Problem set 10.

1. Find the Galois group of $x^4 + 8x + 12$ over $\mathbb{Q}$.

Solution. The resolvent cubic $x^3 - 48x + 64$ does not have rational roots. The discriminant $-27 \times 8^4 + 256 \times 12^3 = 27 (2^{14} - 2^{12}) = 81 \times 2^{12}$ is a perfect square. Therefore the Galois group is $A_4$.

2. Find the Galois group of $x^4 + 3x + 3$ over $\mathbb{Q}$.

Solution. The resolvent cubic is $x^3 - 12x + 9 = (x - 3) (x^2 + 3x - 3)$. The discriminant $D = -27 \times 3^4 + 256 \times 3^3 = 27 (256 - 81) = 3^3 \sqrt{21}$. Therefore the Galois group is $D_4$ or $D_4$.

Now let us check that $x^4 + 3x + 3$ is irreducible over $\mathbb{Q}$. $\sqrt{D} = \mathbb{Q}(\sqrt{21})$. First, $x^4 + 3x + 3$ is not a product of linear and irreducible cubic polynomial, since 3 does not divide the order of the Galois group. Assume

$$x^4 + 3x + 3 = (x^2 + ax + b) (x^2 - ax + c),$$

then

$$-a^2 + b + c = 0, a (c - b) = 0, bc = 3.$$ 

If $a = 0, b = -c$, and $-c^2 = 3$ is impossible in real field. If $b = c$, then $b = \sqrt{3} \notin \mathbb{Q}(\sqrt{21})$. Thus, the Galois group is $D_4$.

3. Find the Galois group of $x^6 - 3x^2 + 1$ over $\mathbb{Q}$.

Solution. Let $y = x^2$. Then $y$ is a root of $y^3 - 3y + 1$, whose Galois group is $Z_3$. Consider three roots $\alpha_1, \alpha_2$ and $\alpha_3$ of $y^3 - 3y + 1$. Then

$$\pm \sqrt[3]{\alpha_1}, \pm \sqrt[3]{\alpha_2}, \pm \sqrt[3]{\alpha_3}$$

are the roots of $x^6 - 3x^2 + 1$. Now note that $\alpha_1, \alpha_2, \alpha_3$ are real, their sum is zero and their product is $-1$. Therefore, without loss of generality we may assume that $\alpha_1, \alpha_2 > 0, \alpha_3 < 0$. Hence $\mathbb{Q}(\sqrt[3]{\alpha_1})$ and $\mathbb{Q}(\sqrt[3]{\alpha_1}, \sqrt[3]{\alpha_2})$ are not splitting fields, but

$$F = \mathbb{Q}(\sqrt[3]{\alpha_1}, \sqrt[3]{\alpha_2}, \sqrt[3]{\alpha_3})$$

is a splitting field, and $(F/\mathbb{Q}) = 24$. The Galois group $G$ has order 24 and is a subgroup of $S_6$. Consider the subgroup $G'$ of all permutations of six roots such that $s(-\beta) = -s(\beta)$ for any root $\beta$. One can see that $G'$ has 24 elements and is generated by a 3-cycle $s$

$$s(\sqrt[3]{\alpha_1}) = \sqrt[3]{\alpha_2}, s(\sqrt[3]{\alpha_2}) = \sqrt[3]{\alpha_3}, s(\sqrt[3]{\alpha_3}) = \sqrt[3]{\alpha_1},$$

Date: May 13, 2006.
and the transpositions \( t_1, t_2, t_3 \) such that
\[
   t_i (\sqrt[n]{\alpha_i}) = -\sqrt[n]{\alpha_i}.
\]
Obviously, \( G \subset G' \), and since \(|G| = |G'|\), \( G = G' \). One can prove that \( G \) is isomorphic to \( A_4 \times \mathbb{Z}_2 \).

