Problem Set 5: Math 454 Spring 2017
Due Thursday February 16

January 6, 2017

Do the problems below. Please write neatly, especially your name! Show all your work and justify all your steps. Write in complete, coherent sentences. I expect and openly encourage you to collaborate on this problem set. I will insist that you list your collaborators on the handed in solutions (list them on the top of your first page).

Problem 1. Let E/F be an extension of fields and $\beta \in E$ be algebraic. Prove that if $P \in F[t]$ is a non-zero polynomial such that $P(\beta) = 0$, then the minimal polynomial P_β of β over F divides P. In particular, the minimal polynomial of β is irreducible.

Problem 2. Let E/F be a finite extension and $L\colon E \to \mathrm{M}(n,F)$ be an injective F–algebra homomorphism with $n = [E:F]$.

(a) Prove that if $c_{L(\beta)}$ is the characteristic polynomial of $L(\beta)$, then P_β divides $c_{L(\beta)}$.

(b) Prove that there exists an F–basis $\{\beta_1, \ldots, \beta_n\}$ of E such that for each $\beta \in E$, if we define the n by n matrix (A_β) to have (i,j) coefficient $(\alpha_{i,j})$ where $\alpha_{i,j}$ is defined by

$$\beta\beta_j = \sum_{i=1}^{n} \alpha_{i,j}\beta_i,$$

then $L(\beta) = A_\beta$.

Problem 3. Let E/F be a finite extension of degree n and $m \in \mathbf{N}$ with $m < n$. Prove that there cannot be an injective F–algebra homomorphism $L\colon E \to \mathrm{M}(m,F)$.

Problem 4. Let $P_1, P_2 \in F[t]$. Prove that if $P \in F[t]$ divides $\gcd(P_1,P_2)$, then there exists an $\alpha \in F$ such that $P = \alpha \gcd(P_1,P_2)$.

Problem 5. Let $P_1, P_2 \in F[t]$. Prove that $\langle P_1 \rangle \langle P_2 \rangle = \langle \gcd(P_1,P_2) \rangle$.

Problem 6. Let $m_1, \ldots, m_n \in \mathbf{N}$ and assume that $\gcd(m_i,m_j) = 1$ for all $i \neq j$.

(a) Prove that

$$\bigcap_{i=1}^{n} m_i\mathbf{Z} = (m_1 \ldots m_n)\mathbf{Z}.$$

(b) Prove that

$$\mathbf{Z}/\langle m_1 \ldots m_n \rangle \cong \prod_{i=1}^{n} \mathbf{Z}/m_i\mathbf{Z}.$$

(c) Prove that if $s_1, \ldots, s_n \in \mathbf{N}$, then

$$\bigcap_{i=1}^{n} s_i\mathbf{Z} = \mathrm{lcm}(s_1, \ldots, s_n)\mathbf{Z}.$$

(d) Prove that if $s,t \in \mathbf{N}$ and s divides t, then there exists a surjective ring homomorphism $\psi_{s,t}\colon \mathbf{Z}/t\mathbf{Z} \to \mathbf{Z}/s\mathbf{Z}$.

(e) If $s = \operatorname{lcm}(s_1,\dots,s_n)$, prove that there exists an injective homomorphism

$$\psi\colon \mathbf{Z}/s\mathbf{Z} \to \prod_{i=1}^{n} \mathbf{Z}/s_i\mathbf{Z}$$

such that the index of $\psi(\mathbf{Z}/\operatorname{lcm}(s_1,\dots,s_n)\mathbf{Z})$ in $\prod_{i=1}^n \mathbf{Z}/s_i\mathbf{Z}$ is $\gcd(s_1,\dots,s_n)$.

(f) Deduce that if $s_1,\dots,s_n \in \mathbf{N}$, then

$$s_1 \dots s_n = \operatorname{lcm}(s_1,\dots,s_n)\gcd(s_1,\dots,s_n).$$

Problem 7. Let $P_1,\dots,P_n \in F[t]$ and assume that $\gcd(P_i,P_j) = 1_F$ for $i \neq j$.

(a) Prove that

$$\bigcap_{i=1}^{n} \langle P_i \rangle = \langle P_1 \dots P_n \rangle .$$

(b) Prove that

$$F[t]/\langle P_1 \dots P_n \rangle \cong \prod_{i=1}^{n} F[t]/\langle P_i \rangle .$$

Problem 8. Let F be a field and $\mathfrak{a}$ be a non-zero, proper ideal in $F[t]$. Prove that if $P_1,P_2 \in \mathfrak{a}$ have minimal degree (among the non-zero elements), then there exists $\alpha \in F$ such that $\alpha P_1 = P_2$. In particular, if $P_1,P_2 \in \mathfrak{a}$ have minimal degree, then $\mathfrak{a} = \langle P_1 \rangle = \langle P_2 \rangle$. Deduce that for each non-zero ideal $\mathfrak{a}$, there exists a unique monic polynomial P of minimal degree and $\langle P \rangle = \mathfrak{a}$.

Problem 9. Let $P_1,\dots,P_n \in F[t]$ and

$$\langle P \rangle = \bigcap_{i=1}^{n} \langle P_i \rangle .$$

(a) Prove that if $Q \in F[t]$ and P_i divides Q for $i = 1,\dots,n$, then P divides Q. Moreover, there is a unique monic polynomial P with this property. We call such a P the **least common multiple** of $P_1,\dots,P_n$ and we denote it by $\operatorname{lcm}(P_1,\dots,P_n)$.

(b) Prove that there exists $\alpha \in F$ such that

$$P_1 \dots P_n = \alpha \operatorname{lcm}(P_1,\dots,P_n)\gcd(P_1,\dots,P_n).$$

Problem 10. Let $P \in F[t]$. Define

$$dP(t) \stackrel{\text{def}}{=} \sum_{i=1}^{m} i\alpha_i t^{i-1}$$

where

$$P(t) = \sum_{i=0}^{m} \alpha_i t^i.$$

(a) Prove that $D\colon F[t] \to F[t]$ defined by $D(P) = dP$ is an F–linear function.

(b) Prove that $P \in F[t]$ is separable if and only if $\gcd(P,dP) = 1_F$.

(c) Prove that if $\operatorname{char}(F) = 0$, then every irreducible polynomial $P \in F[t]$ is separable. [Hint: Use (b)]

(d) Prove that if F is a field with $\operatorname{char}(F) = p \neq 0$ and $P \in F[t]$ is irreducible and not separable, then there exists $Q \in F[t]$ such that $P(t) = Q(t^p)$. [Hint: Use (b)]