SF2732, Galoisteori
Final Exam
Wednesday May 22, 2013

Time: 08:00–13:00
Allowed aids: none
Examiners: Tilman Bauer and Wojciech Chachólski

Present your solutions to the problems in a way such that arguments and calculations are easy to follow. Provide detailed arguments to your answers. An answer without explanation will be given no points.

The final exam consists of six problems, each of which can give up to 6 credits. The score from which the grade will be decided will be the better of the exam and a weighted average of the exam and the homework (which can give up to 12 points), where the exam is given weight $2/3$ and homework $1/3$. In short, score = max$(x,\ 2x/3+h)$, where x is the score on the exam and h the number credits from the homework.

In order to pass the exam, a minimum of 18 credits is required. The grade Fx will be given for 16 or 17 credits. It can be upgraded to E by fulfilling an additional requirement, e.g., passing an oral exam.

The minimum requirements for the various grades are according to the following table:

Grade	**A**	**B**	**C**	**D**	**E**	**Fx**
Total credit	30	27	24	21	18	16

In thew following problems the symbol $\mathbf{Q}$ denotes the field of rational numbers, $\mathbf{C}$ the field of complex numbers and, for a prime number p and a natural number n, $\mathbf{F}_{p^n}$ the field with p^n-elements.

Problem 1

Consider the extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}, i)$.

(a) **(2 points)** Find an element $\alpha \in \mathbf{Q}(\sqrt{2}, i)$ for which $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\alpha)$.

(b) **(2 points)** For that element α find its minimal polynomial over $\mathbf{Q}$.

(c) **(2 points)** Prove that $\mathbf{Q}(\sqrt{2}, i)$ is normal over $\mathbf{Q}$.

Solutions

(a): We claim that $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\sqrt{2}+i)$. Note that $3 = (\sqrt{2}+i)(\sqrt{2}-i)$ and thus $\mathbf{Q}(\sqrt{2}+i) = \mathbf{Q}(\sqrt{2}-i)$. Which means that $\frac{1}{2}((\sqrt{2}+i)+(\sqrt{2}-i)) = \sqrt{2}$ belongs to $\mathbf{Q}(\sqrt{2}+i)$. Thus $i = (\sqrt{2}+i) - \sqrt{2}$ also belongs to $\mathbf{Q}(\sqrt{2}+i)$.

(b): Since i does not belong to $\mathbf{Q}(\sqrt{2})$, both of the extensions $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, i)$ are proper. It follows that $[\mathbf{Q}(\sqrt{2}+i) : \mathbf{Q}] = 4$. Note that $\sqrt{2}+i$ is a root of $(X^2-1)^2+8$. Since it is of degree 4, it has to be the minimal polynomial of $\sqrt{2}+i$.

(c): Consider the polynomial $(X^2-2)(X^2+1)$ note that all its roots are $\sqrt{2}$, $-\sqrt{2}$, i and $-i$. Thus $\mathbf{Q}(\sqrt{2}, i)$ is the splitting field of this polynomial and hence $\mathbf{Q}(\sqrt{2}, i)$ is normal over $\mathbf{Q}$.

Problem 2

Let p and q be distinct prime numbers. Show:

(a) **(3 points)** $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}] = 4$.

(b) **(3 points)** $\mathbf{Q}(\sqrt{p}, \sqrt{q}) = \mathbf{Q}(\sqrt{p}+\sqrt{q})$.

Solutions

(a): Consider the extensions $\mathbf{Q} \subset \mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\sqrt{p}, \sqrt{q})$. Note that $[\mathbf{Q}(\sqrt{p}) : \mathbf{Q}] = 2$. Thus $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}] = 4$ if and only if $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}(\sqrt{p})] = 2$, which happens if $\sqrt{q}$ does not belong to $\mathbf{Q}(\sqrt{p})$. Assume contrary that $\sqrt{q} = a + b\sqrt{p}$ for some rational numbers a and b. Since $\sqrt{q}$ is not rational, $b \neq 0$. Similarly since p and q are different primes, $a \neq 0$. The equality leads to $q = a^2 + 2ab\sqrt{p} + b^2p$ which implies:

$$\sqrt{p} = \frac{q - a^2 - b^2p}{2ab}$$

As $\sqrt{p}$ is not a rational number such an equality can not happen.

