MOCK QUALIFYING EXAMINATION, ALGEBRA, PART A, 2019

September n, 2019

Solve any four questions; indicate which ones are supposed to be graded. Each question is worth 15 points. You must show all work and justify all statements either by referring to an appropriate theorem or by providing a full solution.

1.

(a) List all isomorphism classes of abelian groups of order 120. Is there a simple group of order 120?

(b) What is the maximal number of elements of order 5 in a group of order 120?

(c) How many conjugacy classes are there in S_5?

(a) Note that $120 = 2^3 \times 3 \times 5$. There are only three abelian groups of order 120:

$$\mathbf{Z}_{120} \quad \mathbf{Z}_{60} \times \mathbf{Z}_2 \quad \mathbf{Z}_{30} \times \mathbf{Z}_2 \times \mathbf{Z}_2$$

Suppose for the sake of contradiction that your group G of order 120 is simple. By the third Sylow theorem, the number of Sylow 5-subgroups of G must divide 120 and be congruent to 1 (mod 5), so there can be either 1 or 6 Sylow 5-subgroups. But if there is only 1, then it'll be normal in G contradicting G being simple. So there must be 6 Sylow 5-subgroups. Let X denote this set of Sylow 5-subgroups. By the second Sylow theorem, G acts on this set X by conjugation, permuting the subgroups. This action gives us a map $\varphi\colon G \to S_6$ with each $g \in G$ being sent to the permutation that describes its action on X. But again, if G is simple and doesn't have a normal subgroup then $\mathrm{Ker}(\varphi)$ must be trivial, and φ must be injective, telling us $G \cong \mathrm{Im}(\varphi) < S_6$.

But we can strengthen this and say $G \cong \mathrm{Im}(\varphi) < A_6$. Recall that for $H < S_n$ either $H < A_n$ or exactly half of the elements of H are contained in A_n. But in the latter case $\mathrm{Im}(\varphi) \cap A_n$ would be an index 2 subgroup, and index 2 subgroups are normal subgroups, contradicting $G \cong \mathrm{Im}(\varphi)$ being simple. So we have $G \cong \mathrm{Im}(\varphi) < A_6$.

Now since $|A_6| = 6 \times 5 \times 4 \times 3 = 360$, $\mathrm{Im}(\varphi)$ will be an index three subgroup of A_6. Using the same trick as in the first paragraph, A_6 will act on the set of left cosets $A_6/\mathrm{Im}(\varphi)$ and we'll get a nonzero homomorphism $A_6 \to S_3$. But A_6 is bigger than S_3, so this homomorphism has a nontrivial kernel,

which will be a normal subgroup of A_6. We know A_6 is simple though, so this is our contradiction. $\Rightarrow\!\!\!\!\!\!\!\!\Leftarrow$

(b) By the previous proof, in a group of order 120 there is either a single Sylow 5-subgroup, or there are 6 Sylow 5-subgroups. Since every element of order 5 will be contained in a Sylow 5-subgroup, and the Sylow 5-subgroups of a group must be conjugate (so they only intersect on $\{e\}$), in each of these cases respectively there will be four elements of order 5 or 6×4 equals twenty-four elements of order 5. To show that twenty-four is really the maximal number of order 5 elements (and not four), we just need to find a group of order 120 that has more than four elements of order 5. The group S_5 will do, noting all the all the five-cycles $(\cdot\ \cdot\ \cdot\ \cdot\ \cdot)$ have order five, and there are twenty-four five-cycles in S_5.

(c) There are seven conjugacy classes of elements, one for each possible cycle-type of a permutation of S_5:

$$5 \quad 4+1 \quad 3+2 \quad 3+1+1 \quad 2+2+1 \quad 2+1+1+1 \quad 1+1+1+1+1$$

This is because (1) every element of S_5 can written uniquely as a product of disjoint cycles, (2) the conjugate of a product of disjoint cycles is the product of the conjugates of those cycles, and (3) conjugation preserves cycle-type: for a cycle $(n_1 \cdots n_k)$ for any $\sigma \in S_5$ we have

$$\sigma(n_1 \cdots n_k)\sigma^{-1} = (\sigma(n_1) \cdots \sigma(n_k))\,.$$

2. Let $p > q$ be primes.

(a) Describe *all* groups of order p^2 up to an isomorphism.

(b) Show that a group of order $p^n q, n > 0$, is solvable.

