Midterm : Math 454, Spring 2017

Write clearly and in complete sentences. Justify your work. You are allowed to use the class notes but you cannot read any of the external links. You are not allowed to work with anyone on the problems.

Problem 1. Let $\mathbf{Q}$ denote the field of rational numbers and $\mathbf{Z}$ the subring of the integers. We say that a polynomial $P \in \mathbf{Z}[t]$ is **primitive** if the greatest common divisor of the coefficients is one. Namely, if

$$P(t) = \sum_{j=0}^{n} \alpha_j t^j,$$

then

$$\gcd(\alpha_0, \alpha_1, \ldots, \alpha_n) = 1.$$

(a) Prove that if $P_1, P_2 \in \mathbf{Z}[t]$ are primitive polynomials, then $P_1 P_2$ is primitive.

(b) Prove that if $Q \in \mathbf{Q}[t]$, then there exists a unique decomposition

$$Q = \alpha_Q Q_\star$$

where $Q_\star \in \mathbf{Z}[t]$ is primitive and $\alpha_Q \in \mathbf{Q}$ with $\alpha_Q > 0$.

(c) Prove that if $R \in \mathbf{Q}[t]$ has a factorization $R = PQ$, then

$$R_\star = P_\star Q_\star, \quad \alpha_R = \alpha_P \alpha_Q.$$

(d) Prove that if $P \in \mathbf{Z}[t]$ has a factorization $P = P_1 P_2$ with $P_1, P_2 \in \mathbf{Q}[t]$, then $P = Q_1 Q_2$ with $Q_1, Q_2 \in \mathbf{Z}[t]$, $\deg(P_1) = \deg(Q_1)$, and $\deg(P_2) = \deg(Q_2)$.

(e) Prove that $P \in \mathbf{Z}[t]$ is irreducible over $\mathbf{Z}$ if and only if P is irreducible over $\mathbf{Q}$.

Problem 2. Let $P \in \mathbf{Z}[t]$ with

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

If $\alpha \in \mathbf{Z}$ is such that whenever m^2 divides α, then either $m = \pm 1$, we say that α is square-free.

(a) Let $Q, R \in \mathbf{Q}[t]$ with Q irreducible over $\mathbf{Q}$ and $\deg(Q) = n$. Prove that if

$$Q(R(t)) = \prod_{j=1}^{r} Q_j(t)$$

is the factorization of $Q(R(t))$ into irreducible polynomials, then n divides $\deg(Q_j)$ for $j = 1, \ldots, r$.

(b) Prove that if P is irreducible over $\mathbf{Q}$ and $\beta \in \mathbf{Q}$, then $P_\beta(t) \stackrel{\text{def}}{=} P(t + \beta)$ is irreducible over $\mathbf{Q}$.

(c) Prove that if there exists a prime $p \in \mathbf{N}$ such that p divides α_i for all $i < n$ but p does not divide α_n and p^2 does not divide α_0, then P is irreducible over $\mathbf{Q}$.

(d) Let $p \in \mathbf{N}$ be a prime. Prove that

$$\Phi_p(t) = \frac{t^p - 1}{t - 1}$$

is irreducible over $\mathbf{Q}$.

(e) Prove that if $\alpha \in \mathbf{Z}$ is square-free and $\alpha \neq \pm 1$, then

$$P(t) = t^n - \alpha$$

is irreducible for all $n > 1$.

Problem 3. Let F be a field and $P \in F[t]$ with $\deg(P) = n$. We define

$$P_{\text{rec}}(t) \stackrel{\text{def}}{=} t^n P(t^{-1}).$$

(a) Prove that if

$$P(t) = \sum_{j=0}^{n} \alpha_j t^j$$

then

$$P_{\text{rec}}(t) = \sum_{j=0}^{n} \alpha_{n-j} t^j.$$

(b) Prove that α is a root of P if and only if α^{-1} is a root of P_{rec}.

(c) Prove that if P is irreducible over F and $P(t) \neq t$, then P_{rec} is irreducible over F.

(d) Prove that if P is irreducible and $P = P_{\text{rec}}$, then $\deg(P)$ is even.

(e) Prove that if $R = R_{\text{rec}}$ and $R = PQ$ where $P, Q \in F[t]$ are irreducible, then

$$P_{\text{rec}} = \pm P, \quad Q_{\text{rec}} = \pm Q$$

or

$$P = \alpha Q_{\text{rec}}, \quad Q = \alpha^{-1} P_{\text{rec}}$$

for some $\alpha \in F$.

Problem 4. Do the following problems.

(a) Let E/F be an algebraic extension and $F \leq R \leq E$ be a subring. Prove that R is a subfield.

(b) Let E/F be an extension of fields and $\beta_1, \beta_2 \in E$ be algebraic. Prove that if the degree of the minimal polynomials for β_1, β_2 are relatively prime, then $[F(\beta_1, \beta_2) : F] = [F(\beta_1) : F][F(\beta_2) : F]$.

(c) Let E/F be a finite extension of degree $n > 1$ and F be an infinite field. Prove that $E^\times / F^\times$ is infinite.

Problem 5. Do the following problems.

(a) Let E/F be a degree two extension. Prove that there exists an F–vector space basis $\{1,\beta\}$ such that $\beta^2 \in F$.

(b) Let $E/\mathbf{Q}$ be a degree two extension. Prove that there exists a square-free $m \in \mathbf{Z}$ such that $E = \mathbf{Q}(\sqrt{m})$.

(c) Prove that if $m_1, m_2 \in \mathbf{Z}$ are distinct square-free integers, then $\mathbf{Q}(\sqrt{m_1})$ and $\mathbf{Q}(\sqrt{m_2})$ are not isomorphic.

(d) Prove that there is a bijection between isomorphism classes of degree two extensions of $\mathbf{Q}$ and square-free integers.

Problem 6. In what follows, $\mathbf{F}_p$ denotes the finite field with p elements.

(a) Prove that

$$t^p - t = \prod_{\alpha \in \mathbf{F}_p} (t - \alpha).$$

(b) Let $\ell = p^n$ with $n \in \mathbf{N}$. Prove that

$$P_\ell(t) = t^\ell - t$$

has no repeated roots.

(c) Let $\mathbf{F}_\ell = \text{Roots}(P_\ell)$. Prove that $\mathbf{F}_\ell$ is a field (i.e. the set of roots of closed under addition, multiplication, additive inverses, and multiplicative inverses).

(d) Prove that $\mathbf{F}_\ell$ is the splitting field of P_ℓ over $\mathbf{F}_p$.

(e) Prove that if $\mathbf{F}/\mathbf{F}_p$ is a degree n extension, then

$$t^{p^n} - t = \prod_{\beta \in \mathbf{F}} (t - \beta).$$

(f) Prove that if $\mathbf{F}, \mathbf{F}'$ are degree n extensions of $\mathbf{F}_p$, then $\mathbf{F}, \mathbf{F}'$ are isomorphic.