Modern Algebra II: Problem Set 12

Nilay Kumar

Last updated: April 27, 2013

Problem 1

Consider the field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, with $\omega = (-1 + \sqrt{-3})/2$. We have seen that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$.

(i) Let $\rho \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ be the unique element such that $\rho(\omega) = \omega$ and $\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. It's clear that the fixed field $\mathbb{Q}(\sqrt[3]{2}, \omega)^\rho$ should be $\mathbb{Q}(\omega)$, as anything with a $\sqrt[3]{2}$ is not fixed. To prove this, note that anything in $\mathbb{Q}(\omega)$ is fixed by ρ, and thus, $\mathbb{Q}(\omega) \leq \mathbb{Q}(\sqrt[3]{2}, \omega)^\rho$. Additionally, by look at the degrees of the extensions, we see that

$$3 = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2}, \omega)^\rho][\mathbb{Q}(\sqrt[3]{2}, \omega)^\rho : \mathbb{Q}(\omega)]$$

which tells us that one of the factors is 3 and the other is 1. Note, however, that the first cannot be 1, as $\sqrt[3]{2}$ is not fixed, and thus we see that $[\mathbb{Q}(\sqrt[3]{2}, \omega)^\rho : \mathbb{Q}(\omega)] = 1$, i.e. $\mathbb{Q}(\omega)$ is the fixed field.

(ii) Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ be complex conjugation. It's clear that $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2}, \omega)^\sigma$, as the subfield consists only of real numbers. Again by counting degrees, we have

$$2 = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2}, \omega)^\sigma][\mathbb{Q}(\sqrt[3]{2}, \omega)^\sigma : \mathbb{Q}(\sqrt[3]{2})]$$

and since ω cannot be in the fixed field, it follows that $[\mathbb{Q}(\sqrt[3]{2}, \omega)^\sigma : \mathbb{Q}(\sqrt[3]{2})] = 1$ and thus $\mathbb{Q}(\sqrt[3]{2})$ is the fixed field.

(iii) For the subgroup $H_1 = \langle(12)\rangle$ of S_3, we find that $H_1(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $H_1(\omega\sqrt[3]{2}) = \sqrt[3]{2}$. Note that this permutation fixes $\omega^2\sqrt[3]{2}$, and thus $\mathbb{Q}(\omega^2\sqrt[3]{2})$ must be contained in the fixed field.

The subgroup $H_2 = \langle(13)\rangle$ of S_3 fixes $\omega\sqrt[3]{2}$. Thus $\mathbb{Q}(\omega\sqrt[3]{2})$ must be contained in the fixed field.

Problem 2

Consider the field $\mathbb{Q}(\sqrt[4]{2}, i)$. We have seen that $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ has order 8.

(i) Suppose that $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ corresponds to the permutation $(13)(24)$. Thus $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$, $\sigma(-\sqrt[4]{2}) = \sqrt[4]{2}$, $\sigma(i\sqrt[4]{2}) = -i\sqrt[4]{2}$, $\sigma(-i\sqrt[4]{2}) = i\sqrt[4]{2}$. This yields:

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

and

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

Consequently, we know that $\mathbb{Q}(\sqrt{2}, i)$ is contained in the fixed field. Counting degrees,

$$2 = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt{2}, i)] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2}, i)^{\sigma}][\mathbb{Q}(\sqrt[4]{2}, i)^{\sigma} : \mathbb{Q}(\sqrt{2}, i)]$$

and by the argument that the first term cannot be 1 (as $\sqrt[4]{2}$ is not fixed) we find that the fixed field $\mathbb{Q}(\sqrt[4]{2}, i)^{\sigma} = \mathbb{Q}(\sqrt{2}, i)$.

(ii) Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ be complex conjugation, i.e. the permutation (24). It's clear that $\mathbb{Q}(\sqrt[4]{2})$ is contained in the fixed field, as it contains no complex numbers. We now count degrees:

$$2 = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2}, i)^{\tau}][\mathbb{Q}(\sqrt[4]{2}, i)^{\tau} : \mathbb{Q}(\sqrt[4]{2})]$$

and since the first term cannot be one, we must have that the fixed field $\mathbb{Q}(\sqrt[4]{2}, i)^{\tau} = \mathbb{Q}(\sqrt[4]{2})$.

(iii) Let $\rho \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ correspond to the permutation (13), i.e. switches $\pm\sqrt[4]{2}$. It's clear that $\mathbb{Q}(i\sqrt[4]{2})$ is contained in the fixed field for this permutation. We can count degrees:

$$2 = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt[4]{2})] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2}, i)^{\rho}][\mathbb{Q}(\sqrt[4]{2}, i)^{\rho} : \mathbb{Q}(i\sqrt[4]{2})]$$

and since the first term cannot be 1, because $\sqrt[4]{2}$ is not fixed. Thus we must have the fixed field $\mathbb{Q}(\sqrt[4]{2}, i)^{\rho} = \mathbb{Q}(i\sqrt[4]{2})$. (Note that the overall extension was degree 2 because, writing out the bases, we can conclude that $\mathbb{Q}(i\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}, i)$.

