHk^{-1}$ as desired. $\square$

Problem 2

Statement. Let G be a finite group, H a p -subgroup and P a Sylow p -subgroup (p a prime). Let H act on the left cosets of P in G by left translation. Prove that there is an orbit under this action of length 1. Prove that xP is an orbit of length 1 if and only if H is contained in xPx^{-1} .

Solution. Orbit of length one is fixed point. This is asking us to generalize a certain part of the proof of sylow II.

Let G be a group of order mp^n where $p \nmid m$. Then H has order p^k for some $k \leq n$ and P has order p^n . Now let H act on G/P by left multiplication $h \cdot gP = hgP$. Then since H is a p -group we have that the size of G/H is congruent to the number of fixed points mod p . That is

$$m = |G/P| \equiv |(G/P)^H| \pmod{p}.$$

Then $p \nmid m$ so $m \not\equiv 0 \pmod{p}$ thus $|(G/P)^H|$ is not zero mod p so in particular it is not 0 and there is a fixed point xP such that $h \cdot xP = xP$ for all $h \in H$.

Now for each h this says that there is $y \in P$ such that

$$(hx = xy) \iff (h = xyx^{-1} \in xPx^{-1})$$

thus $H \subseteq xPx^{-1}$ as desired. Then for the converse inclusion just note that if $y \in xPx^{-1}$ then

$$yxP = xy'x^{-1}xP = xy'P = xP.$$

In general if a group G acts on the cosets G/H of a subgroup H by left multiplication then

$$\text{Stab}(gH) = gHg^{-1}.$$

The proof of this statement is just the above paragraph. $\square$

Problem 3

Statement. Let R be a rng (ring without 1) which contains an element u such that for all $y \in R$, there is an $x \in R$ such that $xu = y$. Prove that R contains a maximal left ideal. Hint: imitate the proof (using Zorn's lemma) in the case when R does have 1.

Solution.

Proposition 3.1. An ideal $I \subseteq R$ is proper iff $u \notin I$.

Proof. If I is not proper $I = R$ and contains u . Suppose $u \in I$, and $y \in R$ is arbitrary. Then $y = xu \in I$ since I is an ideal thus closed under scaling. $\square$

Let Σ be the set of proper ideals in R ordered by inclusion. This is non-empty since the 0 ideal is proper (if $R = \{0\}$ this is false.) Let $C = \{I_i\}_{i \in K}$ be a chain in Σ (K is some poset and the ideals are ordered by inclusion w.r.t to K), and define $I = \bigcup_{i \in K} I_i$. Then this is ideal, and clearly a bound on the chain. It remains to show I is proper. Indeed suppose its not. Then it contains $u \in I$, thus $u \in I_i$ for some i , but then this I_i is not proper, a contradiction.

Then we've shown arbitrary chains have upper bounds so by zorns lemma Σ has maximal elements.

TLDR for showing chain is an ideal: Closed under scaling is easy and if $a \in I_i, b \in I_j$ then $a + b \in I_{\max\{i,j\}}$. $\square$

Problem 4

Statement. Let R be a PID (Principal Ideal Domain). Let $(a_1) < (a_2) < \dots$ be an ascending chain of ideals in R . Prove that for some n , we have $(a_j) = (a_n)$ for all $j \geq n$.

Solution. Let $A = \bigcup_{i=1}^{\infty} (a_i)$. We claim A is an ideal of R .

Scaling: Suppose $r \in R$, and $a \in A$. Then $a \in (a_i)$ for some i and $ra \in (a_i) \subseteq A$ since (a_i) is an ideal, thus A is closed under scaling by elements of A .

Differences: Suppose $b \in A$ as well. Then $b \in (a_j)$ for some j . Let $k = \max\{i, j\}$. Then $a, b \in (a_k)$, and thus so is their difference $b - a \in (a_k) \subseteq A$ so A is closed under differences.

Now $A \subseteq R$ is an ideal in a PID so $A = (x)$ for some $x \in R$. Note first that $(a_i) \subseteq A$ by definition. Then also since $x \in (a_n)$ for some n we must have $A \subseteq (a_n)$ hence $A = (a_n)$. Similarly for all $j \geq n$ since $A = (a_n) \subseteq (a_j) \subseteq A$ we must have $(a_j) = (a_n)$ for all $j \geq n$. $\square$

Problem 5

Statement. Let $u = \sqrt{2 + \sqrt{2}}, v = \sqrt{2 - \sqrt{2}}$, and $E = \mathbb{Q}(u)$.

(a) Find (with justification) the minimal polynomial $f(x)$ of u over $\mathbb{Q}$.

(b) Show $v \in E$. Show that E is a splitting field of $f(x)$ over $\mathbb{Q}$.

(c) Determine the Galois group of E over $\mathbb{Q}$, and determine all the intermediate fields F with $E \supset F \supset \mathbb{Q}$.