4. Assume that the polynomial \( x^4 + ax^2 + b \in \mathbb{Q}[x] \) is irreducible. Prove that its Galois group is the Klein subgroup if \( \sqrt{b} \in \mathbb{Q} \), the cyclic group of order 4 if \( \sqrt{a^2 - 4b} \sqrt{b} \in \mathbb{Q} \), and \( D_4 \) otherwise.

Solution. From the previous homework we already know that the possible Galois groups are \( K_4 \), \( Z_4 \) or \( D_4 \). The roots are \( \alpha, \beta, -\alpha, -\beta \) satisfy the following relations:
\[
   \alpha \beta = \sqrt{b}, \alpha^2 - \beta^2 = \sqrt{a^2 - 4b}, \alpha^3 \beta - \beta \alpha^3 = \sqrt{b} \sqrt{a^2 - 4b}.
\]
If \( \sqrt{b} \in \mathbb{Q} \), then \( \alpha \beta \in \mathbb{Q} \). Let \( s \in G \) be such that \( s(\alpha) = \beta \), then \( s(\beta) = \frac{\sqrt{b}}{s(\alpha)} = \alpha \). Similarly, if \( s(\alpha) = -\beta \), then \( s(-\beta) = \alpha \). Finally, if \( s(\alpha) = -\alpha \), then \( s(\beta) = -\beta \). Thus, every element of the Galois group has order 2. That implies that the Galois group is the Klein group.

Now assume that \( \sqrt{b} \sqrt{a^2 - 4b} \in \mathbb{Q} \). Then \( \alpha^3 \beta - \beta \alpha^3 \in \mathbb{Q} \).

Let \( s \) be an element of the Galois groups which maps \( \alpha \) to \( \beta \). If \( s(\beta) = \alpha \), then
\[
   s (\alpha^3 \beta - \beta^3 \alpha) = \beta^3 \alpha - \alpha \beta^3.
\]
This is impossible. Therefore \( s(\beta) = -\alpha \). Thus, \( s \) must have order 4, which implies that the Galois group is \( Z_4 \).

Finally note that the splitting field must contain \( \mathbb{Q}(\sqrt{b}), \mathbb{Q}(\sqrt{a^2 - b}) \) and \( \mathbb{Q}(\sqrt{b} \sqrt{a^2 - 4b}) \).

The irreducibility of the polynomial implies that \( \sqrt{a^2 - 4b} \) is not rational. Therefore if \( \sqrt{b}, \sqrt{a^2 - 4b} \sqrt{b} \notin \mathbb{Q} \), the splitting field contains at least at least three subfields of degree 2. Hence the Galois group is either \( K_4 \) or \( D_4 \). However, if the group is \( K_4 \), then \( \alpha \beta \) is fixed by any element of the Galois group. Since \( \sqrt{b} \) is not rational, the only possibility is \( D_4 \).

5. Let \( f(x) \) be an irreducible polynomial of degree 5. List all (up to an isomorphism) subgroups of \( S_5 \) which can be the Galois group of \( f(x) \). For each group \( G \) in your list give an example of an irreducible polynomial of degree 5, whose Galois group is \( G \).

Solution. \( G \) must contains a 5 cycle, because 5 divides the order of \( G \). Recall also that that if \( G \) contains a transposition, then \( G = S_5 \). Assume first that 3 divides \( |G| \). Any group of order 15 is cyclic, therefore \( S_5 \) does not contain a subgroup of order 15. If \( |G| = 30 \), then \( G \) is not a subgroup of \( A_5 \) (indeed it would be normal in \( A_5 \) but \( A_5 \) is simple). But then \( |G \cap A_5| = 15 \), which is impossible as we already proved. Therefore, if 3 divides \( |G| \), then \( G = A_5 \) or \( S_5 \). Assume now that 3 does not divide \( |G| \). Note first, that \( |G| \neq 40 \), because if \( |G| = 40 \), then \( G \) contains \( D_4 \), hence \( G \) contains a transposition which is impossible. If \( |G| = 5 \), then \( G \) is isomorphic to \( \mathbb{Z}_5 \). If \( |G| = 10 \), then \( G \) is isomorphic to \( D_5 \), since \( S_5 \) does not contains a cyclic
group of order 10. Finally, \(|G|=20\), then \(G\) contains is a semidirect product of a normal subgroup of order 5 and a subgroup of order 4. It is not difficult to see that a subgroup of order 4 is cyclic and \(G\) is isomorphic to \(Fr_5\).

