MATH 115C: MIDTERM EXAMINATION
MAY 7, 2018
DANIEL HALMRAST

Problem 1

Part a. Suppose p is prime, and H is a transitive subgroup of S_p containing a transposition. Prove that $H = S_p$.

Proof. We define a relation $\sim$ on the set $\{1, \cdots, p\}$ as

$$i \sim j \iff (ij) \in H$$

First, observe that $\sim$ is an equivalence relation. Trivially, for every $i \in \{1, \cdots, p\}$, $i \sim i$, since $(ii) = e \in H$. Furthermore, if $i \sim j$, then $(ij) \in H$, and since $(ij) = (ji)$, it follows that $(ji) \in H$ as well, and so $j \sim i$. Finally, observe that if $i \sim j$ and $j \sim k$, then $(ij), (jk) \in H$, and in particular

$$(ij)(jk)(ij) = (ik)$$

is in H as well. Thus, $i \sim k$. Therefore, $\sim$ is an equivalence relation, and partitions $\{1, \cdots, p\}$ into disjoint nonempty equivalence classes.

Next, we show that there is only one equivalence class. Suppose for a contradiction that there is more than one equivalence class in $\{1, \cdots, p\}$ under $\sim$. We show that every equivalence class has the same number of elements. To do so, we will establish a (set-theoretic) bijection between the equivalence classes.

Since H contains a transposition, at least one equivalence class contains more than one element. Let $[i]$ be such an equivalence class. We establish a bijection between the elements of $[i]$ and the elements of $[j]$ for $j \notin [i]$. To do so, let $g \in H$ be such that $g(i) = j$ (which exists since H acts transitively on $\{1, \cdots, p\}$). Let $x \in [i]$ with $x \neq i$. Then,

$$g(ix)g^{-1} = (jz)$$

for some $z \in \{1, \cdots, p\}$. In particular, since $g, g^{-1}, (ix) \in H$, it follows that $(jz) \in H$ as well, and so $z \in [j]$. We define the bijection to be

$$\Phi : [i] \to [j]$$

$$\Phi(x) = z$$

where z is the element described above. This is indeed a bijection, since it is invertible. In particular, the inverse is given as

$$\Phi^{-1} : [j] \to [i]$$

where $z \in [j]$ gets sent to the $x \in [i]$ for which

$$g^{-1}(jz)g = (ix)$$

This is clearly an inverse, since $\Phi^{-1}\Phi(x)$ is given by

$$g^{-1}g(ix)g^{-1}g = (ix)$$

and so

$$\Phi^{-1}\Phi(x) = x$$

and similarly $\Phi\Phi^{-1}(x) = x$. Thus, Φ has a two-sided inverse, and is a bijection.

Now, since the equivalence classes partition $\{1, \cdots, p\}$, and each has the same size (n, say), it follows that n divides p. We have already seen that $n > 1$ since H contains a transposition, so $n = p$. Thus, there is only one equivalence class. Therefore, H contains all transpositions, and since the transpositions generate S_p, $H = S_p$ as desired. $\square$

Part b. Suppose $f \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and has prime degree p. If f has exactly $p-2$ real roots and 2 complex roots, show the Galois group of f over $\mathbb{Q}$ is S_p.

Proof. Let H be the Galois group of f. Since f has exactly p roots and is irreducible, H permutes the p roots of f, and thus H is a subgroup of S_p. Furthermore, H contains the transposition defined by complex conjugation, which transposes the two complex roots. Finally, since f is irreducible, H acts transitively on the roots of f. Thus, H satisfies the criteria of part a, and $H = S_p$ as desired.

To see that H acts transitively on the roots, let K be the splitting field of f, so that $H = \mathrm{Gal}(K/\mathbb{Q})$, and let α, β be roots of f. Then, there exists a field homomorphism

$$\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$$
$$\sigma(q) = q \text{ for } q \in \mathbb{Q}$$
$$\sigma(\alpha) = \beta$$

which fixes $\mathbb{Q}$. Since α and β both have f as their minimal polynomial, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}]$ and so this field homomorphism is indeed an isomorphism by problem 2 part i. Furthermore, this extends to an automorphism of K which fixes $\mathbb{Q}$ and sends α to β, as desired. $\square$

Part c. Determine the Galois group of $x^5 - 4x + 2$ over $\mathbb{Q}$.

Proof. Let $f(x) = x^5 - 4x + 2$. Observe that its derivative

$$f'(x) = 5x^4 - 4$$

has exactly two real roots $\alpha_\pm = \pm(\frac{4}{5})^{\frac{1}{4}}$. Thus, f has at most 3 real roots.

Now, $f(-10) < 0$, $f(0) > 0$, $f(1) < 0$, and $f(100) > 0$. By the intermediate value theorem, f has at least 3 real roots. Thus, f has exactly 3 real roots and 2 complex roots.

