HOMEWORK #1
SOLUTIONS TO SELECTED PROBLEMS

Problem 1.2. (a) To compute $[\mathbb{C} : \mathbb{R}]$, note that $\mathbb{C} = \mathbb{R}(i)$ and i is a solution to the polynomial $x^2 + 1 \in \mathbb{R}[x]$. This polynomial is irreducible, otherwise it would have a linear factor hence a solution in $\mathbb{R}$, which is impossible. So by problem 5 we see that $[\mathbb{C} : \mathbb{R}] = [\mathbb{R}(i) : \mathbb{R}] = 2$.

(b) The field $\mathbb{Q}$ is countable. Hence any simple extension $\mathbb{Q}(\alpha)$ is also countable, but $\mathbb{R}$ is not countable.

To show that a simple extension of a countable field is also countable, note that such an extension is either isomorphic to a homomorphic image of the polynomial ring $F[x]$ (in the case of algebraic extension), or isomorphic to the field or rational functions $F(x)$ (in the case of transcendental extension). Since $F[x] \subset F(x)$ and $F(x)$ is countable, the claim follows.

(c) We use the definition of $K(\alpha)$ as the set of all elements of the form $f(\alpha)/g(\alpha)$ where $f, g \in K[x]$ and $g(\alpha) \neq 0$. Since this set is closed under additions, multiplications and taking inverses, it is a subfield of L. In fact, is it the *minimal* subfield of L containing K and α.

(d) Similar to (c).

(e) Suppose $p \in \mathbb{R}[x]$ is irreducible. Let $\alpha \in \mathbb{C}$ be a solution of $p(x) = 0$ (exists since $\mathbb{C}$ is algebraically closed). Then by problem 5, $[\mathbb{R}(\alpha) : \mathbb{R}] = \deg p$, but $\mathbb{R}(\alpha) \subseteq \mathbb{C}$, hence $[\mathbb{R}(\alpha) : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2$. We deduce that $\deg p \leq 2$.

Problem 1.3. To prove that the $\{l_{ij}\}$ are linearly independent over K, assume that there exist $a_{ij} \in K$ such that $\sum_{i,j} a_{ij} l_{ij} = 0$. Write this sum as

$$0 = \sum_{i,j} a_{ij}\alpha_i\beta_j = \sum_i \left(\sum_j a_{ij}\beta_j \right) \alpha_i$$

For each i, $\sum_j a_{ij}\beta_j \in F$, hence by the linear independence of the α_i over F we get that $\sum_j a_{ij}\beta_j = 0$ for all i. Now using the linear independence of the β_j over K, we get that $a_{ij} = 0$ for all i and j.

Problem 1.4. (a) It is enough to show that the polynomial $f(x) = x^3 - x^2 + x + 2$ is irreducible in $\mathbb{Q}[x]$, since by problem 5 it will follow that for any solution u of $f(x)$ we have $[\mathbb{Q}(u) : \mathbb{Q}] = \deg f = 3$, independent of u.

We prove the irreducibility of f in two steps, which are interesting in their own right.

Lemma. *Let F be a field and let $f \in F[x]$ be a polynomial of degree 2 or 3. Then f is irreducible if and only if it has no roots in F.*

Proof. If f has a root $a \in F$, f has $x - a$ as a factor (this is true for *any* polynomial), and cannot be irreducible. On the other hand, for any non-trivial factorization $f = gh$ in $F[x]$, the degree of (at least) one of the factors would be 1. Since any polynomial of degree 1 has a root in F, it would follow that f has a root in F. □

Lemma. *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. Suppose that $p/q \in \mathbb{Q}$ is a root of f, where p, q are relatively prime. Then:*

$$p \mid a_0 \quad \textit{and} \quad q \mid a_n$$

Proof. By assumption, $f(p/q) = 0$. Multiplying by q^n, we get

$$0 = a_0 q^n + a_1 q^{n-1} p + \ldots a_{n-1} q p^{n-1} + a_n p^n$$

Positive powers of p appear in all summands except for the left one, hence they are divisible by p. Since the total sum is 0, it follows that p divides also $a_0 q^n$. Since p, q are relatively prime, we get $p \mid a_0$. The other assertion is proved similarly. □

Now consider the polynomial $x^3 - x^2 + x + 2$ in $\mathbb{Q}[x]$. By the first lemma, to prove irreducibility it is enough to show that it has no roots in $\mathbb{Q}$. By the second lemma, the only possible roots p/q must have $p \mid 2$ and $q \mid 1$, so that $p \in \{1, -1, 2, -2\}$ and $q \in \{1, -1\}$. Since $-1, 1, 2, -2$ are not roots of f, it follows that f has no rational root and therefore is irreducible.