(a) The proof of this requires two facts which may or may not be important.

LEMMA 1 — If $G/\,\mathrm{Z}(G)$ is cyclic then G is abelian.

Proof First let $Z = \mathrm{Z}(G)$. Since G/Z is cyclic, there exists some $g \in G$ such that $(gZ)^n = aZ$ for any $aZ \in G/Z$. On the level of elements, given any $a \in G$ and any $\zeta \in Z$ we can find $z \in Z$ such that $(gz)^n = g^n z^n = a\zeta$. In particular, $a = g^n z^n \zeta^{-1}$, so every element $a \in G$ can be written as the product of a power of g and an element in Z. Using this fact, we can take

$a, b \in G$ and see that

$$ab = (g^n z_a)(g^m z_b) = g^n g^m z_a z_b = g^m g^n z_b z_a = g^m z_b g^n z_a = ba\,.$$

□

LEMMA 2 — If G is a p-group then it has a nontrivial center.

Proof Let G act on itself by conjugation. Let $\overline{g}$ denote the orbit of g and let $\mathrm{Stab}(g)$ denote the subset $\{h \in G | hgh^{-1} = g\}$. Note that there is a natural bijection between $\overline{g}$ and $G/\mathrm{Stab}(g)$ because for $h, k \in G$

$$\begin{aligned} hgh^{-1} = kgk^{-1} &\iff \left(k^{-1}h\right) g \left(k^{-1}h\right)^{-1} = g \\ &\iff k^{-1}h \in \mathrm{Stab}(g) \iff k\mathrm{Stab}(g) = h\mathrm{Stab}(g) \end{aligned}$$

So $|\overline{g}| = [G : \mathrm{Stab}(g)]$ and since the orbits define an equivalence relation on G,

$$|G| = \sum_i [G : \mathrm{Stab}(g_i)]$$

for each g_i representative of an orbit. We can rewrite this by separating out the center of G and summing over the elements g_i such that $\mathrm{Stab}(g_i) \lneq G$:

$$|G| = |\,\mathrm{Z}(G)| + \sum_i [G : \mathrm{Stab}(g_i)]\,.$$

Since $|G| = p$, and $[G : \mathrm{Stab}(g_i)]$ divides $|G|$ for each $\mathrm{Stab}(g_i)$, and the center contains at least the identity, we have that $|\,\mathrm{Z}(G)|$ is a non-zero power of p. □

Now since the center of G is a subgroup, its order must divide the order of G. The center of a p-group cannot be trivial so its order is either p or p^2. If its order is p^2, then the entire group is abelian. Otherwise if the order is p, then the quotient of G by its center is isomorphic to $\mathbf{Z}_p$. Since $\mathbf{Z}_p$ is cyclic, again we have that G is abelian.

(b) Let n_p denote the number of Sylow p-subgroups and recall that n_p divides $|G|$ and $n_p \equiv 1 \pmod{p}$.

$$n_p \in \{1, q, p, pq, \ldots, p^n, p^n q\} \cap \{1, 1+p, 1+2p, \ldots\}\,.$$

But since $p > q$ and $p^i q \not\equiv 1 \pmod{p}$, we have $n_p = 1$. All Sylow p-

subgroups are conjugate so since there is a unique Sylow p-subgroup, it is normal in G and G is not simple.

3. The action of a group G on a set X is called *transitive* if for every $x, x' \in X$ there exists a $g \in G$ such that $gx = x'$.

(a) Show that the natural action of the symmetric group S_n on the set $\{1, \ldots, n\}$ is transitive and find the stabilizer of an arbitrary element in that set.

(b) Suppose that a group G acts transitively on a set X. Prove that all the subgroups $\mathrm{Stab}_G x$, $x \in X$ are conjugate and find $[G : \mathrm{Stab}_G x]$.

Solution by Jacob Garcia:

(a) Denote $X = \{1, 2, \ldots, n\}$. Note that the action of S_n on X is via evaluation: For $\tau \in S_n$ and $m \in X$, $\tau \cdot m = \tau(m)$. Let $m, k \in X$ be arbitrary. Then the transposition $(m\ k)$ is an element of S_n such that $(m\ k) \cdot m = k$. Thus the action is transitive.

Let $m \in X$ be arbitrary. By definition, $\mathrm{Stab}_{S_n} m = \{\tau \in S_n : \tau \cdot m = m\}$, and since the stabilizer of m is the collection of all permutations that fix m, this is precisely the collection of all permutations on the remaining $n - 1$ elements. Thus, $\mathrm{Stab}_{S_n} m \cong S_{n-1}$.