(iv) Now consider the subgroup $H = \langle(1234)\rangle$. This permutation takes

$$\begin{aligned} H(\sqrt[4]{2}) &= i\sqrt[4]{2} \\ H(i\sqrt[4]{2}) &= -\sqrt[4]{2} \\ H(-\sqrt[4]{2}) &= -i\sqrt[4]{2} \\ H(-i\sqrt[4]{2}) &= \sqrt[4]{2}. \end{aligned}$$

We can compute what the permutation does to i:

$$H(i) = H(i\sqrt[4]{2}/\sqrt[4]{2}) = -\sqrt[4]{2}/i\sqrt[4]{2} = -1/i = i.$$

Thus $\mathbb{Q}(i)$ must be contained in the fixed field.

Problem 3

Let F be a field of characteristic zero and let $n \in \mathbb{N}$.

(i) Let $f(x) = x^n - 1$. We can compute the derivative $Df(x) = nx^{n-1}$. Since f is characteristic zero, Df is nonzero. These are relatively prime, as we can write

$$-1(x^n - 1) + x/n(nx^{n-1}) = 1$$

and thus f does not have a multiple root in any extension field.

(ii) Let E be a splitting field for $x^n - 1$ over F. By definition of a splitting field, $x^n - 1$ must factor completely into linear factors, and since the polynomial has no multiple roots (in any extension field), it must factor into n distinct roots (by the fundamental theorem of algebra), the n^{th} roots of unity. We can show that the roots of $x^n - 1$ form a finite subgroup of F. First note that if α, β are roots, then $\alpha^n\beta^n - 1 = \beta^n(\alpha^n - 1) + \beta^n - 1 = 0$ and thus $\alpha\beta$ is also a root. Furthermore, it is clear that 1 is a root that serves as identity and the inverse is simply α^{-1}, which is a root, as $\alpha^{-n} - 1 = (1 - \alpha^n)/\alpha^n = 0$ ($\alpha \neq 0$ as 0 is not a root). Note, however, that any finite subgroup of a field is cyclic, and thus the roots of unity form a cyclic group. If ζ is any primitive n^{th} root of unity, it's clear that $F(\zeta)$ will contain all powers of ζ, and thus every element can be written as $a_0 + a_1\zeta + \ldots + a_{n-1}\zeta^{n-1}$, $a_i \in F$. Note, however, that the powers of ζ are the roots of $x^n - 1$, and since E is the splitting field for $x^n - 1$ over F we know that $E = F(\zeta, \zeta^2, \ldots, \zeta^{n-1})$ and thus $E = F(\zeta)$.

(iii) E is clearly a normal extension of F, as $f(x) = x^n - 1 \in F[x]$ is a polynomial of degree at least 1 such that E is a splitting field of $f(x)$ over F. Let $\sigma \in \mathrm{Gal}(E/F)$. Then $\sigma(\zeta)$ must be a root of $x^n - 1$ as well, and thus $\sigma(\zeta) = \zeta^i$ for some i. Note that if $d = \gcd(i, n)$, then we must have that $(\zeta^i)^{n/d} = 1^{i/d} = 1$. This implies that ζ^i is a root of $x^{n/d} - 1$, and so is ζ (obtained by σ^{-1} since homomorphisms preserver order). Note, however, that ζ has order n and since $n/d \leq n$, we must have $d = 1$, i.e. i is relatively prime to n.

Hence, if we define $\phi : \mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^*$ by $\sigma(\zeta) = \zeta^{\phi(\sigma)}$ where $\phi(\sigma)$ is well-defined (as above). ϕ is clearly a homomorphism:

$$\sigma(\rho(\zeta)) = \sigma(\zeta^{\phi(\rho)}) = \sigma(\zeta)^{\phi(\rho)} = \zeta^{\phi(\sigma)\phi(\rho)}$$

Note that this is injective because if $f(\sigma) = 1$, then $\sigma(\zeta) = \zeta$ and we have the identity permutation, and the kernel is simply the identity.

(iv) First note that the degree of the extension $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $\deg \Phi_p = p - 1$. Note that $\mathbb{Q}(\zeta_p)$ is a separable extension as Φ_p does not have multiple roots. Furthermore, $\mathbb{Q}(\zeta_p)$ is normal extension as well, because $\mathbb{Q}(\zeta_p)$ is clearly a splitting field for Φ_p over $\mathbb{Q}$. Then, by the theorem proven in class, the order of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is exactly $p - 1$. But from the last part, we have an injective homomorphism from the Galois group to $(\mathbb{Z}/p\mathbb{Z})^*$. However, this homomorphism must be surjective as well, as both groups are of the same order; hence, we have an isomorphism.