Nepal Algebra Project 2016
SOLUTIONS of the midterm exam

Tribhuvan University

June 25^{th} 2016

1. (a) Find the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}$, and *prove* that it is the minimal polynomial.

(5 marks)

Answer. *If we start from the formal identity* $x = \sqrt{3}+\sqrt{5}$, *we deduce that* $(x-\sqrt{3})^2 = 5$. *Hence* $x^2-2 = 2\sqrt{3}x$. *Finally* $f(x) = (x^2-2)^2 - 12x^2 = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$ *has* $\sqrt{3}+\sqrt{5}$ *as one of its root. We check that* $\sqrt{5}$ *is not in* $\mathbb{Q}(\sqrt{3})$ *as follows: if* $\sqrt{5} = a + b\sqrt{3}$ *with* a *and* b *in* $\mathbb{Q}$, *then* $5 = a^2 + 3b^2 + 2ab\sqrt{3}$. *Since* $\sqrt{3}$ *is irrational, this implies* $ab = 0$ *and* $5 = a^2 + 3b^2$, *which is not possible because* 5 *and* 5/3 *are irrational. To conclude that* $f(x)$ *is the minimal polynomial, it is enough to observe (by next problem) that the degree of the minimal polynomial equals* $[\mathbb{Q}(\sqrt{3}+\sqrt{5}) : \mathbb{Q}] = 4$ *and since* $f(x)$ *is divisible by the minimal polynomial, it can only coincide with it.*

(b) Prove that $\mathbb{Q}(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$.

(5 marks)

Answer. *It is plain that* $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$. *To verify the opposite inclusion, it is enough to observe that* $\sqrt{3} = -\frac{7}{2}(\sqrt{3}+\sqrt{5}) + \frac{1}{4}(\sqrt{3}+\sqrt{5})^3$ *and* $\sqrt{5} = \frac{9}{2}(\sqrt{3}+\sqrt{5}) - \frac{1}{4}(\sqrt{3}+\sqrt{5})^3$.

2. Prove the theorem about transitivity of algebraic extensions: If $F \subseteq K \subseteq L$ are field extensions such that K is algebraic over F, and L is algebraic over K, then L is algebraic over F.

(10 marks)

Answer. *The solution can be found on the textbook in page 19, Corollary 1.31(b).*

3. Let F be a finite field with $\mathrm{char}(F) = p(>0)$. Show that $F = \{\text{roots of the equation } X^{p^n} - X = 0\}$, where $n = [F : \mathbb{F}_p]$. (*Hint.* We can use the fact that the multiplicative group $F^* = F - \{0\}$ of F has order $p^n - 1$.)

(10 marks)

Answer. *The field* F *contains* $\mathbb{F}_p$ *and is finite. So we may put* $n = [F : \mathbb{F}_p]$. *Hence* $\sharp(F) = p^n$. *Therefore,* F^* *is a multiplicative group of order* $p^n - 1$. *So, for any* $a \in F^*$, *it holds* $a^{p^n-1} - 1 = 0$. *Setting* $R = \{$*roots of the equation* $X^{p^n} - X = 0\}$, *we know* $a \in R$. *By counting* $0 \in F$, *we have* $F \subset R$. *According to the argument* (1.7), *the algebraic equation over a field has no more roots than its degree. So,* $\sharp R \leq p^n$. *It shows* $F = R$

4. Let F be a field of characteristic $p(>0)$. Suppose $a \in F$ is not a p-th power in F (i.e. We don't have $a = \alpha^p$ for any $\alpha \in F$). Show that $f(X) = X^p - a$ is irreducible in $F[X]$. (This is the fact of Example 2.11 stated without proof.)