Furthermore, f is irreducible. This is clear by the Eisenstein criterion at $p = 2$, since 2 does not divide $a_5 = 1$, but 2 does divide $a_1 = 4$, and $2^2 = 4$ does not divide $a_0 = 2$ (for a_i the coefficient of the ith term of f).

Applying the result of part b, we see immediately that the Galois group of f is S_5, as desired. $\square$

Problem 2

Let K be a field.

Part i. Let F and F' be two finite extensions of K. When the degrees of these two extensions are equal, show that every K-homomorphism $F \to F'$ is an isomorphism.

Proof. Let $\sigma : F \to F'$ be a K-homomorphism. That is, σ is a field homomorphism that fixes $K \subset F, F'$. In particular, thinking of F and F' as K-vector spaces, we see that σ is a linear map. This follows immediately, since for $\alpha \in K$, $x, y \in F$,

$$\sigma(\alpha x + y) = \sigma(\alpha)\sigma(x) + \sigma(y) = \alpha\sigma(x) + \sigma(y)$$

as desired.

Since F and F' have the same dimension as K-vector spaces, we just need to show σ is injective, and σ will automatically be bijective with a linear inverse. However, field homomorphisms are always injective, so σ is a linear isomorphism between F and F'. Thus, σ^{-1} is a linear map, and is seen to be a K-homomorphism by observing that

$$\sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y)$$

for all $x, y \in F'$. Indeed, since

$$xy = \sigma(\sigma^{-1}(xy)) = \sigma(\sigma^{-1}(x))\sigma(\sigma^{-1}(y))$$

we have that

$$\sigma(\sigma^{-1}(xy)) = \sigma(\sigma^{-1}(x)\sigma^{-1}(y))$$

and since σ is bijective,

$$\sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y)$$

Thus, σ is an isomorphism that fixes K, as desired. $\square$

Part ii. Give an example, with justification, of two finite extensions F and F' of K which have the same degree but are not isomorphic over K.

Proof. Let $K = \mathbb{Q}$, and let $F = \mathbb{Q}(\zeta_3)$ with ζ_3 a primitive 3rd root of unity, and let $F' = \mathbb{Q}(\sqrt[3]{2})$. Then, F is the splitting field of $f(x) = x^3 - 1$, and $\mathrm{Gal}(F/K) = \mathbb{Z}/3\mathbb{Z}$. However, F' is not the splitting field of the minimal polynomial of $\sqrt[3]{2}$, and in particular, there are only two K-automorphisms of F': the trivial automorphism, and the automorphism

$$\sigma(\sqrt[3]{2}) = -\sqrt[3]{2}$$

Thus, $\mathrm{Aut}(F) \neq \mathrm{Aut}(F')$, which implies that F is not isomorphic to F'.

To see that $F \ncong F'$, we observe that if $F \cong F'$ via an isomorphism $\sigma : F \to F'$, then $\mathrm{Aut}(F) \cong \mathrm{Aut}(F')$ as groups. This is given by the group homomorphism

$$\Phi : \mathrm{Aut}(F) \to \mathrm{Aut}(F')$$
$$\Phi(g) = \sigma \circ g \circ \sigma^{-1}$$

where we observe that

$$\Phi(gh) = \sigma gh\sigma^{-1} = \sigma g\sigma^{-1}\sigma h\sigma^{-1} = \Phi(g)\Phi(h)$$

Now, this group homomorphism is invertible by

$$\Phi^{-1} : \mathrm{Aut}(F') \to \mathrm{Aut}(F)$$
$$\Phi^{-1}(g) = \sigma^{-1} \circ g \circ \sigma$$

since

$$\Phi^{-1}\Phi(g) = \sigma^{-1}\sigma g \sigma^{-1}\sigma = g$$

and

$$\Phi\Phi^{-1}(g) = \sigma\sigma^{-1} g \sigma\sigma^{-1} = g$$

and thus is an isomorphism.

Thus, since $\mathrm{Aut}(F) = \mathbb{Z}/3\mathbb{Z}$ and $\mathrm{Aut}(F') = \mathbb{Z}/2\mathbb{Z}$, we see that $F \ncong F'$, as desired. $\square$

Part iii. let L be a finite extension of K. Let F and F' be two finite extensions of L. Show that if F and F' are isomorphic as extensions of L, then they are isomorphic as extensions of K.

Proof. Let $\sigma : F \to F'$ be an L-isomorphism of F and F'. In particular, σ fixes $K \subset L$. Thus, σ is a K-isomorphism as well, and $F \cong F'$ as extensions of K, as desired. $\square$

Part iv. Prove or disprove the converse.

Proof. We disprove the statement by contradiction.

