412 Individual HW8

Jack Madden

April 2024

Problem 1

a) We find the irreducible polynomial of $\sqrt{2+\sqrt{2}}$:

$$x = \sqrt{2+\sqrt{2}}$$
$$x^2 - 2 = \sqrt{2}$$
$$x^4 - 4x^2 + 2 = 0$$

This polynomial is irreducible via Eisenstein choosing $p = 2$. We can find its roots by letting $y = x^2$, giving us $y^2 - 4y + 2 = 0$. After plugging this into the quadratic formula, we get $y = 2 \pm \sqrt{2}$, and hence the conjugates of $\sqrt{2+\sqrt{2}}$ in $\mathbb{C}$ are $\pm\sqrt{2 \pm \sqrt{2}}$.

b) We claim that $x^2 - (2+\sqrt{2})$, which has $\sqrt{2+\sqrt{2}}$ as a root is irreducible over $\mathbb{Q}(\sqrt{2})$. This is because from part a we have that $[\mathbb{Q}(\sqrt{2+\sqrt{2}} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2+\sqrt{2}} : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$ and since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ has degree 2, $[\mathbb{Q}(\sqrt{2+\sqrt{2}} : \mathbb{Q}(\sqrt{2})] = 2$ and therefore the polynomial is irreducible and the conjugates are $\pm\sqrt{2+\sqrt{2}}$.

c) We can find the minimal polynomial by multiplying the linear factors $(x - (\sqrt{2}+i))(x - (\sqrt{2}-i))$ to get the minimal polynomial $x^2 - 2\sqrt{2}x + 3$ over the reals, the conjugates are clearly $\sqrt{2}+i, \sqrt{2}-i$.

d) We have:

$$\sqrt{2} + i = x$$
$$2\sqrt{2}i = x^2 - 1$$
$$-8 = x^4 - 2x^2 + 1$$
$$0 = x^4 - 2x^2 + 9$$

We must show that this polynomial is irreducible. Notice that $\sqrt{2}, i \in \mathbb{Q}(\sqrt{2}+i)$ and thus $[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt{2}, i)] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. But this is 4, by the known polynomials x^2+1 and x^2-2. Thus, the degree of $[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}]$ is 4 and therefore this polynomial is irreducible. using the quadratic formula we get that the conjugates are $\pm\sqrt{1 \pm 2\sqrt{-2}}$

Problem 2

a) Consider arbitrary $\sigma \in G(K/F)$. Let $k_1, k_2 \in K$. The properties of an automorphism (ismorphism (homomorphism)) mean that:

$$\sigma(k_1 + k_2) = \sigma(k_1) + \sigma(k_2)$$

and also for $a \in F$, since σ fixes a,

$$\sigma(ak_1) = \sigma(a)\sigma(k_1) = a\sigma(k_1)$$

thus, we have filled the properties of a linear map. Also, since $G(K/F)$ is a group, every map σ has an inverse map σ^{-1}, which is also a linear transformation by the same argument. THus, every σ is an invertible linear map.

b) Consider the field extension $\mathbb{Q} \subset \mathbb{R}$. Consider the linear map $x \to 2x$. This can easily be verified to be a linear map, but it does not fix elements in $\mathbb{Q}$ and thus cannot be an automorphism over it.

c)

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \langle (0,0) \rangle$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \langle (1,0) \rangle$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \langle (0,1) \rangle$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \langle (1,1) \rangle$$

Problem 3

a) We know that $\mathbb{F}_{p^n}$ is the set of roots of $x^{p^n} - x \in \mathbb{F}_p[x]$. Hence, we know that $\sigma^n(x) = x^{p^n} = x$ which is the identity permutation. Suppose that $x^{p^k} = x$ for some $k < n$. But this implies that $x^{p^k - 1} = 1$ for all $x \in \mathbb{F}^*$, which would imply that $\mathbb{F}^*$ is not cyclic, which is a contradiction. Thus, the order of σ is n and therefore it generates a cyclic group isomorphic to $\mathbb{Z}_n$.

b) We know that $|G(\mathbb{F}_p^n/\mathbb{F}_p)| = [\mathbb{F}_p^n : \mathbb{F}_p] = [(\mathbb{F}_p)^n : \mathbb{F}]_p] = n$. This is true because $|\mathbb{F}_p^n| = |(\mathbb{F}_p)^n|$ implies that $\mathbb{F}_p^n \cong (\mathbb{F}_p)^n$ as they are finite fields. Thus, since the order of the Galois group is n and we have found an element that generates a group of order n, $G(\mathbb{F}_p^n/\mathbb{F}_p) \cong \mathbb{Z}_n$.