(b) Let $x, y \in X$ be arbitrary. Since the action is transitive, there exists $g \in G$ such that $g \cdot x = y$. Notice that $x = g^{-1} \cdot y$. We claim that $\mathrm{Stab}_G y = g\ \mathrm{Stab}_G x\ g^{-1}$. First let $ghg^{-1} \in g\ \mathrm{Stab}_G x\ g^{-1}$ be arbitrary. Then $ghg^{-1} \in \mathrm{Stab}_G y$ since $h \in \mathrm{Stab}_G x$ and so $ghg^{-1} \cdot y = gh \cdot x = g \cdot x = y$. Now let $h \in \mathrm{Stab}_G y$ be arbitrary. Define $k = g^{-1}hg$. Then $k \in \mathrm{Stab}_G x$ since $k \cdot x = g^{-1}hg \cdot x = g^{-1}h \cdot y = g^{-1} \cdot y = x$. Therefore $h = gkg^{-1} \in g\ \mathrm{Stab}_G x\ g^{-1}$. This proves the claim.

We claim that $[G : \mathrm{Stab}_G x] = |X|$ for every $x \in X$. Let $x \in X$ be arbitrary. Denote $H = \mathrm{Stab}_G x$. Let $C = \{gH : g \in G\}$, i.e. the collection of all cosets of H. Define $\varphi : C \to X$ via $\varphi(gH) = g \cdot x$. Then φ is surjective, as for any $y \in X$, there exists $g \in G$ such that $g \cdot x = y$ by transitivity, therefore $\varphi(gH) = g \cdot x = y$. Also, φ is injective. If $\varphi(gH) = \varphi(kH)$, then $g \cdot x = k \cdot x$, so $g^{-1}k \cdot x = x$. Thus $g^{-1}k \in H$, which gives $gH = kH$. Therefore φ is a bijection, which proves the claim.

4. Recall that an element a of a ring is called nilpotent if $a^n = 0$ for some positive integer n. Prove the following statements for an *commutative unital ring* R.

(a) The set of all nilpotent elements in R is an ideal.
(b) R is local if and only if for all $x, y \in R$, $x + y = 1_R$ implies that x or y is a unit.
(c) If every non-unit in R is nilpotent then R is local.

(a) Note that 0 is nilpotent, and that r being nilpotent will mean $-r$ is nilpotent. Take two nilpotent elements $x, y \in R$ and say $x^n = 0$ and $y^m = 0$. Then their sum $x + y$ will be nilpotent since

$$\begin{aligned}
& (x+y)^{n+m} \\
= \; & x^n x^m + x^n x^{m-1} y^1 + \cdots + x^n x^1 y^{m-1} + x^n y^m + x^{n-1} y^1 y^m + \\
& \qquad \cdots + x^1 y^{n-1} y^m + y^n y^m \\
= \; & (0) x^m + (0) x^{m-1} y^1 + \cdots + (0) x^1 y^{m-1} + (0)(0) + x^{n-1} y^1 (0) + \\
& \qquad \cdots + x^1 y^{n-1} (0) + y^n (0) \\
= \; & 0 \,.
\end{aligned}$$

And finally for any $r \in R$, since R is commutative we have $(rx)^n = r^n x^n = 0$. So the nilpotent elements of R form an ideal.

(b) Suppose that R is local with unique max ideal $\mathfrak{m}$. This max ideal must contain all the non-units of R, for otherwise if z is a non-unit *not* in $\mathfrak{m}$, then z is contained in another max ideal by Zorn's lemma, contradicting the uniqueness of $\mathfrak{m}$. Now if $x + y = 1_R$, we can't have both x and y be non-units since then $x + y = 1_R \in \mathfrak{m}$ meaning $\mathfrak{m} = R$. So one of x or y has to be a non-unit.