(10 marks)

Answer. *Let us assume the contrary: that is* $f(X) \in F[X]$ *is reducible. Let us induce a contradiction. Now, we may set* $f(X) = g(X)h(X)$ *in* $F[X]$ *where* $g(X) \in F[X]$ *is irreducible and* $\deg(g) < \deg(f)$. *Let* α *be a root of* $g(X)$. *It is a root of* $f(X)$ *at the same time. So we have* $\alpha^p = a$. *Then it holds* $f(X) = X^p - a = X^p - \alpha^p = (X-\alpha)^p$. *Because* $g(X)|f(X)$, *we may put* $g(X) = (X-\alpha)^r$ *with* $1 \leq r < p$. *We have*

$$(X-\alpha)^r = X^r - r\alpha X^{p-1} + \cdots \in F[X].$$

It means $\alpha \in F$. *It contradicts our starting hypothesis.*

5. Let $\zeta = e^{2\pi i/5}$.

(a) Prove that $\mathbb{Q}[\zeta]$ is a Galois extension of $\mathbb{Q}$.

(2 marks)

Answer. *The number* ζ *is a root of* $f = X^4 + X^3 + X^2 + X + 1$*, as are* $\zeta^2, \zeta^3, \zeta^4$*. Thus* $\mathbb{Q}[\zeta]$ *is a splitting field for* f*, and* f *is separable (since, for instance* $\mathrm{char}(\mathbb{Q}) = 0$*), thus* $\mathbb{Q}[\zeta]$ *is a Galois extension of* $\mathbb{Q}$*.*

(b) Calculate $[\mathbb{Q}[\zeta] : \mathbb{Q}]$.

(2 marks)

Answer. *We claim that* $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 4$*. To see this, we need to calculate the minimum polynomial of* ζ *which, since* ζ *is a root of* $f = X^4 + X^3 + X^2 + X + 1$*, is a factor of* f*. But* f *is irreducible (either use Eisenstein, or use lemma from lectures, or some other method). Thus* f *is the minimum polynomial for* ζ*, and since the degree of* f *is* 4*, we are done.*

(c) What is the structure of the Galois group $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$?

(4 marks)

Answer. *Write* G *for the group in question, and notice that the elements of* G *can be thought of as permutations of the set* $\{\zeta, \zeta^2, \zeta^3, \zeta^4\}$*, since these are the roots of* f*.*

Furthermore, once we've specified the destination of the root ζ *we have determined an automorphism of* $\mathbb{Q}[\zeta]/\mathbb{Q}$*, and so determined the element of the Galois group. There are four elements in this group (by the previous two parts and the FTGT), four possible destinations for* ζ*, hence they all occur. Write*

$$\sigma_i : \zeta \mapsto \zeta^i$$

for $i = 1, \ldots, 4$*. Now observe that* σ_3 *has order* 4 *and we conclude that the group is cyclic,* C_4*.*

(d) Give an example of a field M such that $\mathbb{Q} \subset M \subset \mathbb{Q}[\zeta]$.

(2 marks)

Answer. *Let* $M = \mathbb{Q}(\zeta + \zeta^4)$*. This field is real, so is not* $\mathbb{Q}[\zeta]$*. On the other hand it is fixed by* σ_4*, hence is not* $\mathbb{Q}$*.*

6. (a) Prove that $X^n - 2$ is irreducible for all positive integers n.

(2 marks)

Answer. *This follows directly from Eisenstein's criterion.*

(b) Let $\omega = \sqrt[n]{2}$ for some positive integer n. Calculate

$$[\mathbb{Q}[\omega] : \mathbb{Q}].$$

(1 mark)

Answer. *The previous question implies that* $[\mathbb{Q}[\omega] : \mathbb{Q}] = n$*.*

(c) Prove that $\sqrt[n]{2}$ is a constructible number if and only if $n = 2^k$ for some positive integer k.

(7 marks)

Answer. *From lectures we know that* $\sqrt[n]{2}$ *is constructible if and only if it lies in a tower of quadratic extensions.*

In particular if $n \neq 2^k$*, then the degree of* $[\mathbb{Q}[\sqrt[n]{2}] : \mathbb{Q}]$ *has an odd factor, and so (by multiplicativity of degrees), cannot be a subfield of a tower of quadratic extensions, hence* $\sqrt[n]{2}$ *is not constructible.*

On the other hand if $n = 2^k$*. Then we have a tower of quadratic extensions:*

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}] \subset \cdots \subset \mathbb{Q}[\sqrt[n]{2}]$$

and we are done.