Problem 4

a) Let us consider K as a vector space over F. Notice that $F(\alpha_1)$ has a basis $\{1, \alpha_1, \dots, {\alpha_1}^{k_1-1}\}$, and therefore $F(\alpha_1, \alpha_2)$ has a basis

$$\{1, \alpha_2, \dots, \alpha_2^{k_2-1}, \alpha_1\alpha_2, \alpha_1\alpha_2^2, \dots, \alpha_1\alpha_2^{k_2-1}, \alpha_1^2\alpha_2, \alpha_1^2\alpha_2^2, \dots, \alpha_1^2\alpha_2^{k_2-1}, \dots, \alpha_1^{k_1-1}\alpha_2, \alpha_1^{k_1-1}\alpha_2^2, \dots, \alpha_1^{k_1-1}\alpha_2^{k_2-1}\}$$

We can continue this up to $F(\alpha_1, \dots, \alpha_n)$. Thus we see that any element $k \in K$ can be expressed as a linear combination of these basis elements and scalars in F. Since σ must fix F, and $\sigma(\alpha^i) = \sigma(\alpha) \cdots \sigma(\alpha)$ (i times) $= \sigma^i(\alpha)$, for any $\alpha, i \in \mathbb{Z}$ we see that $\sigma(k)$ is determined by the values of $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ for all $k \in K$.

b) Consider the 5th roots of unity and the permutation σ that maps $\zeta^1 \to \zeta^2, \zeta^2 \to \zeta^1, \zeta^3 \to \zeta^3, \zeta^4 \to \zeta^4$. These roots are conjugate but it is an invalid permutation because $\zeta^1 \to \zeta^2$ determines that $\zeta^2 \to \zeta^4$.

Problem 5

a) The roots of $x^p - 1$ are $R = \{1(\zeta^0), \zeta, \dots, \zeta^{p-1}\}$. Since σ must permute these roots, $\sigma(\zeta) \in R$. However, $\sigma(\zeta) \neq \zeta^0 = 1$ as otherwise for some rational number $x \in \mathbb{Q}$, $\sigma(x) = \sigma(x \cdot 1) = \sigma(x \cdot \zeta^0) = x\zeta^k \notin \mathbb{Q}$ for some $k \neq 0$ and if σ does not fix the rationals it is not an isomorphism over them.

b) Suppose $k = 1$. Then $\sigma(\zeta) = \zeta$ and thus $\sigma(\zeta^i) = \sigma(\zeta) \cdots \sigma(\zeta)$ (i times) $= \zeta^i$ which is the identity permutation.

c) This is true because since p is prime, kx, for some $k \in 1, \dots, p-1$ multiplied by all values in $1, \dots, p-1$ gives a unique permutation.

d) We observe that $|G(\mathbb{Q}(\zeta)/\mathbb{Q})| = n - 1$ as $\sigma(\zeta)$ has $n-1$ possible values and the value of $\sigma(\zeta)$ determines σ as $\sigma(\zeta^i) = \sigma^i(\zeta)$. Let σ^k be the isomorphism that sends ζ to ζ^k. Let $\phi : G(\mathbb{Q}(\zeta)/\mathbb{Q}) \to \mathbb{Z}_p^*$, $\phi(\sigma^k) = k$. Let us show that this is an isomorhpism. For $k, \ell \in \mathbb{Z}$, $\phi(\sigma^\ell \circ \sigma^k) = \phi(\sigma^{k\ell}) = \phi(\sigma^{k\ell \ mod \ p}) = kl \ mod \ p = \phi(\sigma^k) \cdot \phi(\sigma^\ell)$. Also, as we showed in part c k can take values $1, \dots, n-1$ which are exactly those elements in $\mathbb{Z}_p^*$ so it is onto and since the groups have same order it is one-to-one. Thus the groups are isomorphic.