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}(\sqrt[4]{2})$, and $F' = \mathbb{Q}(i\sqrt[4]{2})$. Now, these are all intermediate fields of the extension of $\mathbb{Q}$ to the splitting field of $x^4 - 2$, namely $\mathbb{Q}(i, \sqrt[4]{2})$. In particular, we know what $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ looks like: it is the dihedral group D_8, presented as

$$\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$$

where

$$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$$

$$\tau(i) = -i$$

In particular, these are all the automorphisms of the splitting field that fix $\mathbb{Q}$. Thus, any isomorphism from $\mathbb{Q}(\sqrt[4]{2})$ to $\mathbb{Q}(i\sqrt[4]{2})$ must be a restriction of products of these (since any isomorphism of intermediate fields induces an automorphism on the splitting field). In particular, the only ones which send $\mathbb{Q}(\sqrt[4]{2})$ to $\mathbb{Q}(i\sqrt[4]{2})$ are σ, $\tau\sigma$,$\sigma\tau$, and $\tau\sigma^3$. Observe that each of these sends $\sqrt[4]{2}$ to $i\sqrt[4]{2}$. So let σ' be any such isomorphism.

σ' does not fix $\mathbb{Q}(\sqrt{2})$. This is evident, since

$$\sigma'(\sqrt{2}) = \sigma'(\sqrt[4]{2})\sigma'(\sqrt[4]{2}) = -\sqrt{2}$$

and so $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(i\sqrt[4]{2})$ are $\mathbb{Q}$-isomorphic, but not $\mathbb{Q}(\sqrt{2})$-isomorphic. $\square$

Problem 3

Let $F = \mathbb{C}(x, y)$ be the function field in two variables x and y. Let $n \geq 1$, and let $K = \mathbb{C}(x^n + y^n, xy)$.

Part i. Let $K' = K(x^n)$, which is a subfield of F. Show that K'/K is a quadratic extension.

Proof. Observe that the polynomial

$$f(s) = (s - x^n)(s - y^n) = s^2 - (x^n + y^n)s + (xy)^n$$

is in $K[s]$. In fact, it is the minimal polynomial for x^n (since neither x^n nor y^n are in K), and is quadratic. Thus, K'/K is quadratic, as desired. $\square$

Part ii. Show that F/K' is cyclic of order n.

Proof. It is clear that $F = K'(x)$, since $y = (xy)(x)^{-1}$, and so $K'(x)$ contains y. Now, the minimal polynomial for x in K' is

$$f(s) = s^n - x^n = x^n(\frac{s^n}{x^n} - 1) = x^n \prod_{d|n} \Phi_d(\frac{s}{x})$$

where Φ_d is the dth cyclotomic polynomial. This has as its roots $x\zeta_n^k$ where ζ_n is a primitive nth root of unity, and $0 \leq k < n$. Clearly, this is irreducible, since if $f(s) = g(s)h(s)$, then

$$g(s) = \prod_{i \in S}(s - x\zeta_n^i)$$

where $S \subsetneq \{1, \cdots, n\}$. However, expanding this shows that each coefficient (except the first and last) contains a power of x less than n, which is not in K'. So, $g(s) \notin K'[s]$, and $f(s)$ must be irreducible.

Thus, the degree of the extension F/K' is n. Furthermore, the automorphism

$$\sigma : F \to F$$

$$\sigma(x) = x\zeta_n \sigma(y) = y\zeta_n$$

fixes K', since $\sigma(x^n) = (\sigma(x))^n = x$, and has order n. Thus, it exhausts the Galois group of F/K', and so

$$\mathrm{Gal}(F/K') = \langle \sigma \rangle$$

as desired. □

Part iii. Show F/K is Galois, and determine its Galois group.

Proof. In order to show F/K is Galois, we will show that F splits a polynomial in $K[s]$. Namely, consider

$$f(s) = (s^n - x^n)(s^n - y^n) = s^{2n} - (x^n + y^n)s^n + (xy)^n$$

which is clearly in $K[s]$. In particular, this splits in F with roots $x\zeta_n^k$ and $y\zeta_n^k$ for $0 \leq k < n$. Thus, F/K is Galois of degree at most $2n$. By considering the intermediate field $K' \neq F$, we see that $[F : K] = [F : K'][K' : K] \geq 2n$. Thus, $[F : K] = 2n$.

Observe that we have the following K-automorphisms of F

$$\sigma(x) = x\zeta_n$$

$$\sigma(y) = y\zeta_n$$

$$\tau(x) = y$$

$$\tau(y) = x$$

with $\sigma^n = 1$ and $\tau^2 = 1$. This forms an Abelian group, since

$$\sigma\tau(x) = y\zeta_n = \tau\sigma(x)$$

$$\sigma\tau(y) = x\zeta_n = \tau\sigma(y)$$

Clearly, this group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

$\square$

1. Problem 4

Let p be a prime number, and let K denote a finite extension of $\mathbb{F}_p$. Recall that $\mathrm{Gal}(K/\mathbb{F}_p)$ is generated by the Frobenius automorphism $\sigma(t) = t^p$.

