Math 505, WINTER 2018 ***MIDTERM*** ***Peter Gylys-Colwell***

Problem 1

For any $a \in K$ if $a > 0$ then since every positive element of K is a square in K a has a square root. If $a < 0$ then $-a$ is positive with square root $\sqrt{-a}$. Thus $i\sqrt{-a}$ is the squareroot of a since $(i\sqrt{-a})^2 = -1 \cdot -a = a$. Thus we know every element in K has a square root
For any $\alpha = x + iy \in K(i)$ we can write α in polar form (while the notation is analytical, all of the following arguments are algebraic)

$$\alpha = re^{i\theta} = r(\cos(\theta) + i\sin(\theta))$$

where $r = \sqrt{x^2 + y^2} \in K$ and $e^{i\theta} = \cos(\theta) + i\sin(\theta) = \frac{\alpha}{r}$. We have that $\cos(\theta)$ and $\sin(\theta) \in K$ since applying the conjugate automorphism $i \to -i$

$$\overline{e^{i\theta}} = \cos(\theta) - i\sin(\theta)$$

we get the following element is fixed under both automorphisms in $\mathrm{Gal}(K(i)/K)$ and thus in K

$$\cos(\theta) = \frac{e^{i\theta} - \overline{e^{i\theta}}}{2} \in K$$

We have that

$$\sqrt{\alpha} = \sqrt{r}(\cos(\theta/2) + i\sin(\theta/2)) \in K(i)$$

Where $\sqrt{r} \in K$ and for appropriate choice of n (although intuition comes from the half angle formula, this is defined purely algebraically)

$$\cos(\theta/2) = -1^n\sqrt{\frac{1 + \cos\theta}{2}} \in K$$

$$\sin(\theta/2) = \sqrt{\frac{1 - \cos\theta}{2}} \in K$$

The only thing left to check is that we actually have $\left(\sqrt{\alpha}\right)^2 = \alpha$:

$$\left(\sqrt{\alpha}\right)^2 = (\sqrt{r})^2(\cos(\theta/2)^2 - \sin(\theta/2)^2 + 2i\cos(\theta/2)\sin(\theta/2))$$

$$= (\sqrt{r})^2\left(\frac{1 + \cos\theta}{2} - \frac{1 - \cos\theta}{2} + (-1)^n 2\sqrt{\frac{1 - \cos\theta}{2}}\sqrt{\frac{1 + \cos\theta}{2}}i\right)$$

$$= r(\cos(\theta) + (-1)^n\sqrt{1 - \cos^2(\theta)}i) = r(\cos(\theta) + i\sin(\theta)) = \alpha$$

We know that $(-1)^n\sqrt{1 - \cos^2(\theta)} = \sin(\theta)$ since from how $\cos(\theta), \sin(\theta)$ are defined

$$\cos^2(\theta) + \sin^2(\theta) = \left(\frac{x}{\sqrt{x^2 + y^2}}\right)^2 + \left(\frac{y}{\sqrt{x^2 + y^2}}\right)^2 = \frac{x^2 + y^2}{x^2 + y^2} = 1$$

Thus $\sin^2(\theta) = 1 - \cos^2(\theta) \Rightarrow \sin(\theta) = \pm\sqrt{1 - \cos(\theta)}$

Problem 2

For any finite extension E of $K(i)$ generated by $\alpha_1, \alpha_2, \dots \alpha_n$ we have that E is contained in the splitting field L of the product of minimal polynomials $m_1, m_2, \dots m_n$ of the generators. When eliminating duplicates (where $m_i = m_j$) in the product, we get a seprable polynimial p.

p is seperable since if α was a double root, then it must be a root of either some $m_i \neq m_j$ which would contradict both m_i, m_j being irreducible since one must divide the other. The other possibility is that α is a double root of m_i but this cannot happen since K is characteristic 0

K is characteristic 0 since it has a total ordering so if it were the case

$$0 = 0 + 1 + 1 + \dots 1$$

then $0 < 0$ which would contradict our ordering

We can now conclude L is the splitting field of the seprable polynomial p and is thus Galois. We have that L is a finite extension since it is generated by the roots of $m_1, m_2, \dots m_n$ which is a finite set.