Solution. (a) We have

$$\begin{aligned} u^2 &= 2 + \sqrt{2} \\ u^2 - 2 &= \sqrt{2} \\ (u^2 - 2)^2 &= 2 \\ u^4 - 4u^2 + 4 &= 2 \\ u^4 - 4u^2 + 2 &= 0 \end{aligned}$$

so $f(x) = x^4 - 4x^2 + 2$ is an annihilating polynomial for u . Then f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 2$. Then it is monic so it is the unique monic irreducible annihilating polynomial for u hence the minpoly for u .

(b) We have

$$\begin{aligned} f(x) &= (x^2 - 2 - \sqrt{2})(x^2 - 2 + \sqrt{2}) \\ &= (x^2 - u^2)(x^2 - v^2) = (x - u)(x + u)(x - v)(x + v) \end{aligned}$$

thus if E contains v then it contains all the roots $f(x)$ thus contains the splitting field. On the other hand the splitting would contain u so E must be the splitting field. Then it remains to prove that $v \in E$.

We claim $v = \sqrt{2}u^{-1}$. Indeed

$$uv = \sqrt{(2 - \sqrt{2})(2 + \sqrt{2})} = \sqrt{4 - 2} = \sqrt{2}$$

Of course $\sqrt{2} \in \mathbb{Q}(u)$ since

$$(u^2 - 2) = (2 + \sqrt{2} - 2) = \sqrt{2}$$

so the product $u^{-1}\sqrt{2} = v$ in $\mathbb{Q}(u)$ as well.

(c) Let $G = \text{Gal}(\mathbb{Q}(u)/\mathbb{Q})$. Note that

$$|\text{Gal}(\mathbb{Q}(u)/\mathbb{Q})| = [\mathbb{Q}(u) : \mathbb{Q}] = \deg f = 4$$

and since G acts transitively on the roots of the degree 4 equation f we have that G is a transitive subgroup of S_4 thus it is either V_4 or C_4 .

It suffices to find an element of order 4. Since G acts transitively on the roots there is an element $\phi \in G$ such that $\phi(u) = v$. Then also

$$\phi(\sqrt{2}) = \phi(u^2 - 2) = \phi(u)^2 - 2 = v^2 - 2 = -\sqrt{2}.$$

Then necessarily

$$\phi(v) = \phi(\sqrt{2}u^{-1}) = \phi(\sqrt{2})\phi(u^{-1}) = -\sqrt{2}v^{-1} = -u$$

and $\phi(-u) = -\phi(u) = -v$, and finally $\phi(-v) = -\phi(v) = -(-u) = u$. So indeed ϕ has order 4 and this Galois group is cyclic.

Then it only has one intermediate field (aside from the trivial ones $\mathbb{Q}$ and E) namely $\mathbb{Q}(u^2) = \mathbb{Q}(\sqrt{2})$ which Galois group corresponding to the subgroup C_2 . $\square$

Problem 6

Statement. (a) Let G be a finite group. Show that there exists a field extension K/F with $\text{Gal}(K/F) = G$. (You may assume that for any natural number n there is a field extension with Galois group S_n .)

(b) Let K be a Galois extension of F with $|\text{Gal}(K/F)| = 12$. Prove that there exists an intermediate field E of K/F with $[E : F] = 3$.

(c) With K/F as in (b), does an intermediate field L necessarily exist satisfying $[L : F] = 2$? Give a proof or counterexample.

Solution. (a) This needs some qualification. It depends on what F is. For instance $\mathbb{R}$ has no extensions of degree greater than 2 and $\mathbb{C}$ being algebraically closed has none what so ever.

Here is my interpretation of the problem.

Let G be a finite group of order n . Then by letting G act on itself by left multiplication we get an embedding of $G \rightarrow S_n$ so it suffices to show that there is a field extension with Galois group an arbitrary subgroup of S_n .

Now suppose K/L is Galois with Galois group S_n with $G \leq S_n$. Let

$$F := \{\ell \in K : \phi(\ell) = \ell, \text{ for } \phi \in G\}$$

be its fixed field. Then by the Galois correspondence K/F is Galois with

$$\text{Gal}(K/F) = G$$

as desired.

(b) Let $G = \text{Gal}(K/F)$. Since G has order $12 = 2^2 \cdot 3$ we know G sylow a 2-sylow subgroup Q of order 4. Let $E = \{\ell \in K : \phi(\ell) = \ell, \text{ for all } \phi \in Q\}$ be the fixed field for Q . Then by the Galois correspondence

$$[E : F] = [G : Q] = \frac{2^2 \cdot 3}{2^2} = 3$$

as desired.

(c) This would imply G has a subgroup of index 2 or equivalently order 6. Then by (a) it suffices to find a group of order 12 with no subgroup of index 2. Such a group is A_4 .

More formally by part (a) there is an extension K/F with Galois group A_4 . If there was an intermediate extension L/F of degree 2 then taking the invariant subgroup $H = \text{Gal}(K/L)$ since

$$[G : H] = [L : F] = 2$$

we would obtain a subgroup of A_4 with index 2, but there is no such subgroup.