Conversely say that $x + y = 1_R$ implies one of x or y is a unit. Suppose (for the sake of contradiction) that R is *not* local. Take two maximal ideals $\mathfrak{m}_x$ and $\mathfrak{m}_y$. Since these ideals are maximal, $\mathfrak{m}_x + \mathfrak{m}_y = R$, so there exists some $x \in \mathfrak{m}_x$ and $y \in \mathfrak{m}_y$ such that $x + y = 1_R$. But this means one of x or y is a unit, and so one of $\mathfrak{m}_x$ or $\mathfrak{m}_y$ is all of R. $\Rightarrow\!\Leftarrow$

(c) We will use part (b) and show that if every non-unit of R is nilpotent then we have that $x + y = 1_R$ implies either x or y is a unit. If y is *not* a unit already, then it will be nilpotent. Suppose that $y^{n+1} = 0$. Then we have the $x = 1_R - y$ will have inverse $(1 + y + y^2 + \cdots + y^n)$, showing that x must be a unit. So R is local.

5. Let $R = \mathbb{Z} \times \mathbb{Z}$ as an additive abelian group while the multiplication is defined by $(x, y) \cdot (x', y') = (xy' + yx', yy' - xx')$; then R is a commutative ring with unity

$1_R = (0, 1)$. Answer the following questions (all answers must be justified).

(a) Is the ideal of R generated by $(0, 5)$ prime?

(b) Is R a domain? If so, describe it's field of fractions.

(c) Choose a maximal ideal M in R and describe the localization of R at M.

A key thing to notice here is that the ring $R = \mathbf{Z} \times \mathbf{Z}$ in question can be more reasonably thought of as the ring of Gaussian integers $\mathbf{Z}[\mathfrak{i}]$ where the imaginary part is the first component.

(a) No, the ideal $(5) \in \mathbf{Z}[\mathfrak{i}]$ is not prime since $(1 + 2\mathfrak{i})(1 - 2\mathfrak{i}) = 1 + 4 = 5$.

(b) $\mathbf{Z}[\mathfrak{i}]$ is certainly a domain since $\mathbf{Z}[\mathfrak{i}] \cong \mathbf{Z}[x]/(x^2 + 1)$, and since $\mathbf{Z}[x]$ is a domain and $(x^2 + 1)$ is irreducible in $\mathbf{Z}[x]$. The field of fraction of $\mathbf{Z}[\mathfrak{i}]$ must at least contain $\mathbf{Q}[\mathfrak{i}]$ since $\mathbf{Q}$ is the field of fractions of $\mathbf{Z}$. So we must only show $\mathbf{Q}[\mathfrak{i}]$ is a field, which it totally is. Take $a + b\mathfrak{i} \in \mathbf{Q}[\mathfrak{i}]$ and $\frac{1}{a^2+b^2}(a - b\mathfrak{i})$ is its inverse.

(c) The ideal generated by $1 + \mathfrak{i}$ in $\mathbf{Z}[\mathfrak{i}]$ is maximal since it's index two. Since it's maximal it's a prime ideal and the localization of any ring at a prime ideal, denoted $\mathbf{Z}[\mathfrak{i}]_{(i+\mathfrak{i})}$ in this instance, will be a local ring with unique max ideal corresponding to $(i + \mathfrak{i}) \subset \mathbf{Z}[\mathfrak{i}]_{(i+\mathfrak{i})}$. I'm not sure what else there is to say about it.

Mock Algebra Qualifying Examination, Fall 2019, Part b

Answer any four of the following questions. All questions are worth 10 points.

1. Let R be a commutative ring with identity and let a be a non-zero element in R. Suppose that P is a prime ideal properly contained in the principal ideal generated by a. Prove that $P = aP$. Suppose now that P is also principal. Prove that there exists $b \in R$ with $(1-ab)P = 0$. What can you conclude about P if R is an integral domain and a is not a unit?

Solution from Derek Lowenberg:

We have $aP \subset P$ because P is an ideal. Since $P \subset (a)$ we know that every $p \in P$ can be written $p = ac$ for some $c \in R$. But since P is a prime ideal of a commutative ring, $ac \in P$ implies $a \in P$ or $c \in P$. As P is properly contained in (a) we know that $a \notin P$ therefore $c \in P$. Thus $P \subset aP$ and we conclude $P = aP$.

Suppose P is principal, generated by p. As above, $p = ac$ where $c \in P$, that is, $c = bp$ for some $b \in R$. Then $p = abp$. For any $xp \in P$ (where $x \in R$) we have

$$(1-ab)xp = xp - abxp = x(p - abp) = 0$$

Thus $(1-ab)P = 0$. If R is an integral domain then $(1-ab)xp = 0$ implies $1 - ab = 0$ or $xp = 0$ and if a is not a unit we have $1 - ab \neq 0$ so $xp = 0$. Since this equation holds for any element xp of P we conclude in this case that $P = 0$.

