Math 121 Homework 8 Solutions

- Section 14.6 # 1, 2, 3, 4, 40bc, 44
- **Optional**: Section 14.6 # 49

Problem 1 in 14.6. Show that a cubic with a multiple root has a linear factor. That is, if $f \in F[x]$ is cubic and has a multiple root in an extension field, then it has a linear factor in $F[x]$. Assume that the characteristic is not 3. Is the same true for quartics?

Solution. The key insight is that it does not matter whether we take the greatest common divisor of f and f' in $F[x]$ or in $E[x]$. We will digress to discuss this point.

We remind the reader that although the notion of greatest common divisor is useful for unique factorization domains, it is particularly simple over principal ideal domains.

If R is a principal ideal domain and $f, g \in R$, then the greatest common divisor of f and g may be characterized as a generator δ of the ideal $I = Rf + Rg$. It has the property that δ divides both f and g, and that δ can be written as $\delta = mf + ng$, $m, n \in R$.

Lemma 1. *Let $R \subseteq S$ be principal ideal domains and let $f, g \in R$. Let δ be the greatest common divisor of f and g as an element of R. Then δ is also the greatest common divisor of f and g as an element of S.*

Proof. We have δ dividing f and g (in R) and $\delta = mf + ng$ for $m, n \in R$. These facts remain true in S, so δ is the greatest common divisor of f and g as an element of S. □

Now we may finish the proof. Let h be the greatest common divisor of f and f' in $F[x]$. Because f has a multiple root, the degree of h is at least 1. But it is at most 2 since f' has degree 2. Therefore h is a polynomial in $F[x]$ of degree 1 or 2 that divides f. Thus either h or f/h is linear, proving that f has a linear factor.

We are asked whether the statement remains true when f is quartic. The answer is no. For example, we could take $f(x) = g(x)^2$, where $g(x)$ is an irreducible quadratic. This has two multiple roots in the splitting field, namely the roots of $g(x)$. But $f(x)$ has no linear factors.

Problem 2 in 14.6. Determine the Galois groups of the following polynomials:

(a) $x^3 - x^2 - 4$

(b) $x^3 - 2x + 4$

(c) $x^3 - x + 1$

(d) $x^3 + x^2 - 2x - 1$.

Solution. We recall that the discriminant of $f(x) = x^3 + bx + c$ is $-(27c^2 + 4b^3)$.

(a) This polynomial is reducible, since $x = 2$ is a root. We factor it as $(x-2)(x^2+x+2)$. The quadratic here is irreducible over $\mathbb{Q}$ since the discriminant -7 is not a square. So in this case the Galois group is S_2.

(b): This one is also reducible since $x = -2$ is a root. We factor it as $(x+2)(x^2-2x+2)$. The quadratic has discriminant -4, which is not a square (since it is negative). The Galois group is S_2, generated by complex conjugation.

(c): If the polynomial x^3-x+1 were reducible over $\mathbb{Q}$ it would be reducible over $\mathbb{Z}$ by Gauss' Lemma, hence reducible over $\mathbb{F}_p$ for every prime p. But it is irreducible over $\mathbb{F}_2$ where it is cubic but has no root. So it is irreducible. The discriminant is -23. This is negative, so the Galois group is S_3.

(d): You may remember this as the irreducible polynomial satisfied by $\zeta_7 + \zeta_7^{-1} = 2\cos\left(\frac{2\pi}{7}\right)$. So it generates the unique cubic subfield inside $\mathbb{Q}(\zeta)$, which is abelian over $\mathbb{Q}$. So the Galois group is cyclic, Z_3. Alternatively, let us compute the discriminant. Making the change of variables $x \mapsto x - \frac{1}{3}$ gives the polynomial $x^3 - \frac{7}{3}x - \frac{7}{27}$ so the discriminant is

$$-27\left(-\frac{7}{27}\right)^2 - 4\left(-\frac{7}{3}\right)^3 = 49.$$

Since $49 = 7^2$ this is a square over $\mathbb{Q}$, so the Galois group is Z_3. If you know some algebraic number theory, the 7 will tell you to look for it inside the cyclotomic field of 7-th roots of unity.

Problem 3 in 14.6. Prove that for any $a, b \in \mathbb{F}_{p^n}$ if x^3+ax+b is irreducible then $-4a^3-27b^2$ is a square in $\mathbb{F}_{p^n}$.

