Math 210B: Algebra, Homework 9

Ian Coley

March 4, 2014

Problem 1.
Let $I$ be the ideal in $\mathbb{Q}[X, Y]$ generated by $X^2 + Y$ and $Y^2 - 2$. Is the factor ring $\mathbb{Q}[X, Y]/I$ a field?

Solution.
We have

$$\mathbb{Q}[X, Y]/I = (\mathbb{Q}[Y]/(Y^2 - 2))[X]/(X^2 + Y).$$

We examine this term piecewise. To begin, we have $\mathbb{Q}[Y]/(Y^2 - 2) \cong \mathbb{Q}(\sqrt{2})$, where we identify $Y = -\sqrt{2}$. Then we have the new quotient $\mathbb{Q}(\sqrt{2})[X]/(X^2 - \sqrt{2})$. Then we again have a quadratic extension, since this polynomial is irreducible over $\mathbb{Q}(\sqrt{2})$, and we see this quotient is isomorphic to $\mathbb{Q}(\sqrt{2})$ under the identification $X = \sqrt{2}$. Therefore the quotient $\mathbb{Q}[X, Y]/I$ is indeed a field. \qed

Problem 2.
Let $p$ be a prime integer, $\zeta \in \mathbb{C}$ a primitive $p$th root of unity. Find the degree of the extension $\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}$.

Solution.
We have the following tower of fields:

$$\mathbb{Q}(\zeta) \supseteq \mathbb{Q}(\zeta + \zeta^{-1}) \supseteq \mathbb{Q}.$$

We will use Galois correspondence to compute the degree of $\mathbb{Q}(\zeta + \zeta^{-1})$ over $\mathbb{Q}$. The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is by previous calculation $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, with elements $\sigma_r(\zeta) = \zeta^r$, for $1 \leq r \leq p - 1$. To see which elements of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ fix $\zeta + \zeta^{-1}$, we note

$$\sigma_r(\zeta + \zeta^{-1}) = \zeta^r + (\zeta^r)^{p-1} = \zeta^r + \zeta^{-r}.$$

Therefore the only choices of $r$ which are valid are $r = 1$, which is clear, and $r = p - 1$, because

$$\zeta^{p-1} + \zeta^{-(p-1)} = \zeta^{p-1} + \zeta^{-(p-1)} \cdot \zeta = \zeta + \zeta^{-1}.$$

Since the degree of this extension is equal to the index of the subgroup fixing the extension, have $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) : \langle \sigma_{p-1} \rangle| = (p - 1)/2$. \qed
Problem 3.
Find a field \( F \) such that for every \( n \geq 1 \) there exists a subfield \( F_n \subset F \) with \( [F : F_n] = n \).

Solution.
Let \( F = \mathbb{C}(X) \). Consider the subfield \( \mathbb{C}(X^n) \). Then we see that \( X \) is a root of the polynomial \( Y^n - X^n \), which is irreducible over \( \mathbb{C}(X^n) \) since \( X^n \) is a prime element of \( \mathbb{C}[X^n] \) and we may apply Eisenstein’s criterion. Therefore \( [\mathbb{C}(X) : \mathbb{C}(X^n)] = n \). Since this is viable any \( n \in \mathbb{N} \), we are done with the choice \( F_n = \mathbb{C}(X^n) \).

Problem 4.
Let \( K/F \) be a quadratic extension. Prove that if \( \text{char } F \neq 2 \), then \( K = F(\alpha) \) for some \( \alpha \in K \) so that \( \alpha^2 \in F \).

Solution.
This extension must be separable. If it were inseparable and \( \text{char } F = p > 2 \), then we would have \( p | 2 \), which is impossible. Let \( a \in K \setminus F \). Then \( [F(a) : F] > 1 \), so we have \( F(a) = K \). Therefore let the minimal polynomial of \( a \) be \( X^2 + BX + C \), with \( B, C \in F \). Then since \( \text{char } F \neq 2 \) so that we may divide by 2, we may apply the quadratic formula to this polynomial:

\[
a = \frac{-B \pm \sqrt{B^2 - 4C}}{2}.
\]

Without loss of generality, assume that we can choose + for the \( \pm \). Then we have

\[
F(a) = F\left(\frac{-B \pm \sqrt{B^2 - 4C}}{2}\right) = F(\sqrt{B^2 - 4C}).
\]

Therefore \( \sqrt{B^2 - 4C} \) is an appropriate choice for \( \alpha \).

Problem 5.
Let \( K/F \) be a separable quadratic extension. Prove that if \( \text{char } F = 2 \), then \( K = F(\alpha) \) for some \( \alpha \in K \) such that \( \alpha^2 + \alpha \in F \).

Solution.
Again as above, choose \( a \in K \setminus F \), so that \( F(a) = K \). Then let the minimal polynomial of \( a \) be \( X^2 + BX + C \). We must have \( B \neq 0 \), else the polynomial \( X^2 + C = (X + \sqrt{C})^2 \) is not separable, which contradicts our assumptions. Then we see that

\[
(a + d)^2 + B(a + d) + C = a^2 + Ba + c + d^2 + Bd = d(d + B).
\]

Therefore the choice \( d = -B \) yields

\[
(a - B)^2 + B(a - B) + C = 0.
\]

We know that \( C \) is the product of the roots, so \( a(a - B) = C \). Performing a linear change of variables \( \alpha = a - B + 1 \), we have \( F(a) = F(\alpha) \). Further, \( \alpha^2 + \alpha = C \in F \), so we are done.
Problem 6.
Let $L/F$ be a field extension and let $E$ and $K$ be two subfields $L$ containing $F$. Show that there is a smallest subfield $M \subset L$ containing $E$ and $K$. Prove that $E/F$ is separable, then $M/K$ is also separable.