If we have the 2-Sylow subgroup $H \subset G = \mathrm{Gal}(L/K)$, then we have $|H| = 2^n$ and $|G| = 2^n m$ where m odd. Letting $F = L^H$ be the fixed field of H we have

$$[L : F][F : K] = [L : K] = |G| = 2^n m$$

By the correspondence of Galois theory we have $|H| = [L : F] = 2^n$ and thus the degree of F over K is odd

$$[F : K] = m$$

Problem 3

From the Primitive Element Theorem since F is a seperable (seperable since K is characteristic 0) and finite extension of K we know there exists $\alpha \in F$ such that

$$F = K(\alpha)$$

We have that the degree of the minimal polynimial d_α satisfies

$$d_\alpha = [K(\alpha) : K] = m$$

Thus d_α is odd as we established m to be odd in problem 2. Thus since every odd degree polynimial has a root in K, in order for m_α to be irriducible it must be linear. Hence

$$d_\alpha = [F : K] = 1$$

Since $m = 1$ we have established G is a 2-Group:

$$|G| = 2^n$$

Problem 4

We have that $\text{Aut}(L/K(i))$ is a subgroup of $\text{Gal}(L/K)$ with the corresponding fixed field $K(i)$. As a consequence of the Fundamental Theorem of Galois Theory (which states that the size of a subgroup is equal to the index of the Galois Extention over the fixed field)

$$[L : K(i)] = |\text{Aut}(L/K(i))|$$

And thus L is a Galois extension of $K(i)$

Problem 5

Letting $G_1 = \text{Gal}(L/K(i))$, we have that G_1 is a subgroup of $G = \text{Gal}(L/K)$. As we proved in problem 3, $|G| = 2^n$ and thus $|G_1| = 2^k$ for some $k \leq n$. If G_1 is nontrivial it must have a subgroup H_1 of size 2^{k-1} of index 2 follwing from the fact that every group of order p^n has a subgroup of order p^r for all $r < n$. The reason for this is as follows:
We can induct on n where $|G| = p^n$, begining with the trivial base case $n = 1$ which has no subgroups except for the trivial group
We have that G has a nontrivial center Z since from the class equations

$$|G| = |Z| + \sum |G : C_G(g_i)| = p^n$$

$p|[G : C_G(g_i)]$ so $p||Z|$ and since $\text{id} \in Z$, $|Z| \geq 1$ so $|Z| = p^k$ for some k
From our classification of abelian groups we know abelian groups of size p^k have subgroups of each order p^i for any $i < k$. We can apply our inductive hypothesis to G/Z since

$$|G/Z| = p^{n-k}$$

G/Z has groups of all order p^i for $i < (n - k)$ and thus from the correspondence theorem we get groups of all orders p^{i+k} in G. Thus we get subgroups of p^r for all $r < n$ either by having a subgroup of Z when $r \leq k$ or from the correspondence of subgroups of the quotient group when $r > k$

Problem 6

Letting $F_1 = L^{H_1}/K(i)$ be the fixed field of H_1 from the Fundamental Theorem of Galois Theory

$$[F_1 : K(i)] = |H_1| = 2$$

This is a contradiction of our conclusion of problem 1 since letting α be a generator of $F_1/K(i)$ we have that the minimal polynimial of α must be quadratic but we have shown in problem 1 every quadratic polynimial splits and thus is reducible. Thus G_1 must be trivial. Thus

$$1 = |G_1| = [L : K(i)] \Rightarrow L = K(i)$$

Thus $K(i)$ is algebraically closed since we have shown any algebraic extension of $K(i)$ is degree 1

Problem 7

Notice that for $\alpha \in \mathbb{C} \setminus \mathbb{R}$, $|\alpha| = 1 \Rightarrow \frac{1}{\alpha} = \overline{\alpha}$ where $\overline{a + bi} = a - bi$ denotes the conjugate. The conjugate is an isomorphism of $\mathbb{C}$ which fixes $\mathbb{R}$ and thus $\overline{f} = f$. We thus have that $\frac{1}{\alpha}$ is a root of f:

$$0 = \overline{f(\alpha)} = f(\overline{\alpha}) = f(\frac{1}{\alpha})$$

If we consider any other root of f β, since f is irriducible, there exists an isomorphism

$$\varphi : k(\alpha) \to k(\beta)$$

which fixes k and maps $\alpha \to \beta$. Thus $\varphi(1/\alpha) = \varphi(1/\beta)$ and so $1/\beta$ is a root of f

$$0 = \varphi(f(1/\alpha)) = f(\varphi(1/\alpha)) = f(1/\beta)$$

Thus f is reciprocal.