2. (a) Let R be a commutative ring with identity and regard R as a module for itself via left multiplication. Prove that this module is simple iff R is a field. (b) Define a free module for a ring R. Suppose that R is a commutative ring with identity and satisfies the following condition: any submodule of a free module is free. Prove that R is a principal ideal domain.

(a) Suppose your R-module R is simple, and take nonzero $x \in R$. Since R has no non-trivial submodules, the submodule generated by x, $Rx = \{rx \mid r \in R\}$, must be all of R. In particular there must be some $r_x \in R$ such that $r_x.x = 1_R$, which shows that x, an arbitary nonzero element of R, is a unit, so R is a field. Conversely recall that R is a field iff it has no proper non-trivial ideals because everything in R must be a unit. A submodule of R considered as an R-module would *be* an ideal of R, so R cannot have any submodules, and must be simple.

(b) F is a free R-module if it has a basis $\{x_i\}_{i \in I} \subset F$ such that the x_i are linearly independent and for any $f \in F$ we have $f = r_1 x_{j_1} + \cdots + r_k x_{j_k}$ for a unique choice of $x_{j_\ell} \subset \{x_i\}_{i \in I}$. Equivalently F is free if $F \cong \bigoplus_I R$. Suppose that any submodule of a free R-module is free and consider R as an R-module. Take any nonzero ideal $I \subset R$ and note that this is a submodule of R, so it too must be free. Let B be a basis of I as a free R-module. Suppose (for the sake of contradiction) that B has at least two elements. Take distinct $u, v \in B$ and note that these elements cannot be linearly independent

since $u, v \in R$ too, and we have $(u)v - (v)u = 0$. Therefore B can have at most one element, and that element will principally generate the ideal I, so R is a PID.

3. Give examples to show that the following can happen for a ring R and modules M,N,
(i) $M \otimes_R N \ncong M \otimes_{\mathbf{Z}} N$, where $\mathbf{Z}$ is the ring of integers.
(ii) $u \in M \otimes_R N$ but $u \neq m \otimes n$ for any $m \in M$ and $n \in N$.
(iii) $u \otimes v = 0$ but $u, v \neq 0$.

(i) Take $M \cong R$ and $N \cong \mathbf{Z}$. Then $R \otimes_R \mathbf{Z} \cong \mathbf{Z} \ncong R \cong R \otimes_{\mathbf{Z}} \mathbf{Z}$.

(ii) Let $\boldsymbol{k}$ be a field, and take $M \cong N \cong \boldsymbol{k}^2$ each with standard basis $\{e_1, e_2\}$. The tensor $e_1 \otimes e_1 + e_2 \otimes e_2$ cannot be written as a simple tensor.

(iii) Consider $\mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}_3$ and the simple tensor $1 \otimes 2$.

4. Suppose that E is a three dimensional vector space over a field F and $f\colon E \to E$ is a non-zero linear transformation. Prove that there exists bases B_1 and B_2 of E such that the matrix of f is exactly one of the following.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Since $f\colon E \to E$ is a nonzero linear transformation it must have rank either 1, 2, or 3, where $\operatorname{rank} f = \dim(\operatorname{Im} f)$. Let M be the matrix of f with respect to the standard basis. Let R_1 and R_2 and R_3 be those matrices above such that R_i has rank i. M must be equivalent to one of the R_i because equivalence partitions a set of matrices by rank. So for some invertible matrices P and Q we have $PMQ = R_i$ depending on the rank of f. This P, Q will give us the bases B_1 and B_2 respectively, by selecting the columns/rows of P and Q appropriately to get your basis vectors.

5. Suppose that $D = (d_1, \ldots, d_n)$ is a diagonal matrix where the d_i, $1 \leq i \leq n$ are not necessarily distinct. What are the elementary and invariant factors of D? Suppose that A is similar to D. What can you say about its elementary divisors and invariant factors?

