HOMEWORK 12

Due date: Week 13

Exercises: 9.18, 10.2, 10.3, 10.6(b), 10.7, 10.8, 10.9, 11.5, 12.3, 12.7, M.10, M.11, pages 509-512

For a solution of Ex 12.3, see this link. The assertion of M.9 is false, see this link for a counterexample.

Problem 1. *Solve the following polynomial equations with radicals. The coefficients are in* $\mathbb{Q}$.

$$f = x^3 + 7x + 1,$$
$$g = x^4 + 2x^3 + 3x^2 + x + 1.$$

Problem 2. *Repeat the proof of Galois criterion. In other words, let* F *be a field with characteristic* 0 *and let* $f \in F[x]$. *Show that* f *is solvable by radicals if and only if* G_f *is solvable.*

You can use the lemma we proved in classes. This is Exercise M.12, page 512.

Let $f \in F[x]$ be an irreducible polynomial of degree 5. It is known that G_f is a transitive subgroup of S_5. We classified transitive subgroups of S_4 in last class. Transitive subgroups of S_5 can also be classified, which are given by (up to conjugation)

(1) C_5: generated by (12345);
(2) D_{10}: generated by (12345) and (25)(34);
(3) $(\mathbb{Z}/5) \rtimes (\mathbb{Z}/5)^\times$: generated by (12345) and (2354);
(4) A_5;
(5) S_5.

Note that $(\mathbb{Z}/5) \rtimes (\mathbb{Z}/5)^\times$ has a unique group structure because there is a unique nontrivial group homomorphism $(\mathbb{Z}/5)^\times \to \mathrm{Aut}(\mathbb{Z}/5)$ up to conjugation. See HW12 of Linear Algbera II. We know that $|(\mathbb{Z}/5) \rtimes (\mathbb{Z}/5)^\times| = 20$. Moreover, the transitive subgroups of A_5 are C_5, D_{10} and A_5 itself.

See this link for the above classification. This is also Exercise 12.2, page 510.

We have seen in class that there exists an irreducible polynomial $f \in \mathbb{Q}[x]$ such that $G_f \cong S_5$.

Problem 3. (1) *Consider the polynomial* $f = x^5 - 2 \in \mathbb{Q}[x]$. *Show that* $G_f \cong (\mathbb{Z}/5) \rtimes (\mathbb{Z}/5)^\times$.

(2) *Let* $\zeta_{11} = \exp\left(\frac{2\pi\sqrt{-1}}{11}\right)$. *Let* $\alpha = \zeta_{11} + \zeta_{11}^{-1}$. *Find the minimal polynomial* f *of* α *over* $\mathbb{Q}$ *and show that* $G_f \cong C_5$.

This should be easy by counting degree.

Problem 4 $(*)$**.** *Consider the polynomial* $f = x^5 + ax + b$ *with* $a \geq 0$. *Show that* f *has at least one complex root. Moreover, if* f *is irreducible, show that* G_f *cannot be* C_5.

Hint: for the first part, use calculus. For the second part, notice that the complex conjugation is in the Galois group.

It is complicate to determine exactly what the Galois group of an irreducible quintic polynomial is. See this article for more details.

1. A Theorem of Dedekind on Galois groups

Let $\psi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ be the mod p map for a prime p.

Theorem 1.1 (Dedekind)**.** *Let* $f \in \mathbb{Z}[x]$ *be an irreducible polynomial with degree* $n \geq 1$. *Let* p *be a prime such that*

$$\psi_p(f) = g_1 \dots g_k$$

*with $g_1, \dots, g_k \in \mathbb{F}_p[x]$ irreducible and **distinct**. Assume $\deg(g_i) = n_i$ so that $n = n_1 + \cdots + n_k$. Then G_f (as a subgroup of S_n) contains an element with cycle length $n_1, n_2, \dots, n_k$. In other words, G_f contains an element of the form*

$$(i_1 i_2 \dots i_{n_1})(i_{n_1+1} \dots i_{n_1+n_2}) \dots .$$

The proof of this theorem is not easy. We assume it in the following. If you want a proof, see page 145 of this link.

The following is one example of how we apply the above theorem.