Proof that A_4 has no subgroup of order 6: Since A_4 has index 2 it contains the square of every element in S_4 . Then if H we're a subgroup of A_4 of index two it would be normal and contain all squares of elements in A_4 . Then all the 8 3-cycles in S_4 are contained in A_4 , and their squares are also 3-cycles so H must contain 8-elements contradiction. $\square$

Problem 7

Statement. (a) Show that two 3×3 matrices over the complex numbers are similar if and only if their characteristic polynomials are equal and their minimal polynomials are equal.

(b) Does the conclusion of the previous part hold for 4×4 matrices? Justify your answer with a proof or counterexample.

Solution. **(a)** First a reduction. Suppose $A, B \subseteq \mathbb{C}^{3 \times 3}$. Then they have jordan canonical forms

$$A = PJ_AP^{-1}, \text{ and } B = QJ_BQ^{-1}.$$

Suppose $A = TBT^{-1}$ are similar. Then

$$B = TPJ_AP^{-1}T^{-1}, \text{ and } A = TQJ_BQ^{-1}T^{-1}$$

then since Jordan canonical forms are unique up to permutation of the blocks A and B have identical canonical forms. Then this question is equivalent to showing that jordan canonical forms are uniquely determined by the characteristic and minimal polynomial.

Of course one direction is trivial. If A and B have the same canonical forms then their char polys being the same as the char poly of their forms must be equal, and similarly for the min poly's.

For the converse we show the char poly and min poly uniquely determine the canonical form.

Now suppose A is a 3×3 matrix over $\mathbb{C}$. Then its char poly a monic degree polynomial in $\mathbb{C}$ say $\chi_A(\lambda)$. Let r_1, r_2, r_3 be its roots listed with multiplicities. Then we have the following possibilities

- r_i distinct. Then char poly is minpoly and the blocks all have size 1 so the only possible form is

$$\begin{bmatrix} r_1 & & \\ & r_2 & \\ & & r_3 \end{bmatrix}$$

- Repeated root say $r_2 = r_3$. Then char poly is $(\lambda - r_1)(\lambda - r_2)^2$. The only possible min poly's are $(\lambda - r_1)(\lambda - r_2)$, and $(\lambda - r_1)(\lambda - r_2)^2$. Then we have one chain of length 1 for r_1 and for r_2 in the first case the largest chain size is 1 so they all have size 1. In the 2nd case we must have a chain of size 2 and it must be the only chain so we get the forms

$$\begin{bmatrix} r_1 & & \\ & r_2 & \\ & & r_2 \end{bmatrix}, \text{ and } \begin{bmatrix} r_1 & & \\ & r_2 & 1 \\ & & r_2 \end{bmatrix}.$$

- All roots equal. Char poly is $(\lambda - r)^3$. The possible min polys are

$$(\lambda - r), (\lambda - r)^2, (\lambda - r)^3.$$

These tell us the largest block size for r . In order they correspond to

1. All blocks of size 1
2. A block of size 2 and a block of size 1
3. One block of size 3

(b) Almost certainly no. And the problem should come from having ambiguity in block sizes. For example consider the case of a single eigenvalue λ and the two canonical forms

$$\begin{bmatrix} \lambda & 1 & & \\ & \lambda & & \\ & & \lambda & 1 \\ & & & \lambda \end{bmatrix}, \text{ and } \begin{bmatrix} \lambda & 1 & & \\ & \lambda & & \\ & & \lambda & \\ & & & \lambda \end{bmatrix}$$

These both have char poly $(x - \lambda)^4$ and min poly $(x - \lambda)^2$, but the first have two blocks of size 2 while the second only has 1 block of size 2. Then they are not similar since one is not just the result of reordering the blocks. $\square$

Problem 8

Statement. Let V be a vector space over a field F and V^* its dual. A symmetric bilinear form $(\cdot, \cdot)$ on V is a map $V \times V \rightarrow F$ satisfying the rules

$$(av_1 + bv_2, w) = a(v_1, w) + b(v_2, w) \quad \text{and} \quad (v, w) = (w, v)$$

for $a, b \in F$ and $v_1, v_2, v, w \in V$. The form is nondegenerate if the only element w satisfying $(v, w) = 0$ for all $v \in V$ is $w = 0$.

Suppose $(\cdot, \cdot)$ is a symmetric nondegenerate bilinear form on V . If W is a subspace of V , define

$$W^\perp = \{v \in V \mid (v, w) = 0 \text{ for all } w \in W\}.$$

(a) Show that if X and Y are subspaces of V with $Y \subset X$, then $X^\perp \subseteq Y^\perp$.

(b) Define an injective linear map $\psi : Y^\perp / X^\perp \hookrightarrow (X/Y)^*$ which is an isomorphism if V is finite-dimensional.

Solution. See the write up in *Non-degenerate forms and dual spaces*. $\square$