Solution. We will write $q = p^n$. Let α, β, γ be the roots of $f(x) = x^3 + ax + b$. Because f is assumed to be irreducible, these lie in the unique cubic extension field $E = \mathbb{F}_{q^3}$. Therefore $r = (\alpha-\beta)(\alpha-\beta)(\beta-\gamma) \in E$. The square r^2 is the discriminant $D(f)$, which is in $F = \mathbb{F}_q$. Since $r^2 \in F$, r lies in the unique quadratic extension of F. But this field is not contained in E. Both fields $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$ are contained in $\mathbb{F}_{q^6}$, so we can take their intersection, but this intersection is just $\mathbb{F}_q$. Since $r \in \mathbb{F}_{q^3} \cap \mathbb{F}_{q^2} = \mathbb{F}_q$, we see that $D(f) = r^2$ is a square in $\mathbb{F}_q$.

Problem 4 in 14.6. Determine the Galois group of $x^4 - 25$ over $\mathbb{Q}$.

Solution. This polynomial is reducible over $\mathbb{Q}$:

$$x^4 - 25 = (x^2 - 5)(x^3 + 5).$$

So the roots are $\pm\sqrt{5}$ and $\pm\sqrt{5}i$. Clearly the splitting field is $\mathbb{Q}\left(\sqrt{5}, i\right)$. It has degree 4 over $\mathbb{Q}$ and every automorphism sends $\sqrt{5}$ to $\pm\sqrt{5}$ and i to $\pm i$, so the Galois group is $Z_2 \times Z_2$.

Problem 40bc. Express the following polynomials as polynomials in the elementary symmetric functions. In three variables these are

$$e_1 = x_1 + x_2 + x_3, \qquad e_2 = x_1x_2 + x_1x_3 + x_2x_3, \qquad e_3 = x_1x_2x_3.$$

Note: The book tells you to use a particular procedure, but I don't require you to do this. Also, the book uses the notations s_i for the elementary symmetric functions, but the notation e_i is **standard** in the mathematical literature since at least the 1980's.

(b) $x_1^2 + x_2^2 + x_3^2$.

(c) $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$.

Solution. (b) We have

$$e_1^2 = x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3 = x_1^2 + x_2^2 + x_3^2 + 2e_2$$

so $x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2$.

(c) We have

$$e_2^2 = x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2x_1^2x_2x_3 + 2x_2^2x_1x_3 + 2x_3^2x_1x_2 = x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2e_1e_3$$

so

$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = e_2^2 - 2e_1e_3.$$

Problem 44 in 14.6. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of a quartic polynomial $f(x)$ over $\mathbb{Q}$. Show that the quantities $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$ and $\alpha_1\alpha_4 + \alpha_2\alpha_3$ are permuted by the Galois group of $f(x)$. Conclude that these elements are the roots of a cubic polynomial with coefficients in $\mathbb{Q}$ (sometimes called the *cubic resolvent* of $f(x)$).

Solution. If $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, where E is the splitting field of f, then $\sigma(\alpha_1), \sigma(\alpha_2), \sigma(\alpha_3)$ and $\sigma(\alpha_4)$ are $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in some order, and it is therefore clear that $\sigma(\alpha_1\alpha_2 + \alpha_2\alpha_3) = \sigma(\alpha_1)\sigma(\alpha_2) + \sigma(\alpha_3)\sigma(\alpha_4)$ is one of $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ and $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$, and so forth. Since σ permutes β_1, β_2 and β_3, the symmetric functions in β_1, β_2 and β_3 are invariant under σ. In particular, σ fixes a, b, c where

$$x^3 + ax^2 + bx + c = (x - \beta_1)(x - \beta_2)(x - \beta_3), \tag{1}$$

so

$$a = -(\beta_1 + \beta_2 + \beta_3), \qquad b = \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1, \qquad c = \beta_1\beta_2\beta_3.$$

Thus a, b, c are in $\mathbb{Q}$, and the cubic resolvent (1) is in $\mathbb{Q}[x]$.

Problem 49 in 14.6 (Optional: this will not be graded). Prove that the Galois group over $\mathbb{Q}$ of $x^6 - 4x^3 + 1$ is isomorphic to the dihedral group of order 12. (**Hint:** Observe that the two real roots are inverses of each other.)

Solution. We will prove that $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3 \times Z_2$, where E is the splitting field of $f(x) = x^6 - 4x^3 + 1$. Then we will point out that $D_{12} \cong S_3 \times Z_2$.