Since the matrix D consists entirely of Jordan blocks of size 1, it will decompose into a direct sum of 1×1 matrices corresponding to those Jordan blocks.

$$M = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & d_n \end{pmatrix} = (d_1) \oplus (d_2) \oplus \cdots \oplus (d_n)$$

In terms of the linear transformation that D defines on some n dimensional $\boldsymbol{k}$-vector space V (with a choice of basis), this decomposition gives us a $\boldsymbol{k}[x]$-module decomposition

of V with respect to D

$$V \cong \boldsymbol{k}[x]\big/(x-d_1) \oplus \boldsymbol{k}[x]\big/(x-d_2) \oplus \cdots \oplus \boldsymbol{k}[x]\big/(x-d_n)$$

And these $\{(x-d_1),(x-d_2),\ldots,(x-d_n)\}$ are the elementary divisors of D. To talk about the invariant factors of D we should write those diagonal entries with mulitplicity, as $\{(d_1,m_1),(d_2,m_2),\ldots,(d_k,m_k)\}$ where d_i occurs m_i times along the diagonal of D. Then D will have characteristic polynomial

$$(x-d_1)^{m_1}(x-d_2)^{m_2}\cdots(x-d_k)^{m_k}$$

and, again because the Jordan blocks have size 1, will have minimal polynomial

$$(x-d_1)(x-d_2)\cdots(x-d_k)\,.$$

This minimal polynomial is the generator of the annihilator of V in $\boldsymbol{k}[x]$ and hence is the "largest" invariant factor. The next invariant factor will be the product of all $(x-d_i)$ such that $m_i \geq 2$.

$$\begin{aligned} V &\cong \boldsymbol{k}[x]\big/(x-d_1)(x-d_2)\cdots(x-d_k) \oplus \cdots \\ &= \bigoplus_{k=1}^{\infty} \boldsymbol{k}[x]\big/\prod_{d_i\in\{d_1,\ldots,d_n\},m_i\geq k}(x-d_i) \end{aligned}$$

Mock Algebra Qualifier 2019 - Part C

Do 4 out of the 5 problems.

(1) Let K be a field and $f \in K[x]$. Let n be the degree of f. Prove the theorem which states that there exists a splitting field F of f over K with $[F : K] \leqslant n!$.

Solution from Noble Williamson

We proceed by induction on n. If $n = 1$ or if f splits over K then the result obviously holds. Suppose $n > 1$ and f does not split over K then f has an irreducible factor g such that the degree of g is greater than 1. Now we need the following lemma.

Lemma 3 — Let g be a monic irreducible polynomial in $K[x]$ for some field K then there exists a simple extension $K(u)$ over K such that $[K(u) : K] = \deg\ g$ and $g(u) = 0$.

Proof Let g be a monic irreducible polynomial and u a root of g. Let $\deg\ g = d$. Recall that for a simple algebriac extension $K(u)$, we have $K(u) = K[u]$ and every element of $K[u]$ is of the form $f(u)$ where $f \in K[x]$. Hence, by the division algorithm $f = qg + r$ where $q, r \in K[x]$ and $\deg\ r < \deg\ g$ so

$$f(u) = q(u)g(u) + r(u) = r(u) = c_0 + c_1u + \cdots + c_mu^c$$

where $c < d$ so $\{1, u, \ldots, u^{d-1}\}$ spans $K[u] = K(u)$. Linear independence follows from the irreducibility of g so the dimension of $K(u)$ as a vector space over K is d. □

Hence, there exists a simple extension $K(u)$ over K such that $g(u) = 0$ and $[K(u) : K] = \deg\ g > 1$. Since u is a root of g it is also a root of f so we can write $f = (x - u)h$ where $h \in K(u)[x]$ and $\deg\ h = n - 1$ then by the induction hypothesis there exists a splitting field F of h over $K(u)$ such that $[F : K(u)] \leq (n - 1)!$. Since F is a splitting field of h over $K(u)$, $F = K(u)(v_1, \ldots, v_{n-1}) = K(u, v_1, \ldots, v_{n-1})$ where $\{v_1, \ldots, v_{n-1}\}$ are the roots of h so F is a splitting field of f over K

and

$$[F : K] = [F : K(u)][K(u) : K] \leq (n-1)! \deg\ g \leq (n-1)!n = n!.$$

(2) Let K be a subfield of $\mathbb{R}$. Let L be an intermediate field of $\mathbb{C}/K$. Prove that if L/K is a finite Galois extension of odd degree, then $L \subseteq \mathbb{R}$.