Solution.
First, such an $M$ exists because $L$ is a subfield of itself containing both $E$ and $K$. Therefore take the set $E \cap K$. Then we uniquely close this set under addition, multiplication, and inversion to obtain a subfield $M$. By definition, this is $M = F(E \cup K)$, and any subfield containing $E$ and $K$ must contain $M$, else it is not closed under field operations.

Now suppose that $E/F$ is separable, and let $\alpha \in E$. Then consider the tower $M \supset K(\alpha) \supset K$. Since $\alpha$ is separable over $F$, it is also separable over $K$, so $K(\alpha) \supset K$ is separable. Since this holds for every $\alpha \in E$, and these elements generate $M$ over $K$, every element of $M/K$ is separable.

Problem 7.
Prove that a finite extension of a perfect field is also perfect.

Solution.
Let $F$ be a perfect field and $K/F$ a finite extension. Let $L/K$ be a finite extension. Then $L/F$ is a finite extension as well, so it is separable. Since separable extensions are a good class of extensions the subextension $L/K$ is as as well. Therefore by Problem 8, $K$ is a perfect field.

Problem 8.
Prove that a field $F$ is perfect if and only if any finite extension of $F$ is separable.

Solution.
First, suppose that $\text{char } F = 0$. Then $F$ is a fortiori perfect. Further, the derivative of any nonconstant polynomial is nonzero, so every irreducible polynomial is separable. Let $E/F$ be a finite extension. Then for every $\alpha \in E$, the minimal polynomial of $\alpha$ is separable, so $E/F$ is separable.

Now if $\text{char } F = p$, then every polynomial of the form $f(X^p)$ for $f \in F[X]$ has derivative 0. Let $\varphi$ denote the $p$th power map $x \mapsto x^p$. Therefore let $E/F$ be a finite extension. Suppose that $\alpha \in E$ is an inseparable element. Then the minimal polynomial of $\alpha$ is of the form $f(X^{p^n})$ for a separable polynomial $f$. Therefore write

$$\sum_{i=1}^{r} a_i (\alpha^{p^n})^i = 0.$$

Since $\varphi$ is an automorphism on $F$, for each of the $a_i$, there is a $p$th root $\varphi^{-1}(a_i)$, and by induction a $p^n$th root. Let $b_i$ be the $p^n$th root of $a_i$. Then

$$\sum_{i=1}^{r} a_i (\alpha^{p^n})^i = \left( \sum_{i=1}^{r} b_i \alpha^i \right)^{p^n} = 0 \implies \sum_{i=1}^{r} b_i \alpha^i = 0.$$
Therefore we must have \( n = 0 \) in the first case, so that the minimal polynomial of \( \alpha \) is itself separable. Therefore every inseparable element of \( E \) lies in \( F \) itself, so the entire extension is separable. Conversely, suppose that \( F \) is not perfect. Then \( \varphi \) is not surjective, so let \( a \in F \setminus F^p \). Then the polynomial \( X^p - a \) has no roots in \( F \). Further, it is an inseparable polynomial since it has derivative zero. Therefore the finite extension of \( F \) given by adjoining a root of \( X^p - a \) is not separable. This completes the proof.

**Problem 9.**
Let \( E/F \) be a field extension of a field \( F \) of characteristic \( p > 0 \). Prove that for any \( \alpha \in E \), which is separable over \( F \), \( F(\alpha) = F(\alpha^p) \).

**Solution.**
We have a tower of fields \( F \subset F(\alpha^p) \subset F(\alpha) \). Since \( \alpha \) is separable over \( F \), it is also separable over \( F(\alpha^p) \). But \( \alpha \) is a root of \( X^p - \alpha^p \), which factors as \((X - \alpha)^p \) in \( F(\alpha) \). Since the minimal polynomial of \( \alpha \) over \( F(\alpha^p) \) must have only simple roots, it must be \( X - \alpha \) alone. Therefore \( \alpha \in F(\alpha^p) \), so \( F(\alpha) = F(\alpha^p) \).

**Problem 10.**
Let \( F \) be a field of characteristic \( p > 0 \). Show that there are infinitely many fields \( K \) such that \( F(X^p, Y^p) \subset K \subset F(X, Y) \).

**Solution.**
Let \( K_f = F(X + f \cdot Y) \), where \( f \in F[X^p, Y^p] \) is a nonconstant polynomial. First, note that \( K_f \neq F(X, Y) \), since \([K_f : F(X^p, Y^p)] = p\) and \([F(X, Y) : F(X^p, Y^p)] = p^2\). We claim that for \( f \neq g \), we have \( K_f \neq K_g \). Suppose there were \( f \neq g \) such that \( K_f = K_g \). Call this field \( K \). Then

\[
X + g \cdot Y - g/f \cdot (X + f \cdot Y) = (1 - g/f)X \in K.
\]

Since \( g \neq f \), \( 1 - g/f \in K^\times \), so \( X \in K \). Hence \( X, Y \in K \), so \( K = F(X, Y) \), which is a contradiction. Therefore since there are infinitely choices for \( f \), there are infinitely many nonisomorphic intermediate fields \( K_f \).