Thus, the possible Galois groups are \(\mathbb{Z}_5, D_5, Fr_5, A_5\) or \(S_5\). To get a polynomial with a given Galois group \(G\), start for example with

\[
f(x) = x^5 - 6x + 3,
\]

it is irreducible by Eisenstein criterion and has exactly two complex roots. Hence its Galois group over \(\mathbb{Q}\) is \(S_5\). Denote by \(F\) a splitting field for \(f(x)\). Let \(G\) be any subgroup of \(S_5\), then the Galois group of \(f(x)\) over \(F^G\) is \(G\). Since \(G\) acts transitively on the roots of \(f(x)\), \(f(x)\) is irreducible over \(F^G\).

6. Let \(G\) be an arbitrary finite group. Show that there is a field \(F\) and a polynomial \(f(x)\) such that the Galois group of \(f(x)\) is isomorphic to \(G\).

Solution. Any group \(G\) is a subgroup of a permutation group \(S_n\). There exists a field \(F\) and a polynomial \(f(x)\) (for example general polynomial) with Galois group \(S_n\). Let \(E\) be the splitting field of \(f(x)\) and \(B = E^G\). Then \(G\) is the Galois group of \(F(x)\) over \(B\).

Problem set 11.

1. Let \(E\) and \(B\) be normal extensions of \(F\) and \(E \cap B = F\). Prove that

\[
\text{Aut}_F EB \cong \text{Aut}_F E \times \text{Aut}_F B.
\]

Solution. \(\text{Aut}_E EB\) and \(\text{Aut}_B EB\) are normal subgroups in \(\text{Aut}_F EB\). It is obvious that

\[
\text{Aut}_E EB \cap \text{Aut}_B EB = \{1\}.
\]

By the theorem of natural irrationalities the restriction maps

\[
\text{Aut}_E EB \to \text{Aut}_F B, \text{Aut}_B EB \to \text{Aut}_F E
\]

are isomorphisms. Therefore

\[
|\text{Aut}_F EB| = |\text{Aut}_F B||\text{Aut}_B EB| = |\text{Aut}_E EB||\text{Aut}_B EB|,
\]

hence

\[
\text{Aut}_F EB = \text{Aut}_E EB \text{Aut}_B EB,
\]

that implies

\[
\text{Aut}_F EB \cong \text{Aut}_E EB \times \text{Aut}_B EB \cong \text{Aut}_F E \times \text{Aut}_F B.
\]

2. Find the Galois group of the polynomial \(x^3 - 3\) \((x^3 - 2)\) over \(\mathbb{Q}\).

Solution. Let \(\omega\) be a primitive \(3 - d\) root of 1,

\[
F = \mathbb{Q}(\omega), E = F(\sqrt[3]{2}), B = F(\sqrt[3]{3}).
\]

Then by the previous problem \(H = \text{Aut}_F EB \cong \mathbb{Z}_3 \times \mathbb{Z}_3\). \(H\) is a subgroup of index 2 in the Galois group \(\text{Aut}_F EB\). The complex conjugation \(\sigma\) generates a subgroup of order 2 in \(G\). Thus \(G\) is a semisdirect product of \(< \sigma >\) and \(H, |G| = 18\). \(G\) is the subgroup of \(S_6\) generated by \((123),(456)\) and \((23)(45)\).
3. Let \( f(x) \) be an irreducible polynomial of degree 7 solvable in radicals. List all possible Galois groups for \( f(x) \).