Part a. If $h(z) = \frac{-1}{1+z}$, for $z \in K$, $z \neq 0, -1$, show that $h^3(z) = z$. Hence, show that $f(x) = x^{p+1} + x^p + 1$ can only have irreducible factors of degree three or one.

Proof. Observe first that

$$\begin{aligned} h^2(z) &= \frac{-1}{1+\frac{-1}{1+z}} \\ &= \frac{-1(1+z)}{(1+\frac{-1}{1+z})(1+z)} \\ &= \frac{-(1+z)}{z} \\ h^3(z) &= \frac{-1}{1+\frac{-(1+z)}{z}} \\ &= \frac{-1(z)}{(1+\frac{-(1+z)}{z})(z)} \\ &= \frac{-z}{-1} = z \end{aligned}$$

as desired.

Now, we consider $f(x) = x^{p+1} + x^p + 1$. Rewriting this, we see that for $x \neq 0, -1$,

$$\begin{aligned} f(x) &= x\sigma(x) + \sigma(x) + 1 \\ &= (x+1)\sigma(x) + 1 \\ &= (x+1)(\sigma(x) - \frac{-1}{1+x}) \\ &= (x+1)(\sigma(x) - h(x)) \end{aligned}$$

Thus, if $\alpha \neq 0, -1$ is a root of f, then $\sigma(\alpha) = h(\alpha)$. So, for α not in $\mathbb{F}_p$, the extension $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ has Galois group generated by $\sigma(t)$. But on the roots of f, $\sigma(t) = h(t)$ has order 3, and so the Galois group of $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ has order 3. Therefore, the minimal polynomial for α has degree 3, and so the irreducible factors of f are either linear (if $\alpha \in \mathbb{F}_p$) or of degree 3 (the minimal polynomial for α). $\square$

Part b. Show further that f has at most two linear factors over $\mathbb{F}_p$, and that if $p \neq 2$, f has such factors if and only if -3 is a square in $\mathbb{F}_p$.

Proof. We observe that

$$h(z) = \frac{-1}{1+z}$$

is the identity only at $\alpha_\pm = \frac{-1\pm\sqrt{-3}}{2}$ (which is obtained by solving the quadratic $z = \frac{-1}{1+z}$). In particular, this means that if $\beta \neq \alpha_\pm$ is a root of f, then the extension $\mathbb{F}_p(\beta)/\mathbb{F}_p$ is strictly a degree three extension with Galois group generated by h. Thus, f can have at most two linear factors, specifically $\alpha_\pm$.

Now, if $p = 2$, then $2 = 0$, and so $\alpha_\pm \notin \mathbb{F}_2$, since it would require dividing by zero. However, if $p \neq 2$, and -3 is a square in $\mathbb{F}_p$, then $\alpha_\pm \in \mathbb{F}_p$, and so

$$\begin{aligned} f(\alpha_\pm) &= (\alpha_\pm + 1)(\sigma(\alpha_\pm) - h(\alpha_\pm)) \\ &= (\alpha_\pm + 1)(\alpha_\pm - \alpha_\pm) = 0 \end{aligned}$$

where we have used the fact that $\sigma(\alpha) = \alpha$ for $\alpha \in \mathbb{F}_p$. Thus, f has $\alpha_\pm$ as two of its roots, and these roots are in $\mathbb{F}_p$, so f has two linear factors.

Conversely, if -3 is not a square in $\mathbb{F}_p$, then $\alpha_\pm \notin \mathbb{F}_p$. Therefore, f does not have $\alpha_\pm$ as linear factors over $\mathbb{F}_p$. Since these are the only possible linear factors of f, f must not have any linear factors, as desired. □

Part c. Deduce that -3 is a square in $\mathbb{F}_p$ for primes $p = 3n + 1$ but not for primes $p = 3n + 2$.

Proof. Clearly, f has degree $p + 1$. Thus, if $p = 3n + 1$, f has $3n + 2$ roots. Since the irreducible factors of f are of degree 3 or 1, there must be exactly two linear factors of f. Thus, -3 is a square in $\mathbb{F}_{3n+1}$.

However, for $p = 3n + 2$, f has degree $3(n + 1)$, and thus has $3(n + 1)$ roots. Since the irreducible factors of f are of degree 3 or 1, with at most two factors being linear, all irreducible factors must be of degree 3, and therefore -3 is not a square in $\mathbb{F}_{3n+2}$. □