(b): Note that $(\sqrt{p}+\sqrt{q})(\sqrt{p}-\sqrt{q}) = p-q$. It follows that $\mathbf{Q}(\sqrt{p}+\sqrt{q}) = \mathbf{Q}(\sqrt{p}-\sqrt{q})$. Thus $\sqrt{p} = \frac{1}{2}(\sqrt{p}+\sqrt{q}+\sqrt{p}-\sqrt{q})$ and $\sqrt{q} = -\frac{1}{2}(\sqrt{p}-\sqrt{q}-(\sqrt{p}+\sqrt{q}))$ belong to $\mathbf{Q}(\sqrt{p}+\sqrt{q})$. which implies $\mathbf{Q}(\sqrt{p}, \sqrt{q}) = \mathbf{Q}(\sqrt{p}+\sqrt{q})$.

Problem 3

(6 points) Let $K \subset L$ be a field extension and $f \in K[X]$ be a polynomial such that it splits into distinct linear factors in $L[X]$ and the set of its roots form a subfield of L. Prove that $\mathrm{char}(K) = p \neq 0$ and $f = X^{p^n} - X$ for some integer $n > 0$.

Solutions

The set of roots of f is finite. It then follows that L contains a finite subfield. This can happen only if L has a non zero characteristic. As a sub field of L, the field K has then also a non zero characteristic. Let $p = \mathrm{char}(K)$. Let n be the number such that the set of roots of f is isomorphic to $\mathbf{F}_{p^n}$. Let α_i be all the roots of f. Then in $L[X]$ we have $f = \prod(X - \alpha_i)$. In $\mathbf{F}_{p^n}[X]$ we also have $\prod(X - \alpha_i) = X^{p^n} - X$. It thus follows that $f = X^{p^n} - X$.

Problem 4

(6 points) Compute the Galois groups of the polynomial $X^3 + X^2 + 1$ over $\mathbf{Q}$.

Solutions

The polynomial is irreducible because otherwise it would have to have a zero, and it does not have a zero modulo 2. So the Galois group is a transitive subgroup of S_3, thus either $\mathbf{Z}/3$ or S_3. The polynomial has local extrema over $\mathbf{R}$ at $X = 0$ and $X = -\frac{2}{3}$, and is positive at both of these points, hence it only has one real root. The transposition of the complex roots is an order 2 element of the Galois group, so it must be S_3. Alternatively, use the discriminant.

Problem 5

(6 points) Let p be a prime. Show that for any $x \in \mathbf{F}_{p^n}$, we have $x^{\frac{p^n-1}{p-1}} \in \mathbf{F}_p$.

Solutions

We can write $x^{\frac{p^n-1}{p-1}} = x \cdot x^p \cdot x^{p^2} \cdot \dots \cdot x^{p^{n-1}}$, which is the norm of x because the Frobenius $F(x) = x^p$ generates the Galois group $\mathbf{Z}/n\mathbf{Z}$ of $\mathbf{F}_{p^n}$.

Problem 6

(6 points) For the field extension from Problem 4, find all the intermediate fields. Hint: the discriminant of $X^3 + X^2 + 1$ is -31.

Solutions

Let K denote the splitting field of $X^3 + X^2 + 1$ over $\mathbf{Q}$. The intermediate fields are in one-to-one correspondence with the subgroups of S_3, and those are $A_3 = \mathbf{Z}/3$ and three pairwise conjugate groups of order 2 given by transpositions, in addition to the trivial subgroup and all of S_3. Let α be the real root of $X^3 + X^2 + 1$ and $\beta, \overline{\beta}$ the two complex roots. The three subfields corresponding to the order-2 subgroups are $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$, $\mathbf{Q}(\overline{\beta})$.

The subfield corresponding to A_3 is $\mathbf{Q}(\sqrt{\Delta})$, where Δ is the discriminant of $X^3 + X^2 + 1$ (which happens to be -31). Indeed, since $\Delta = (a - b)^2(a - \bar{b})^2(b - \bar{b})^2$, $\sqrt{\Delta} \in K$ and thus $K \supseteq \mathbf{Q}(\sqrt{\Delta}) \supseteq \mathbf{Q}$. By considering the degrees, we see that $\mathbf{Q}(\sqrt{\Delta})$ must correspond to A_3.