MAT401 Polynomial Equations and Fields
Assignment 5

Due Wednesday August 3 at the beginning of the lecture

Please write your arguments neatly and clearly. Numbers in [ ] indicate how much a question or a part of it is worth. The assignment is out of 50. Throughout, the letters F, F', K and L denote fields.

1. [7] Determine if each statement is true or false. No explanation is necessary. (But make sure you know exactly why a given statement is true or false.)

We use the following notation: If α is algebraic over F, the minimal polynomial of α over F is denoted by $m_{\alpha,F}(x)$.

(a) Every subfield of $\mathbb{C}$ contains $\mathbb{Q}$.
(b) There are no ring homomorphisms $\mathbb{Q} \to \mathbb{Z}$.
(c) If F and F' are finite extensions of $\mathbb{Q}$ such that $[F : \mathbb{Q}] = [F' : \mathbb{Q}]$, then every ring homomorphism $F \to F'$ is actually an isomorphism.
(d) If F and F' are finite extensions of $\mathbb{Q}$ such that $[F : \mathbb{Q}] = [F' : \mathbb{Q}]$, then F and F' are isomorphic as rings.
(e) If $F \subset K$, $\alpha \in K$ is algebraic over F, and $f(x) \in F[x]$ is such that $f(\alpha) = 0$, then $m_{\alpha,F}(x) \mid f(x)$.
(f) If $F \subset K$, $\alpha \in K$ is a root of $f(x) \in F[x]$ of degree $n \geq 1$, then $[F(\alpha) : F] \leq n$.
(g) If $\mathbb{Q} \subset F \subset \mathbb{C}$ and $F/\mathbb{Q}$ is finite, then there is a polynomial $f(x) \in \mathbb{Q}[x]$ such that F is contained in the splitting field of $f(x)$ over $\mathbb{Q}$.
(h) If $F \subset K \subset L$, and $\alpha \in L$ is algebraic over F, then $m_{\alpha,F}(x) \mid m_{\alpha,K}(x)$ in $K[x]$.
(i) If $F \subset K \subset L$, and $\alpha \in L$ is algebraic over F, then $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$ in $K[x]$.
(j) The polynomial $x^8 + 6x^3 + 9x + 21$ has 8 distinct roots in $\mathbb{C}$.
(k) If $F \subset K$ and $\alpha \in K$ is such that α^3 is algebraic over F, then α is also algebraic over F.
(l) Every algebraic extension is finite.
(m) If $F \subset \mathbb{C}$, then every ring homomorphism $F \to \mathbb{C}$ fixes $\mathbb{Q}$.
(n) If $f(x) \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and has degree n, and $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ are the roots of $f(x)$, then every ring homomorphism $\varphi : \mathbb{C} \to \mathbb{C}$ restricts to an automorphism of $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$. (In other words, the statement is claiming that if $\varphi : \mathbb{C} \to \mathbb{C}$ is a ring homomorphism, then the association $z \mapsto \varphi(z)$ defines an isomorphism $\mathbb{Q}(\alpha_1, \cdots, \alpha_n) \to \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$.)

2. [6] (a) [2] Suppose K/F is a field extension, $\alpha \in K$ such that $\alpha^2 \in F$. Show that $[F(\alpha) : F]$ is either 1 or 2.
(b) [4] Suppose $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ are such that $\alpha_i^2 \in \mathbb{Q}$ for each i. Show that $\sqrt[5]{2} \notin \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$.

3. [12] Let us give a definition first. We say a finite extension K/F is *simple* if there is $\omega \in K$ such that $K = F(\omega)$. The goal of this question is to prove the following theorem: If $F \subset K \subset \mathbb{C}$ and K/F is finite, then K/F is simple.

(a) [1] Argue that to prove the theorem it suffices to prove the following: If $F \subset \mathbb{C}$ and $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ are algebraic over F, then $F(\alpha_1, \cdots, \alpha_n)$ is a simple extension of F.

(b) [9] On page 4 of this document, you can find a sketch of a proof of the statement given in Part (a), with several steps and justifications left to you. Fill in the "gaps". (You don't have to rewrite the full argument; just complete the gaps. If you decide to rewrite the completed argument, please clearly indicate where you address each gap.)

