Quizzes for Math 402

QUIZ 1. a) Let K be a field. Let L be a field containing K. What does it mean that L/K is finite? What does it mean that $a \in L$ is algebraic over K?

b) Let a be a complex number which is algebraic of degree 17 over $\mathbb{Q}$.Prove that $\mathbb{Q}(a) = \mathbb{Q}(a^5 + 3a^2 - 5)$.

Solution: a) We say that L/K is finite if L, considered as a vector space over K, has finite dimension.

We call a **algebraic** over K if $f(a) = 0$ for some non-zero polynomial $f \in K[x]$.

b) We have $\mathbb{Q} \subseteq \mathbb{Q}(a^5 + 3a^2 - 5) \subseteq \mathbb{Q}(a)$. Since a has degree 17 over $\mathbb{Q}$, we have $[\mathbb{Q}(a) : \mathbb{Q}] = 17$. On the other hand,

$$[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(a^5 + 3a^2 - 5)][\mathbb{Q}(a^5 + 3a^2 - 5) : \mathbb{Q}].$$

Since 17 is a prime number, we must have either $[\mathbb{Q}(a) : \mathbb{Q}(a^5 + 3a^2 - 5)] = 1$ or $[\mathbb{Q}(a^5 + 3a^2 - 5) : \mathbb{Q}]$. In the former case, $\mathbb{Q}(a) = \mathbb{Q}(a^5 + 3a^2 - 5)$. The latter case is not possible, since it would mean that $\mathbb{Q}(a^5 + 3a^2 - 5) = \mathbb{Q}$, so $a^5 + 3a^2 - 5 = q$ is rational, i.e. a is a root of a degree 5 polynomial $x^5 + 3a^2 - 5 - q$ with rational coefficients, which contradicts the assumption that a is of degree 17.

QUIZ 2. a) Let K be a field. What does it mean that $a \in K$ is a primitive $n-$th root of 1?

b) Find the splitting field L of $x^3 - 3$ over $\mathbb{Q}$. What is $[L : \mathbb{Q}]$?

Solution: a) An element a of a field K is called a **primitive $n-$th root of 1** if $a^n = 1$ and $a^k \neq 1$ for $1 \leq k < n$. Equivelently, a primitive $n-$th root of unity is an element of order n in the multiplicative group $K^\times$.

b) The polynomial x^3-3 is irreducible over $\mathbb{Q}$ (since it has degree 3 and no rational roots). Its roots are $\sqrt[3]{3}$, $\rho\sqrt[3]{3}$ and $\rho^2\sqrt[3]{3}$, where ρ is a primitive 3−rd root of 1, i.e. a root of $x^2+x+1=0$. We see that

$$L=\mathbb{Q}(\sqrt[3]{3},\rho\sqrt[3]{3},\rho^2\sqrt[3]{3})=\mathbb{Q}(\sqrt[3]{3},\rho).$$

Note that $[\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}]=3$, since the minimal polynomial of $\sqrt[3]{3}$ over $\mathbb{Q}$ has degree 3. The number ρ is not real and $\mathbb{Q}(\sqrt[3]{3})$ consists of real numbers, so $\rho\notin\mathbb{Q}(\sqrt[3]{3})$. It follows that x^2+x+1 is the minimal polynomial of ρ over $\mathbb{Q}(\sqrt[3]{3})$ and therefore $[\mathbb{Q}(\sqrt[3]{3},\rho):\mathbb{Q}(\sqrt[3]{3})]=2$. Thus

$$[\mathbb{Q}(\sqrt[3]{3},\rho):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{3},\rho):\mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}]=2\cdot 3=6.$$

QUIZ 3. a) Compute the 12-th cyclotomic polynomial $\Phi_{12}(x)$.

b) Let L/K be finite and let $charK=p>0$. Show that if $p\nmid[L:K]$ then L/K is separable.

Solution: a) Recall that $x^n-1=\Pi_{d|n}\Phi_d(x)$. Thus

$$x^{12}-1=\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x).$$

On the other hand,

$$x^{12}-1=(x^6-1)(x^6+1)=\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)(x^6+1).$$

Comparing the above two equalities we see that

$$x^6+1=\Phi_4(x)\Phi_{12}(x).$$

Now $\Phi_4(x)=x^2+1$ so

$$\Phi_{12}(x)=(x^6+1)/(x^2+1)=x^4-x^2+1.$$

Another solution: Note first that $\Phi_6(x)=x^2-x+1$. If u is a primitive 12−th root of 1 then u^2 is a primitive 6−th root of 1 so $\Phi_6(u^2)=0$. It follows that every primitive 12−th root of 1 is a root of $\Phi_6(x^2)$, so $\Phi_{12}(x)|\Phi_6(x^2)$. But both polynomials are monic of degree 4 so $\Phi_{12}(x)=\Phi_6(x^2)=x^4-x^2+1$.

b) Suppose that $[L : K]$ is not separable. Then there is $a \in L$ which is not separable over K. Let f be the minimal polynomial of a over K. Since f is irreducible and not separable, we have $f(x) = g(x^p)$ for some $g \in K[x]$. In particular, p divides the degree of f, i.e. $p|[K(a) : K]$. Since $[K(a) : K]|[L : K]$, we get that $p|[L : K]$, a contradiction.

QUIZ 4. a) State Galois Correspondence Theorem.

b) Let F_1, F_2, K be subfields of a field L. Suppose that F_1/K and F_2/K are Galois. Prove that $F_1 \cap F_2/K$ is Galois.