Solution. Those are subgroups of \( Fr_7 \) which contain \( \mathbb{Z}_7 \). There are four such subgroups: \( \mathbb{Z}_7, D_7 \), a semidirect product of \( \mathbb{Z}_3 \) and \( \mathbb{Z}_7 \) and \( Fr_7 \).

4. Find the Galois group of \( x^6 - 4x^3 + 1 \) over \( \mathbb{Q} \).

Solution. Let \( \alpha = 2 + \sqrt[3]{3} \) be a root of \( x^2 - 4x + 1 \), \( \beta \) be a root of \( x^3 - \alpha \), \( \omega \) be a primitive 3\textsuperscript{-}d root of 1. Note that \( \frac{1}{\alpha} \) is also a root of \( x^2 - 4x + 1 \). Therefore all roots of \( x^6 - 4x^3 + 1 \) are \( \beta_1 = \beta, \beta_2 = \beta \omega, \beta_3 = \beta \omega^2, \beta_4 = \frac{1}{\beta}, \beta_5 = \frac{\omega}{\beta}, \beta_6 = \frac{\omega^2}{\beta} \).

Hence \( F = \mathbb{Q}(\beta, \omega) \) is the splitting field, \( (F/\mathbb{Q}) = 12 \), therefore the order of the Galois group is 12. The subfield \( \mathbb{Q}(\alpha, \omega) \) corresponds to the normal subgroup of order 3 generated by the permutation \((123)(456)\); the complex conjugation is represented by the permutation \((23)(45)\). These two permutations generate the subgroup isomorphic to \( S_3 \). To obtain the whole Galois group add the permutation \((14)(25)(36)\) which sends any root to its inverse. Thus, the Galois group is isomorphic to the direct product of \( S_3 \) and \( \mathbb{Z}_2 \).

5. Let \( f(x) = g(x) h(x) \) be a product of two irreducible polynomials over a finite field \( \mathbb{F}_q \). Let \( m \) be the degree of \( g(x) \) and \( n \) be the degree of \( h(x) \). Show that the degree of the splitting field of \( f(x) \) over \( \mathbb{F}_q \) is equal to the least common multiple of \( m \) and \( n \).

Solution. \( \mathbb{F}_{q^m} \) is the splitting field for \( g(x) \), \( \mathbb{F}_{q^n} \) is the splitting field for \( h(x) \). The minimal field which contains \( \mathbb{F}_{q^m} \) and \( \mathbb{F}_{q^n} \) is the splitting field of \( f(x) \). \( \mathbb{F}_{q^l} \) contains \( \mathbb{F}_{q^m} \) and \( \mathbb{F}_{q^n} \) if and only if \( m \) and \( n \) divide \( l \). The minimal \( l \) is the least common multiple of \( m \) and \( n \).

6. Let \( F \subset E \) be a normal extension with Galois group isomorphic to \( \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \). Assuming that \( \text{char} F \neq 2 \), prove that

\[
E = F \left( \sqrt{b_1}, \ldots, \sqrt{b_s} \right)
\]

for some \( b_1, \ldots, b_s \in F \).

Solution. We prove it by induction on the number of \( \mathbb{Z}_2 \)-components. The base of induction was done in some previous homework. Now we write \( G = H \times \mathbb{Z}_2 \). Let \( B = E^{2a_2} \), then \( \text{Aut}_F B = H \), and therefore by induction assumption \( E = F \left( \sqrt{b_1}, \ldots, \sqrt{b_{a-1}} \right) \). Let \( K = E^H \), then \( (K/F) = 2 \), hence \( K = F(\sqrt{b_a}) \). Since \( E = BK \), we are done.

7. Prove that the splitting field of the polynomial \( x^4 + 3x^2 + 1 \) over \( \mathbb{Q} \) is isomorphic to \( \mathbb{Q}(i, \sqrt{5}) \).