(c) [2] Let $K = \mathbb{Q}(\sqrt{2}, i)$. Following the method given in the proof of (b), find ω such that $K = \mathbb{Q}(\omega)$.

4. [6] Suppose $\varphi : R \to S$ is a ring isomorphism (i.e. a bijective ring homomorphism).

(a) [3] Show that $\varphi^{-1} : S \to R$ is also a ring isomorphism.

(b) [3] Show that R is an integral domain if and only if S is an integral domain

5. [8] Let L be the splitting field of $x^n - 3$ over $\mathbb{Q}$. Let $\zeta_n = e^{2\pi i/n}$ and $\alpha = \sqrt[n]{3}$.

(a) [2] Show that $L = \mathbb{Q}(\alpha, \zeta_n)$.

(b) [3] Suppose for the rest of the question that $n = p$ is prime. Find $[L : \mathbb{Q}]$.

(c) [3] Show that $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}(\alpha)$.

6. [11] Let us start with a definition. Given $F \subset K \subset \mathbb{C}$ with K/F finite, we say the extension K/F is *Galois* if it satisfies any (and hence all) of the equivalent conditions of Theorem 5 of the notes. If K/F is Galois, then we call the group $\mathrm{Aut}(K/F)$ the *Galois group* of K/F. It is constumary to use the notation $\mathrm{Gal}(K/F)$ for $\mathrm{Aut}(K/F)$ in this case. (So $\mathrm{Gal}(K/F)$ and $\mathrm{Aut}(K/F)$ are the same thing, except that we use the first notation only if K/F is a Galois extension.)

Below all fields are subfields of $\mathbb{C}$.

(a) [1] Let K be a Galois extension of F. Let $f(x) \in F[x]$ be an irreducible polynomial which has a root in K. Is it true that K contains all (complex) roots of $f(x)$? No explanation necessary.

(b) [4] Let K/F be Galois, and that $f(x) \in F[x]$ be a nonzero polynomial all whose complex roots are in K. Let $\alpha_1, \cdots, \alpha_n$ be all the distinct roots of $f(x)$, and for brevity denote the set $\{\alpha_1, \cdots, \alpha_n\}$ by $\mathrm{roots}(f(x))$. Let $\sigma \in \mathrm{Gal}(K/F)$. Show that there is a bijection

$$\mathrm{roots}(f(x)) \to \mathrm{roots}(f(x))$$

given by $\alpha_i \mapsto \sigma(\alpha_i)$. (In other words, show that σ permutes the roots of $f(x)$.) Denote the bijection above by $\sigma\,|_{\mathrm{roots}(f(x))}$, the *restriction of* σ *to the set of roots of* $f(x)$.

(c) [2] For any nonempty set X, denote the symmetric group on X by S_X. Recall that as a set S_X is the set of all bijections $X \to X$, and the group operation is composition of functions. Continuing with the notation as in (b), show that

$$\mathrm{Gal}(K/F) \to S_{\mathrm{roots}(f(x))} \qquad \sigma \mapsto \sigma\,|_{\mathrm{roots}(f(x))} \tag{1}$$

is a group homomorphism. (One may refer to this map as the restriction to the set of roots of $f(x)$.)

(d) [2] Now suppose moreover that K is the splitting field of $f(x)$ over F. Show that the map (1) above is injective.

We usually identify $\mathrm{Gal}(K/F)$ with its image under this injection, and think of an element of the Galois group as a permutation of the roots of $f(x)$.

(e) [1] Read the example on page 46 of the notes (done in class on Wednesday July 27). With the notation as in the example, identifying the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ with a subgroup of $S_{\{\alpha_1,\alpha_2,\alpha_3\}}$, is complex conjugation equal to the transposition $(\alpha_2\ \alpha_3)$?[†]

(f) [1] Agian in regards to the example on page 46 of the notes, show that $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.

[†]For any finite nonempty set X, the cycle notation in S_X is just like the case of $S_n = S_{\{1,\cdots,n\}}$. Here $(\alpha_2\ \alpha_3)$ refers to the element of $S_{\{\alpha_1,\alpha_2,\alpha_3\}}$ that sends $\alpha_2 \mapsto \alpha_3$, $\alpha_3 \mapsto \alpha_2$, and $\alpha_1 \mapsto \alpha_1$.