f is seperable since it is irriducible in a field of Characteristic 0. Thus the $\deg(f)$ is equal to the number of roots. f must be even degree since it has an even number of roots. There is an even number of roots since we can pair every root α with $1/\alpha$ and the only times $\alpha = \frac{1}{\alpha}$ is if $\alpha = \pm 1$ which would contradict f being irreducible over k

Problem 8

f is irreducible since if f were reducible, then f can be factored as such $f(x) = g(x)h(x)$ where $\deg(h), \deg(g) \geq 1$. Letting H be the splitting field of h over k we have

$$[K : k] = [K : H][H : k]$$

We know that $[H : k] \leq \deg(h)!$ and $[K : H] \leq \deg(g)!$

Since $n = \deg(h) + \deg(g)$ and $\deg(h), \deg(g) \geq 1$, it is the case

$$n! > \deg(h)! \deg(g)! \geq [K : H][H : k] = n!$$

Which is a contradiction. Thus f cannot be be factored

We have that f is seperable following from the fact that we know the degree of a splitting field is bound from above by $\deg(f)!$

$$n! = |\mathrm{Aut}(K/k)| \leq [K : k] \leq \deg(f)! = n!$$

$$\Downarrow$$

$$|\mathrm{Aut}(K/k)| = [K : k]$$

Thus K/k is Galois which implies that f is seperable (Theorem 13 of Dummit and Foote section 14.2).

If $\alpha \in K$ was a root of f then any automorphism $\varphi \in \mathrm{Aut}(k(\alpha)/k)$ is fully determined by $\varphi(\alpha)$. If it was the case that φ was not the identity, then it must be the case $\varphi(\alpha) = \beta$

where $\beta \neq \alpha$ is a root of f. Thus $k \in k(\alpha)$. Then it would be the case that letting $h(x) = (x-\alpha)(x-\beta) \in k(\alpha)[x]$, that $h(x)|f(x) \Rightarrow f(x) = h(x)g(x)$. From this we have the following

$$n! = [K : k] = [K : k(\alpha)][k(\alpha) : k]$$

We have that $K/k(\alpha)$ is the splitting field of g and so $[K : k(\alpha)] \leq \deg(g)!$ and $[k(\alpha) : k] = \deg(f) = n$. Since $\deg(g) = \deg(f) - 2 = n - 2$ we are led to the contradiction

$$n! = n \cdot (n-2)!$$

Thus the only possible automorphism is the identity

Problem 9

Since $F = \overline{k}^{\langle\sigma\rangle}$, we have that

$$\mathrm{Aut}(\overline{k}/F) = \langle\sigma\rangle$$

Notice that for any finite extension $K \supset F$ (with $K \subset \overline{k}$) we have that any automorphism which fixes F

$$\varphi : K/F \to K/F$$

extends to an automorphism

$$\overline{\varphi} : \overline{k}/F \to \overline{k}/F$$

since $\overline{k}$ was defined by taking splitting fields of polynomials, we can extend φ to each splitting field to get our automorphism defined over all of $\overline{k}$

From this fact it follows there is an embedding of groups

$$\mathrm{Aut}(K/F) \subset \mathrm{Aut}(\overline{k}/F) = \langle\sigma\rangle$$

Thus it must be the case that K is cyclic over F

Problem 10

We know that every finite field is of the form $\mathbb{F}_{p^n}$. If $p = 2$ then every element is a square since the Frobenius endomorphism is bijective.

If otherwise, we can consider the mapping

$$s : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$

$$\alpha \to \alpha^2$$

We have that the polynimial $x^2 - s(\alpha)$ has at most two roots so only two elements can map to the same element in s. This fact along with knowing no nonzero elements are nilpotent give us a bound on the size of the image

$$|s(\mathbb{F}_{p^n})| \geq \frac{|\mathbb{F}^*_{p^n}|}{2} + |\{0\}| = \frac{p^n - 1}{2} + 1$$

For any $\alpha \in \mathbb{F}_{p^n}$ we have that the set

$$\alpha - s(\mathbb{F}_{p^n})$$

is also of size $\frac{p^n-1}{2} + 1$ since the addition mapping is one-to-one. Thus we have

$$|s\left(\mathbb{F}_{p^n}\right)| + |\alpha - s(\mathbb{F}_{p^n})| \geq p^n + 1 > |\mathbb{F}_{p^n}|$$

Thus from the pigeon hole principle the sets must intersect. So there exists $\beta, \gamma \in \mathbb{F}_{p^n}$

$$\alpha - \beta^2 \in s(\mathbb{F}^{p^n})$$

$$\Downarrow$$

$$\alpha = \beta^2 + \gamma^2$$