If α is a root of this, then α^3 is a root of $x^2 - 4x + 1$, that is, $\alpha^3 = 2 \pm \sqrt{3}$. Hence the splitting field E contains $\sqrt{3}$. Over the subfield $\mathbb{Q}\left(\sqrt{3}\right)$, we may factor the polynomial

$$x^6 - 4x^3 + 1 = \left(x^3 - 2 - \sqrt{3}\right)\left(x^3 - 2 + \sqrt{3}\right).$$

Note that $2 + \sqrt{3}$ and $2 - \sqrt{3}$ are inverses, so α^{-1} is a root of $x^3 - 2 + \sqrt{3}$. Therefore we may completely factor the polynomial

$$x^6 - 4x^3 + 1 = (x - \alpha)(x - \rho\alpha)(x - \rho^2\alpha)(x - \alpha^{-1})(x - (\rho\alpha)^{-1})(x - (\rho^2\alpha)^{-1}).$$

It is clear that the splitting field $E = \mathbb{Q}(\alpha, \rho)$ where $\rho = e^{2\pi i/3}$, and since $\mathbb{Q}(\rho) = \mathbb{Q}\left(\sqrt{-3}\right)$, E contains the biquadratic field $\mathbb{Q}\left(\sqrt{3}, \sqrt{-3}\right)$.

Since the polynomial $x^3 - 2 - \sqrt{3}$ has imaginary roots, its discriminant is negative, and so it is irreducible over $\mathbb{Q}\left(\sqrt{3}\right) \subseteq \mathbb{R}$, with Galois group S_3. This proves that $\mathrm{Gal}\left(E/\mathbb{Q}\left(\sqrt{3}\right)\right)$ contains Galois automorphisms corresponding to all permutations of the roots $\alpha, \rho\alpha, \rho^2\alpha$ of $x^3 - 2 - \sqrt{3}$. Given such a permutation, the effect on the other roots $\alpha^{-1}, (\rho\alpha)^{-1}$ and $(\rho^2\alpha)^{-1}$ is determined. So $\mathrm{Gal}\left(E/\mathbb{Q}\left(\sqrt{3}\right)\right)$ is a subgroup isomorphic to S_3.

To obtain other elements of $\mathrm{Gal}(E/\mathbb{Q})$, let us extend the automorphism $\sqrt{3} \longrightarrow -\sqrt{3}$ of $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}\right)$ to an automorphism θ of $\mathrm{Gal}(E/\mathbb{Q})$. We have some flexibility in this extension, since we may compose with an arbitrary element of $\mathrm{Gal}\left(E/\mathbb{Q}\left(\sqrt{3}\right)\right)$, and so we may arrange that $\theta(\alpha) = \alpha^{-1}$, $\theta(\rho\alpha) = (\rho\alpha)^{-1}$ and $\theta(\rho^2\alpha) = (\rho^2\alpha)^{-1}$. In other words, $\theta(\gamma) = \gamma^{-1}$ for every root γ of f.

Now let $\sigma \in \mathrm{Gal}\left(E/\mathbb{Q}\left(\sqrt{3}\right)\right)$. We show that $\sigma\theta = \theta\sigma$. Indeed, if γ is one the roots of f then $\sigma\theta(\gamma) = \sigma(\gamma^{-1}) = \sigma(\gamma)^{-1} = \theta\sigma(\gamma)$. We see that $\theta^2 = 1$ and that it commutes with $\mathrm{Gal}\left(E/\mathbb{Q}\left(\sqrt{3}\right)\right) \cong S_3$. Since $\mathrm{Gal}\left(E/\mathbb{Q}\left(\sqrt{3}\right)\right)$ is obviously the union of S_3 and the coset θS_3, it is clear that $\mathrm{Gal}\left(E/\mathbb{Q}\left(\sqrt{3}\right)\right) \cong S_3 \times Z_2$.

We have found the Galois group, but it remains to be shown that this group is dihedral. The group S_3 is already dihedral of order 6, so let σ be a 3-cycle and τ a transposition. In terms of generators and relations

$$S_3 = \langle \sigma, \tau | \sigma^3 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle,$$

$$S_3 \times Z_2 = \langle \sigma, \tau, \theta | \sigma^3 = \tau^2 = \theta^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1}, \sigma\theta = \theta\sigma, \tau\theta = \theta\tau \rangle.$$

Now let $\rho = \sigma\theta$. Then ρ has order 6, and $\sigma = \rho^4$, $\theta = \rho^3$ are both in the cyclic group $\langle\rho\rangle$. In other words $\langle\rho\rangle \cong Z_3 \times Z_2 \cong \langle\sigma, \theta\rangle$. We also have $\tau\rho\tau^{-1} = \rho^{-1}$, so

$$\langle \sigma, \tau, \theta | \sigma^3 = \tau^2 = \theta^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1}, \sigma\theta = \theta\sigma, \tau\theta = \theta\tau \rangle = \langle \rho, \tau | \rho^6 = \tau^2 = 1, \tau\rho\tau^{-1} = \rho^{-1} \rangle.$$

This proves that $S_3 \times Z_2 \cong D_{12}$.