Solution: a) **Galois Correspondence Theorem:** Let L/K be a finite Galois extension with Galois group $Gal(L/K) = G$. Let $\mathcal{F}$ be the set of all intermediate subfields between K and L:

$$\mathcal{F} = \{F : K \subseteq F \subseteq L \text{ and } F \text{ is a subfield of } L\}$$

and let $\mathcal{G}$ be the set of all subgroups of G. Define maps $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ and $\beta : \mathcal{G} \longrightarrow \mathcal{F}$ as follows:

$$\alpha(F) = Gal(L/F) \text{ and } \beta(H) = L^H.$$

Then

1. α and β are inverse of each other bijections;
2. These bijections reverse the inclusion, i.e. for $F_1 \subseteq F_2$ in $\mathcal{F}$ and $H_1 \subseteq H_2$ in $\mathcal{G}$ we have
$$Gal(L/F_1) \supseteq Gal(L/F_2) \text{ and } L^{H_1} \supseteq L^{H_2}.$$
3. for $F_1, F_2 \in \mathcal{F}$ and $H_1, H_2 \in \mathcal{G}$ we have
$$Gal(L/F_1F_2) = Gal(L/F_1) \cap Gal(L/F_2) \text{ and } L^{H_1 \cap H_2} = L^{H_1}L^{H_2}.$$
4. for $F_1, F_2 \in \mathcal{F}$ and $H_1, H_2 \in \mathcal{G}$ we have
$$Gal(L/(F_1 \cap F_2)) =< Gal(L/F_1) \cup Gal(L/F_2) > \text{ and } L^{<H_1 \cup H_2>} = L^{H_1} \cap L^{H_2},$$
where $< S >$ stands for the subgroup of G generated by the subset S.

5. for $\tau \in G$, $F \in \mathcal{F}$ and $H \in \mathcal{G}$ we have $\tau(F) \in \mathcal{F}$, $\tau H \tau^{-1} \in \mathcal{G}$ and

$$Gal(L/\tau(F)) = \tau Gal(L/F)\tau^{-1} \text{ and } L^{\tau H \tau^{-1}} = \tau(L^H).$$

6. for $F \in \mathcal{F}$, the extension F/K is Galois iff $Gal(L/F)$ is a normal subgroup of G, iff $\tau(F) = F$ for all $\tau \in G$. If this is the case, then the map $Gal(L/K) = G \longrightarrow Gal(F/K)$, which assignes to $\tau \in G$ its restriction to the field F, is a surjective homomorphism of groups with kernel $Gal(L/F)$. In particular, the groups $Gal(L/K)/Gal(L/F)$ and $Gal(F/K)$ are naturally isomorphic.

b) Note that F_1F_2/K is Galois, since it is separable and normal. In fact, if $F_1 = K(S_1)$, $F_2 = K(S_2)$ then $F_1F_2 = K(S_1 \cup S_2)$ and since each element of $S_1 \cup S_2$ is separable over K, the extension F_1F_2/K is separable. If F_i is the splitting field of f_i over K for $i = 1, 2$ then F_1F_2 is a splitting field of f_1f_2, hence it is normal over K. Thus we may assume that $L = F_1F_2$ is Galois over K. Now if F_i corresponds to a subgroup H_i of $G = Gal(L/K)$ then H_i are normal subgroups of G by (6) of Galois correspondence and by (4) the field $F_1 \cap F_2$ corresponds to $< H_1 \cup H_2 >$. Recall now that for normal subgroups H_1, H_2 we have $< H_1 \cup H_2 >= H_1H_2$ is normal, so $F_1 \cap F_2/K$ is Galois.

Second method We need to show that $F_1 \cap F_2/K$ is normal and separable. Since F_1/K is separable, so is $F_1 \cap F_2/K$. Suppose that $f \in K[x]$ is irreducible and has a root in $F_1 \cap F_2$. Then f has a root in F_1 and in F_2. Since both fields are normal over K, the polynomial f has all its roots in F_1 and F_2, hence in $F_1 \cap F_2$. This means that $F_1 \cap F_2/K$ is normal.

QUIZ 5. a) Define term ordering.

b) Find the smallest and largest elements in the graded lexicographic order among the monomials: $X_1^5X_2X_3$, $X_1^4X_2^2X_3^2$, $X_1^3X_2^4X_3$, X_1^6.

c) Consider the lexicographic order on monomials in X, Y, with $X > Y$. Let $f = X^3Y + X^2Y + X + Y^2$, $f_1 = X^2 + Y$, $f_2 = X^2Y + 1$. Use the division algorithm to find the remainder of f with respect to (f_1, f_2).

Solution: a) A **term ordering** is a total ordering $\leq$ on $\mathbb{N}^k$ such that:

1. $(0, ..., 0)$ is the smallest element;

2. If $\underline{n} < \underline{m}$ then $\underline{n} + \underline{w} < \underline{m} + \underline{w}$ for all $\underline{w} \in \mathbb{N}^k$.

b) The largest element is $X_1^4 X_2^2 X_3^2$ and the smallest element is X_1^6.

c) We start with

$$f = 0 \cdot (X^2 + Y) + 0 \cdot (X^2Y + 1) + 0 + (X^3Y + X^2Y + X + Y^2).$$

The algorithm produces the following steps:

$$f = XY \cdot (X^2 + Y) + 0 \cdot (X^2Y + 1) + 0 + (X^2Y - XY^2 + X + Y^2),$$

$$f = (XY + Y) \cdot (X^2 + Y) + 0 \cdot (X^2Y + 1) + 0 + (-XY^2 + X),$$

$$f = (XY + Y) \cdot (X^2 + Y) + 0 \cdot (X^2Y + 1) + (-XY^2) + X,$$

$$f = (XY + Y) \cdot (X^2 + Y) + 0 \cdot (X^2Y + 1) + (-XY^2 + X) + 0.$$

Thus the remainder is $-XY^2 + X$.