Solution from James Alcala

Let $\sigma : \mathbb{C} \to \mathbb{C}$ be complex conjugation. Since $K \subset \mathbb{R}$, σ is a K-homomorphism. Since L/K is finite dimensional and Galois, it is in particular normal, so $\sigma(L) = L$ by Hungerford, 3.14iii) (chapter on Fields and Galois theory). In particular, $\sigma|_L$ is a K-automorphism of L, so it is an element of $Aut_K L$. Because L/K is Galois, this group has the same order as the extension, which is odd. Now, $\sigma|_L \in Aut_K L$ means that $< \sigma|_L >$ must have order one or two. But if it were order two, then that would be a subgroup of $Aut_K L$ of order 2, which can't exist as $|Aut_K L|$ is odd. So, $< \sigma|_L >$ has order one, which means complex conjugation on L is the identity, so it cannot contain any complex numbers, which implies the result.

Solution from Derek Lowenberg

To show $L \subset \mathbb{R}$ it suffices to show that $i \notin L$. Suppose $i \in L$ so that $K(i)/K$ is an intermediate field extension of L/K. By the Galois correspondence we have that $\mathrm{Aut}_{K(i)}L$ is a subgroup of $\mathrm{Aut}_K L$ such that $[K(i) : K] = [\mathrm{Aut}_K L : \mathrm{Aut}_{K(i)}L]$. However $|\mathrm{Aut}_K L|$ is odd but $[K(i) : K] = 2$, thus it cannot divide $|\mathrm{Aut}_K L|$, a contradiction. Hence $i \notin L$.

(3) Let K be a finite field of characteristic p. Prove that every element of K has a unique p-th root in K.

Solution from Derek Lowenberg

The map $K \to K$ given by the p^{th} power, $x \mapsto x^p$, is a ring homomorphism: for $a, b \in K$ we have $a^p b^p = (ab)^p$ and $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$ since for $i \neq 0, p$ we have that $\binom{p}{i}$ is divisible

by p and is thus 0 in K. Since the p^{th} power map is a nonzero ring homomorphism from a field, its kernel is 0. Since an injective endomorphism of a finite set must also be surjective, the p^{th} power map is an isomorphism. Therefore each element of K has a unique p^{th} root, given by the inverse of this isomorphism.

(4) Let $f(X) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ Prove that $f(x) = 0$ is not solvable by radicals over $\mathbb{Q}$.

Solution by Jacob Garcia.

First, recall *Theorem V.4.12* in Hungerford:

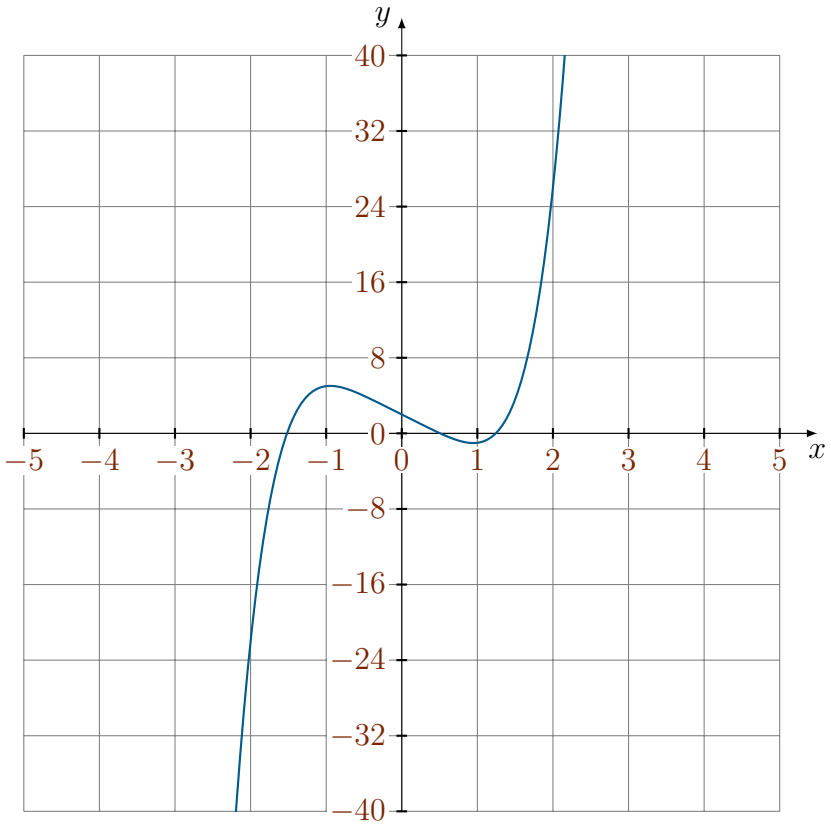
THEOREM 4 — If p is prime and f is an irreducible polynomial of degree p over $\mathbb{Q}$ which has precisely two non-real roots in the field of complex numbers, then the Galois group of f is isomorphic to S_p.