(c) If ζ is a primitive n-th root of unity, then all other n-th roots of unity are powers of ζ, because the powers of ζ are n distinct elements which are roots of unity, but on the other hand, the polynomial $x^n - 1$ has at most n solutions.

Therefore, for another primitive n-th root of unity ζ', we have $\zeta' \in \mathbb{Q}(\zeta)$, hence $\mathbb{Q}(\zeta') \subseteq \mathbb{Q}(\zeta)$. Interchanging roles gives $\mathbb{Q}(\zeta') = \mathbb{Q}(\zeta)$, so the field is independent on the particular choice of primitive n-th root.

(d) $[L_2 : \mathbb{Q}] = 1$, $[L_3 : \mathbb{Q}] = 2$, $[L_4 : \mathbb{Q}] = 2$.

To prove these, note that -1 is a primitive 2-th root of unity; i is a primitive 4-th root of unity solving the equation $x^2 + 1 = 0$ and $\omega = e^{2\pi i/3}$ is a primitive 3-th root of unity solving $x^2 + x + 1 = 0$. These polynomials of degree 2 are irreducible in $\mathbb{Q}[x]$ since they have no rational roots.

Problem 1.5. Let L/K be a field extension and let $\alpha \in L$ be any element. We can define a homomorphism of rings $\varphi_\alpha : K[x] \to L$ by setting $\varphi_\alpha(f) = f(\alpha) \in L$.

Let's consider the kernel $\ker \varphi_\alpha$, which is an ideal of $F[x]$. There are two possibilities:

1. $\ker \varphi_\alpha = (0)$. In this case α is called *transcendental* over K.
2. $\ker \varphi_\alpha \neq (0)$. In this case α is *algebraic* over K. We concentrate on this latter case.

Since $K[x]$ is a principal ideal domain, the ideal $\ker \varphi_\alpha$ is generated by one element, which could be scaled to be monic (upper coefficient is 1). Denote it by m_α, so that $\ker \varphi_\alpha = (m_\alpha)$.

I claim that m_α is irreducible in $K[x]$. Indeed, if m_α factorizes as $m_\alpha(x) = g(x)h(x)$, then applying φ_α, one would get $0 = m_\alpha(\alpha) = g(\alpha)h(\alpha)$, hence one of g, h, say g, is in $\ker \varphi_\alpha = (m_\alpha)$, so that both $g \mid m_\alpha$ and $m_\alpha \mid g$ and the factorization is trivial.

Now let's consider the image of φ_α. $\operatorname{Im}\varphi_\alpha \subset L$ is a sub-ring. By the isomorphism theorem

$$\operatorname{Im}\varphi_\alpha \simeq K[x]/\ker\varphi_\alpha = K[x]/(m_\alpha)$$

Since m_α is irreducible, the ideal (m_α) is maximal, hence the quotient $K[x]/(m_\alpha)$ is a field. It follows that $\operatorname{Im}\varphi_\alpha$ is a subfield of L.

Obviously, $K \subset \operatorname{Im}\varphi_\alpha$ (as the image of the constant polynomials of degree 0) and $\alpha \in \operatorname{Im}\varphi_\alpha$ (as the image of the polynomial x). On the other hand, any field containing K and α must contain the elements $f(\alpha) = \varphi_\alpha(f)$ for all $f \in K[x]$. It follows that $\operatorname{Im}\varphi_\alpha$ is the *minimal* subfield of L containing K and α, i.e. $\operatorname{Im}\varphi_\alpha = K(\alpha)$.

We conclude that $K(\alpha) \simeq K[x]/(m_\alpha)$. To compute $[K(\alpha) : K]$, it is enough to construct a basis of $K[x]/(m_\alpha)$ over K. Denote by $\bar{f}$ the image of $f \in K[x]$ in the quotient ring $K[x]/(m_\alpha)$. I claim that $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ is such a basis, where $n = \deg m_\alpha$. Hence $[K(\alpha) : K] = \deg m_\alpha$.

The elements are independent over K, since any dependency leads to a polynomial $g(x)$ of degree *less* than n whose image is 0, which is impossible unless $g = 0$. On the other hand, it is clear that the elements span $K[x]/(m_\alpha)$: any polynomial $f \in K[x]$ can be written as $f = qm_\alpha + r$ with $\deg r < n$, and then $\bar{f} = \bar{r}$ is a linear combination of $\bar{1}, \ldots, \bar{x}^{n-1}$.