Solution. One can check that the Galois group of this polynomial is \( K_4 \) by Problem 4 in Homework 10. Hence the splitting field must be generated by two square roots (see the previous problem). Let
\[ \alpha_1 = \sqrt{-3 + \sqrt{5}} \quad \frac{2}{2}, \quad \alpha_2 = \sqrt{-3 - \sqrt{5}} \].

Then \( \sqrt{5} = \alpha_1^2 - \alpha_2^2 \) is in the splitting field.

\[ (\alpha_1 + \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 = -1 \]

Therefore \( \alpha_1 + \alpha_2 = \pm i \) is in the splitting field.

Problem set # 12

1. Trisect the angle of 18° by ruler and compass.

   **Solution.** Construct the angle of 30° on the side of a given angle. The difference
   is 12°, construct the symmetric angle inside the given angle and bisect it.

2. Let \( l \) be the least common multiple of \( m \) and \( n \). Assume that regular \( m \)-gon
   and regular \( n \)-gon are constructible by ruler and compass. Prove that regular \( l \)-gon
   is also constructible by ruler and compass.

   **Solution.** Let \( d \) be the greatest common divisor of \( m \) and \( n \). One can find
   integers \( u \) and \( v \) such that \( nu + mv = d \). Since the angles \( \frac{2\pi}{m} \) and \( \frac{2\pi}{n} \) are constructible,
   one can construct

   \[ \frac{2\pi}{m} u + \frac{2\pi}{n} v = \frac{2\pi}{mn} = \frac{2\pi}{l} \]

3. Find the minimal equation over for \( \cos \frac{2\pi}{7} \) over \( \mathbb{Q} \). Hint: express \( \cos \frac{2\pi}{7} \) in terms
   of 7-th roots of 1.

   **Solution.** Let \( \omega \) denote the 7-th roots of 1. Use

   \[ \cos \frac{2\pi}{7} = \frac{\omega + \omega^{-1}}{2} \]

   The answer:

   \[ x^3 + \frac{x^2}{2} - \frac{x}{2} - \frac{1}{8} \]

4.

   (a) Prove that the angle of 25° is not constructible by ruler and compass;
   (b) Prove that angle of \( n \)° is constructible by ruler and compass if and only if \( n \) is
   a multiple of 3.

   **Solution.** First, let us construct the angle of 3°. Since a regular pentagon is
   constructible, one can construct the angle of 108°. Then by subtracting the right
   angle we get 18°. Trisecting it will give 6°. Finally we can get 3° by bisecting 6°.
   Then, clearly we can construct any multiple of 3°. Assume that 3 does not divide \( n \).
   Then \( n = 3k + 1 \) or \( 3k + 2 \). But the angles of 1° and 2° are not constructible because
   if we can construct one of them, we can get 20°. Thus, \( n \)° is not constructible.
5. Given three segments \(a, b,\) and \(c\), construct a triangle whose altitudes equal \(a, b,\) and \(c\).

**Solution.** Construct a triangle with sides \(\frac{1}{a}, \frac{1}{b}, \frac{1}{c}\). The required triangle is similar to this one.

6. Let \(f(x)\) be an irreducible polynomial over \(\mathbb{Q}\) of degree 7. Assume that \(f(x)\) has exactly three real roots. Prove that \(f(x)\) is not solvable in radicals.

**Solution.** Assume that \(f(x)\) is solvable in radicals. Then the Galois group is a subgroup of Frobenius group. Enumerate the roots of \(f(x)\) by the elements of \(\mathbb{Z}_7\). Then the Galois group acts on them by linear functions \(s(t) = at + b\). But the number of elements \(t \in \mathbb{Z}_7\) such that \(s(t) = t\) is 0, 1 or 7 (when \(s\) is the identity. However, the Galois group contains a complex conjugation, which fixes exactly 3 roots. Contradiction.