Problem 6

a) The extensions are determined to where $\sqrt{2}$ gets mapped. Since $\sqrt{2}$ is a root of the irreducible polynomial $x^2 - 2$, we can either map $\sqrt{2}$ to $\sqrt{2}$ or $-\sqrt{2}$ and this determines the extension.

b) If in the lower extesnsion, $\sqrt{2} \to \sqrt{2}$, then $\sqrt{2+\sqrt{2}} \to \pm\sqrt{2+\sqrt{2}}$. Otherwise, $\sqrt{2+\sqrt{2}} \to \pm\sqrt{2-\sqrt{2}}$.

c)

d)

Problem 7

a) This induces an isomorphism $\bar{\sigma}\,(a_nx^n + \cdots + a_0) = \sigma(a_n)x^n + \cdots + \sigma(a_0)$. Let us prove that this is an isomorphism. Take $a_nx^n + \cdots + a_0, b_mx^m + \cdots + b_0$ and wlog let $n \geq m$.

$$\bar{\sigma}(a_nx^n + \cdots + (a_m + b_m)x^m + \cdots + (a_0 + b_0)) = \sigma(a_n)x^n + \cdots + \sigma(a_m + b_m)x^m + \cdots + \sigma(a_0 + b_0)$$

Since σ is an isomorphism:

$$\bar{\sigma}(a_nx^n + \cdots + (a_m + b_m)x^m + \cdots + (a_0 + b_0)) = \sigma(a_n)x^n + \cdots + \sigma(a_m)x^m + \sigma(b_m)x^m + \cdots + \sigma(a_0) + \sigma(b_0)$$

$= \sigma(a_n)x^n + \cdots + \sigma(a_m)x^m + \cdots + \sigma(a_0) + \sigma(b_m)x^m + \cdots + \sigma(b_0) = \bar{\sigma}(a_nx^n + \cdots + a_0) + \bar{\sigma}(b_mx^m + \cdots + b_0)$

Also:

$$\bar{\sigma}((a_nx^n + \cdots + a_0)(b_mx^m + \cdots + b_0)) = \sigma(a_nb_mx^{m+n}) + \cdots + \sigma(a_0b_0)$$

$$= \sigma(a_n)\sigma(b_m)x^{m+n}) + \cdots + \sigma(a_0)\sigma(b_0) = \bar{\sigma}(a_nx^n + \cdots + a_0)\bar{\sigma}(b_mx^m + \cdots + b_0)$$

The map is onto as for any polynomial $a_nx^n + \cdots + a_0 \in L[x]$ there exists a polynomial $f(x) = \sigma^{-1}(a_n)x^n + \cdots + \sigma^{-1}(a_0) \in K[x]$ such that $\bar{\sigma}(f(x)) = a_nx^n + \cdots + a_0$. Also, suppose that $\bar{\sigma}(a_nx^n + \cdots + a_0) = \bar{\sigma}(b_mx^m + \cdots + b_0)$ Then:

$$\sigma(a_n)x^n + \cdots + \sigma(a_0) = \sigma(b_m)x^m + \cdots + \sigma(b_m)$$

and thus we can conclude that $n = m$ and $b_i = a_i$ for $a \in \{0, 1, \ldots, m\}$. So it is an isomorphism.

b) Let $f(x)$ be an irreducible polynomial in K. Suppose that $\bar{\sigma}(f(x))$ is reducible, i.e. $\bar{\sigma}(f(x)) = g(x)h(x)$, $g(x), h(x) \in L[x], deg(g(x)), deg(h(x)) < deg(\bar{\sigma}(f(x)))$. But then:

$$f(x) = \bar{\sigma}^{-1}(\bar{\sigma}(f(x))) = \bar{\sigma}^{-1}(g(x)h(x)) = \bar{\sigma}^{-1}(g(x))\bar{\sigma}^{-1}(h(x))$$

and since the isomorphism preserves the degree of polynomials we have shown that $f(x)$ is reducible in $K[x]$ which is a contradiction. The other direction is trivial, if $f(x) \in K[x]$ reduces to $g(x)h(x)$ then $\bar{\sigma}(f(x))$ clearly reduces to $\bar{\sigma}(g(x))\bar{\sigma}(h(x))$.

c) We observe that for the diagram to be commutative, for $x \in K$, $\tau(x) = \sigma(x)$. This inspires the following isomorphism. Given a simple field extension $K(\alpha)$, we have that every $y \in K(\alpha)$ can be uniquely written as $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ where $n = deg(irr(\alpha, K))$ and $a_i \in K$. We claim that for any root β of the polynomial $\bar{\sigma}(f(x))$, $L(\beta)$ is isomorphic to $K(\alpha)$ under

$$\tau(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{n-1})\beta^{n-1}$$

This isomorphism holds because

$$K(\alpha) \cong K[x]/f(x) \cong \bar{\sigma}(L[x]/f(x)) = L[x]/irr(\beta, L) \cong L(\beta)$$

and isomorphism is transitive.