Problem 5. *Consider $f = x^5 - x - 1 \in \mathbb{Z}[x]$.*

1. *Show that $\psi_3(f)$ is irreducible and conclude that f itself is irreducible.*
2. *Show that G_f contains a cycle of order 5.*
3. *Factorize $\psi_2(f)$ and show that G_f contains a transposition using the above Dedekind's theorem.*
4. *Conclude that $G_f \cong S_5$.*

For part (3), we cannot get a transposition directly using Dedekind's theorem. But certain power would suffice.

The following is a special case of the above theorem.

Proposition 1.2. *Let α be an algebraic integer such that $K := \mathbb{Q}(\alpha)$ is a Galois extension. Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α. If there exists a prime integer p such that $\psi_p(f)$ is irreducible, then $\mathrm{Gal}(K/F) = G_f$ is cyclic.*

Note that, the relation between α and K in the above is: α is a primitive element of K. In particular, $[K : \mathbb{Q}] = \deg(f)$.

Problem 6. *Show that Theorem 1.1 implies Proposition 1.2.*

Problem 7. *Consider the polynomial $f = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$. Show that for any prime p, $\psi_p(f)$ is reducible. Moreover, $\psi_p(f)$ cannot have a degree 3 irreducible factor.*

This is M.4 page 476 of Artin's book. Do this problem using Proposition 1.2.

Problem 8. *Consider the polynomial $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Z}[x]$. Show that f is irreducible and $\psi_p(f)$ is reducible for any prime p.*

Hint: Consider the splitting field of $x^3 - 2$ and the element $\alpha + \omega$, where $\alpha = \sqrt[3]{2}, \omega = e^{2\pi i/3}$. Moreover, try to factorize $\psi_p(f)$ for some small p, like $p = 2, 3, 5, 7$. As a comparison, for example, for the polynomial $g = x^6 + 2x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Z}[x]$, $\psi_p(g)$ is indeed irreducible for $p = 23, 73, 79$ as you may check. The reason for it is that a single root of g does not generate the splitting field of g. In fact, $G_g \cong S_6$. Thus $[Spl(g, \mathbb{Q}) : \mathbb{Q}] = 72$, and $Spl(g, \mathbb{Q})$ cannot be generated by a single root of a polynomial of degree 6.

Warning: in Proposition 1.2, it is necessary to assume that the element α is primitive. Otherwise, the conclusion is false. For example, for $f = x^5 - x - 1$ in Problem 8, we know that $\psi_3(f)$ is irreducible. But this does not mean G_f is cyclic because f is not the minimal polynomial of some primitive element of $K = Spl(f, \mathbb{Q})$. Actually, any single root of f won't generate K. This, of course, just means that $[K : \mathbb{Q}] > 5$.

Problem 9 $(*)$**.** *Construct another irreducible polynomial $h \in \mathbb{Z}[x]$ of degree 6 such that $\psi_p(h) \in \mathbb{F}_p[x]$ is reducible for any prime p.*

2. Quadratic reciprocity law

Let p be an odd prime. Let $\mathbb{F}_p^{\times,2} = \{x^2 : x \in \mathbb{F}_p^\times\}$. For any $x \in \mathbb{F}_p^\times$, we define

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{if } x \in \mathbb{F}_p^{\times,2}, \\ -1, & \text{if } x \in \mathbb{F}_p^\times - \mathbb{F}_p^{\times,2}. \end{cases}$$

For any $a \in \mathbb{Z}$, if $(a, p) = 1$, we define

$$\left(\frac{a}{p}\right) := \left(\frac{\overline{a}}{p}\right),$$

where $\overline{a}$ is the image of a under the natural map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Problem 10. *Consider the map $\chi_p : \mathbb{F}_p^\times \to \mathbb{C}^\times$ defined by*

$$\chi_p(x) = \left(\frac{x}{p}\right).$$

Show that χ_p is a nontrivial quadratic character. Show that $\mathbb{F}_p^{\times,2}$ is the unique subgroup of $\mathbb{F}_p^\times$ of index 2. Moreover, if $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is a nontrivial quadratic character (χ is non-trivial means there exists on $x \in \mathbb{F}_p^\times$ such that $\chi(x) \neq 1$), show that $\chi = \chi_p$.