**Problem set #12**

1. Prove that the Galois group of \(f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1\) over \(\mathbb{Q}\) is cyclic of order 5. Hint: let \(\omega\) be the 11-th root of 1. Prove that \(f(x)\) is the minimal polynomial for \(\omega + \omega^{-1}\).

**Solution.** I skip the calculation of the minimal polynomial because it is straightforward. The Galois group of \(\mathbb{Q}(\omega)\) is \(\mathbb{Z}_{10}\), \(\mathbb{Q}(\omega + \omega^{-1})\) is fixed by the subgroup \(\mathbb{Z}_2\). Therefore the Galois group of \(\mathbb{Q}(\omega + \omega^{-1})\) is \(\mathbb{Z}_{10}/\mathbb{Z}_2 = \mathbb{Z}_5\).

2. Let \(p\) be an odd prime, \(\omega\) be a primitive \(p\)-th root of 1.
   (a) Prove that \(\mathbb{Q}(\omega)\) contains exactly one quadratic extension of \(\mathbb{Q}\); 
   (b) If \(p = 4k + 1\), then this quadratic extension is isomorphic to \(\mathbb{Q}(\sqrt{p})\);
   (c) If \(p = 4k + 3\), then this quadratic extension is isomorphic to \(\mathbb{Q}(\sqrt{-p})\).

**Solution.** For (a) just note that the Galois group of \(\mathbb{Q}(\omega)\) is \(\mathbb{Z}_{p-1}\), and therefore it has exactly one subgroup of index 2. Let \(b\) be a generator of this index 2 subgroup. Let

\[
\alpha = \omega + \omega^b + \omega^{b^2} + \ldots, \quad \beta = \omega^c + \omega^{bc} + \omega^{b^2c} + \ldots,
\]

where \(c\) is chosen so that \(\omega^c\) does not appear in the expression for \(\alpha\). One can see that \(\alpha + \beta = -1\).

If \(p = 4k + 1\), then \(\omega^{-1}\) appears in the expression for \(\alpha\). One can check that in this case \(\alpha\beta = -\frac{p-1}{4}\). Therefore \(\alpha\) is a root of \(x^2 + x - \frac{p-1}{4}\). The discriminant of this equation is \(p\), hence \(\sqrt{-p} \in \mathbb{Q}(\omega)\).

If \(p = 4k + 3\), then \(\omega^{-1}\) appears in the expression for \(\beta\). One can check that in this case \(\alpha\beta = \frac{p+1}{4}\). Therefore \(\alpha\) is a root of \(x^2 + x + \frac{p+1}{4}\). The discriminant of this equation is \(-p\), hence \(\sqrt{-p} \in \mathbb{Q}(\omega)\).

3. Find the Galois group of \(x^4 + 2x^3 + x + 3\) over \(\mathbb{Q}\) using reduction modulo 2 and 3.

**Solution.** The polynomial is irreducible modulo 2 and splits as \(x(x^3 + 2x + 1)\) modulo 3. Hence the Galois group contains a 3-cycle and a 4-cycle. Therefore the Galois group is \(S_4\).
4. Give an example of a polynomial of degree 6 whose Galois group over $\mathbb{Q}$ is $S_6$.

**Solution.** It suffices to find an irreducible $f(x)$ whose Galois group contains a 5-cycle and a transposition. Let $f(x) = x^6 + 40x^5 + 34x^2 + 16x + 70$. Then $f(x)$ is irreducible by Eisenstein criterion for $p = 2$. Modulo 5 $f(x) = x^6 - x^2 + x = x(x^5 - x + 1)$. Check that $x^5 - x + 1$ is irreducible modulo 5. Finally, modulo 7 we have $f(x) = x^6 - 2x^5 - x^2 + 2x = x(x - 1)(x + 1)(x - 2)(x^2 + 1)$. Thus, the Galois group of $f(x)$ is $S_6$. 