Also see *Corollary V.9.5*:

THEOREM 5 — Let K be a field and $f \in K[x]$. If the equation $f(x) = 0$ is solvable by radicals, then the Galois group of f is a solvable group.

(A slightly stronger version of this fact can be found in *Corollary V.9.7.*)

Now consider $f'(x) = 5x^4 - 4$. Usual calculus arguments show that $f'(x)$ has two local extrema, and that f is increasing on $(-\infty, -\sqrt[4]{\frac{4}{5}}) \cup (\sqrt[4]{\frac{4}{5}}, \infty)$, and is decreasing on $(-\sqrt[4]{\frac{4}{5}}, \sqrt[4]{\frac{4}{5}})$. Also note that $f(-2) = -22$, $f(0) = 2$, $f(1) = -1$, and $f(2) = 26$. Thus by intermediate value theorem, there exists real zeros between -2 and 0, between 0 and 1, and between 1 and 2. These are the only real zeros by the increasing/decreasing information, and so by above theorem, f has Galois group of S_5. Then apply the contrapositive of the corollary for the desired result.



(5) Let F/K be a field extension whose transcendence degree is finite. Prove that if F is algebraically closed, then every K-monomorphism $F \to F$ is in fact an automorphism.

Solution from James Alcala.

Suppose that F/K is a field extension with finite transcendence degree, F is algebraically closed, and $\sigma : F \to F$ is a $K-$monomorphism. Let $u \in F$, and let $S = \{s_1, s_2, \ldots, s_n\}$ be a transcendence base of F/K, and consider the field $L = K(\sigma(s_1), \sigma(s_2), \ldots, \sigma(s_n))$. F is algebraic over L (see justification below), so there exists a minimal polynomial $g \in L[x]$ such that $g(u) = 0$. Then $\sigma^{-1}(g) \in K(s_1, s_2, \ldots, s_n)[x]$ factors completely in F. σ sends roots to roots, so every root of g is in the image of σ. So because u is in the image of σ, $\exists u'$ such that $\sigma(u') = u$, so σ is surjective and hence a $K-$automorphism.

Solution from Derek Lowenberg.

Let F/K be a field extension whose transcendence degree n is finite. Let $\sigma\colon F \to F$ be a K-monomorphism. Let $\{y_1, \ldots, y_n\}$ be a transcendence base for F over K. Consider the field $L = K(\sigma(y_1), \ldots, \sigma(y_n))$. Since σ is injective, if there is some nonzero $f \in K[x_1, \ldots, x_n]$ such that $f(\sigma(y_1), \ldots, \sigma(y_n)) = 0$, then $f(y_1, \ldots, y_n) = 0$, which is not true by assumption. Hence $\sigma(y_1), \ldots, \sigma(y_n)$ are also algebraically independent. Indeed, they also comprise a maximal algebraically independent set; denote this by S.

This implies that F is algebraic over L, as follows: pick $\alpha \in F$ where $\alpha \notin S$. Then $S \cup \{\alpha\}$ is algebraically dependent, so there is some $h \in K[x_0, x_1, \ldots, x_n]$ such that
$h(\alpha, \sigma(y_1), \ldots, \sigma(y_n)) = 0$. Since S is algebraically independent, α must appear in this expression, so that

$$h(\alpha, \sigma(y_1), \ldots, \sigma(y_n)) = p_0(\sigma(y_1), \ldots, \sigma(y_n)) + \cdots + p_m(\sigma(y_1), \ldots, \sigma(y_n))\alpha^m = 0$$

Thus we see that α is algebraic over $K(\sigma(y_1), \ldots, \sigma(y_n)) = L$. Of course, the elements of S are also algebraic over L, so F is an algebraic extension of L.

Let $u \in F$. Since F is algebraic over L, u has a minimal polynomial in $L[x]$, say g. Then $\sigma^{-1}(g) \in K(y_1, \ldots, y_n)$ factors completely in F, as F is algebraically closed. Since σ sends roots to roots, we see that every root of g is in the image of σ; in particular u is in the image of σ. Therefore σ is also surjective, that is, a K-automorphism.