Here are some terminologies used in the last problem. A character $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is just a group homorphism (namely, $\chi(ab) = \chi(a)\chi(b)$). A character is called quadratic if $\chi(x)^2 = 1$ for any $x \in \mathbb{F}_p^\times$.

Theorem 2.1 (Quadratic reciprocity law)**.** *Let p, q be two distinct odd primes. Then*

(1) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
(2) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;
(3) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

We proved the above (1) and (3) in class. We recall the proof of (3) in the following. Denote $\zeta_p = e^{2\pi\sqrt{-1}/p}$. Recall that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^\times,$$

and the isomorphism is given as follows. For $k \in \mathbb{F}_p^\times$, define $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ by $\sigma_k(\zeta_p) = \zeta_p^k$. Then the isomorphism is given by $\sigma_k \mapsto k$. It is indeed well-defined and is an isomorphism. Moreover, consider

$$S = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\zeta_p^a.$$

This is called a Gauss sum. We computed that $S^2 = \left(\frac{-1}{p}\right)p$. Consider the field $L = \mathbb{Q}(S)$. Since $S^2 \in \mathbb{Q}$, we know that $[L : \mathbb{Q}] \leq 2$. But $S \notin \mathbb{Q}$ and thus $[L : \mathbb{Q}] = 2$. Moreover, we have $S \in \mathbb{Q}(\zeta_p)$ by definition. Thus we have the tower fields

$$\mathbb{Q} \subset L = \mathbb{Q}(S) \subset K := \mathbb{Q}(\zeta_p).$$

Thus we have the exact sequence

$$1 \to \mathrm{Gal}(K/L) \to \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 1.$$

Denote the projection map $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ by π. Thus we have $[K : L] = \frac{p-1}{2}$ and $\mathrm{Gal}(K/L) \cong \mathbb{F}_p^{\times,2}$. Consider the element $\sigma_q \in \mathrm{Gal}(K/\mathbb{Q})$ defined by $\sigma_q(\zeta_p) = \zeta_p^q$. By the description of the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^\times$, we see that

$$q \in \mathbb{F}_p^{\times,2} \text{ iff } \sigma_q \in \mathrm{Gal}(K/L) \text{ iff } \sigma_q \in \mathrm{Ker}(\pi) \text{ iff } \sigma_q|_L = 1 \text{ iff } \sigma_q(S) = S.$$

This implies that $\sigma_q(S) = \left(\frac{q}{p}\right)S$. The above (3) follows from this equation easily. The proof of (2) is simpler. It is given in the following.

Problem 11. *Let $\zeta = e^{2\pi\sqrt{-1}/8}$ and $\tau = \zeta + \zeta^{-1}$.*

(1) *Show that $\tau^2 = 2$.*
(2) *Show that there exists an element $\alpha \in \mathbb{Z}[\zeta]$ such that $\tau^p - \left(\frac{2}{p}\right)\tau = p\alpha$.*
(3) *Show that there exists an element $\beta \in \mathbb{Z}[\zeta]$ such that $\tau^p - (\zeta^p + \zeta^{-p}) = p\beta$.*
(4) *If $p \equiv \pm 1 \bmod 8$, show that $\zeta^p + \zeta^{-p} = \tau$ and $\left(\frac{2}{p}\right) = 1$.*
(5) *If $p \equiv \pm 3 \bmod 8$, show that $\zeta^p + \zeta^{-p} = -\tau$ and $\left(\frac{2}{p}\right) = -1$.*

The last two parts are equivalent to $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Problem 12. *Let $p = 1093$, which is known to be a prime number. Determine whether 516 is in $\mathbb{F}_p^{\times,2}$ or not.*

Problem 13 (∗)**.** *Let x be an integer. Show that any prime divisor of $x^4 - x^2 + 1$ is congruent to 1 modulo 12.*

Hint: Use quadratic reciprocity law and the identities $(x^2 - 1)^2 = (x^4 - x^2 + 1) - x^2$ and $(2x^2 - 1)^2 = 4(x^4 - x^2 + 1) - 3$.

Problem 14. (1) *Determine all prime numbers p such that $3 \in \mathbb{F}_p^{\times,2}$.*

(2) *Determine all prime numbers p such that $7 \in \mathbb{F}_p^{\times,2}$.*