THEOREM 1. If $F \subset \mathbb{C}$ and $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ are algebraic over F, then $F(\alpha_1, \cdots, \alpha_n)/F$ is a simple extension.

PROOF. First note that the result certainly holds when $n = 1$: $F(\alpha_1)/F$ is finite (as α_1 is algebraic over F) and is clearly simple. Thus we need to prove the result for $n \geq 2$. We do this by induction on n. Let us assume the base case ($n = 2$) for the moment.

Gap 1: Carry out the induction. In other words, suppose the result holds for some $n \geq 2$, and prove it for $n + 1$. (Note that we are assuming the base case for now. You can use it.)

Now we turn our attention to the base case, i.e. when $n = 2$. Suppose $\alpha, \beta \in \mathbb{C}$ are algebraic over F. Our goal is to show that there is ω such that $F(\alpha, \beta) = F(\omega)$. Let $f(x)$ (resp. $g(x)$) be the minimal polynomial of α (resp. β) over F. Let $k = \deg(f(x))$ and $l = \deg(g(x))$. Let $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_k$ be the roots of $f(x)$ in $\mathbb{C}$, and $\beta_1 = \beta, \beta_2, \cdots, \beta_l$ be the roots of $g(x)$ in $\mathbb{C}$. Let $c \in F$ be an element that is not equal to any of the numbers

$$\frac{\alpha_i - \alpha}{\beta - \beta_j} \quad (1 \leq i \leq k, 2 \leq j \leq l).$$

Gap 2: How de we know such c exists?

Set $\omega = \alpha + c\beta$. We claim that $F(\alpha, \beta) = F(\omega)$.

Gap 3: Is $F(\omega) \subset F(\alpha, \beta)$? Why?

To establish the claim, we need to show that $F(\alpha, \beta) \subset F(\omega)$. For this it suffices to show $\alpha, \beta \in F(\omega)$. Define $h(x) := f(\omega - cx)$.

Gap 4: Is $h(x) \in (F(\omega))[x]$? Why?

Gap 5: Verify that β a root of $h(x)$.

Gap 6: Show that none of $\beta_2, \cdots, \beta_l$ can be a root of $h(x)$.

Let $g_1(x)$ be the minimal polynomial of β over $F(\omega)$. Note that in particular, $g_1(x) \in (F(\omega))[x]$.

Gap 7: Does it follow that $g_1(x) \mid g(x)$ and $g_1(x) \mid h(x)$? Why?

Gap 8: Argue that β is the only root of $g_1(x)$ (in $\mathbb{C}$).

Thus $g_1(x)$ is of the form $a(x - \beta)^r$ for some $r \geq 1$ and $a \in F(\omega)$. Since $g_1(x)$ is monic, $a = 1$, and $g_1(x) = (x - \beta)^r$. Since $g_1(x)$ is irreducible over $F(\omega)$, it cannot have any repeated roots. This $r = 1$ and $g_1(x) = x - \beta$.

Gap 9: Does it follows that $\beta \in F(\omega)$? Why?

Gap 10: Use $\beta \in F(\omega)$ and $\omega = \alpha + c\beta$ to conclude that $\alpha \in F(\omega)$ as well. This completes the proof of the theorem.

□

Practice Problems. The following problems are for your own practice. Please **do not** hand them in. Throughout F and K denote fields.

1. Suppose $\varphi : R \to S$ is a ring isomorphism. Let $a \in R$. Show that $a \in U(R)$ if and only if $\varphi(a) \in U(S)$.

2. Suppose R and S are isomorphic rings. Show that R is a field if and only if S is a field.

3. Let L be the splitting field of $x^3 + 9x + 3$ over $\mathbb{Q}$. Show that $[L : \mathbb{Q}] = 6$ and that $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.

4. Suppose $\varphi : R \to S$ is a ring isomorphism. Let $a \in R$. Show that a is irreducible in R if and only if $\varphi(a)$ is irreducible in S.

5. Suppose $\varphi : R \to S$ is a ring isomorphism. Let $I \subset R$ be an ideal. Show that I is a prime ideal if and only if $\varphi(I)$ is a prime ideal of S.

6. Suppose $F \subset K \subset \mathbb{C}$ and $[K : F] = 2$. Show that K/F is a Galois extension.

More practice problems to be posted.