Midterm 2 Review Problems: Math 453 Spring 2019

April 16, 2019

1 Definitions

There will be two definitions on the exam.

Problem 1. Given a commutative ring R, state the cancellation property for R.

Problem 2. Given a commutative ring R, state the definition for $r \in R$ to be a zero divisor.

Problem 3. Given commutative rings R, S, state the definition for a function $\psi \colon R \to S$ to be a ring homomorphism.

Problem 4. Given a commutative ring R, state the definition for $r \in R$ to be a unit.

Problem 5. Given a commutative ring R, state the definition for a subset $\mathscr{I} \subset R$ to be an ideal.

Problem 6. Given a commutative ring R, state the definition for a subset $\mathscr{I} \subset R$ to be a prime ideal.

Problem 7. Given a commutative ring R, state the definition for a subset $\mathscr{I} \subset R$ to be a maximal ideal.

Problem 8. State the definition of a monic polynomial $P \in F[t]$ where F is a field.

Problem 9. State the definition of an irreducible polynomial $P \in F[t]$ where F is a field.

Problem 10. Given polynomials $P, Q \in F[t]$, state the definition of $\gcd(P, Q)$.

2 True/False

There will be four true/false questions. Two will be true and two will be false. Flip a coin in doubt. Good luck.

3 Work Problems

There will be four work problems on the exam.

3.1 General ring problems; mostly the problems previously known as problem set 7

Problem 11. Let R be a commutative ring and let $S \subset R$ is closed under multiplication. Let $\mathfrak{a}$ to be an ideal in R such that $\mathfrak{a} \cap S = \emptyset$. We further assume that if $\mathfrak{b}$ is an ideal in R such that $\mathfrak{a} \subset \mathfrak{b}$ and $\mathfrak{a} \neq \mathfrak{b}$, then $\mathfrak{b} \cap S \neq \emptyset$. Prove that $\mathfrak{a}$ is a prime ideal in R.

Problem 12. Let R be a commutative ring and take $S = \{1\}$. Prove that if $\mathfrak{a}$ is an ideal satisfying the condition in the Problem 1 for $S = \{1\}$. Prove that $\mathfrak{a}$ is a maximal ideal.

Problem 13. Let R be a commutative ring and let $\mathfrak{m}$ be a maximal ideal. Prove that $\mathfrak{m}$ satisfies the condition in Problem 1 for $S = \{1\}$.

Problem 14. Let R be a commutative ring. Prove that every maximal ideal in R is a prime ideal.

Problem 15. Let $\mathfrak{a}$ be an ideal in $\mathbf{Z}$. Define $m_{\mathfrak{a}}$ to be the smallest positive integer $m_{\mathfrak{a}} \in \mathfrak{a}$.

(a) Prove that if $\ell \in \mathfrak{a}$, then $m_{\mathfrak{a}}$ divides ℓ.

(b) Prove that $\mathfrak{a} = m_{\mathfrak{a}}\mathbf{Z}$ where

$$m_{\mathfrak{a}}\mathbf{Z} = \{jm_{\mathfrak{a}} \ : \ j \in \mathbf{Z}\}.$$

Problem 16. Prove that $\gcd(n-1, n^2+n+1) = 1$ or 3 for all $n \in \mathbf{Z}$.

Problem 17. Let R be a finite, integral domain. Prove that R is a field.

Problem 18. Let $\overline{a} \in \mathbf{Z}/m\mathbf{Z}$ with $\overline{a} \neq \overline{0}$. Prove that $\overline{a}$ is invertible in $\mathbf{Z}/m\mathbf{Z}$ if and only if $\gcd(a,m) = 1$.

Problem 19. Prove that $\mathbf{Z}/m\mathbf{Z}$ is a field if and only if m is prime.

Problem 20. Let $p \in \mathbf{N}$ be a prime such that $p \equiv 1 \mod 4$. Prove that $p = a^2 + b^2$ for some $a, b \in \mathbf{Z}$.

Problem 21. Let R be a ring with the following property: For all $r, s, t \in R$ with $r \neq 0$ such that $rs = tr$, we have $s = t$. Prove that R is commutative.

Problem 22. Let R be a commutative ring with the property that every ideal $\mathfrak{a}$ of R with $\mathfrak{a} \neq R$ is a prime ideal. Prove that R is a field.

Problem 23. Let R be a commutative ring with the following property: for each $r \in R$, there exists $n_r \in \mathbf{N}$ such that $r^{n_r} = r$. Prove that if $\mathfrak{p}$ is a prime ideal in R, then $\mathfrak{p}$ is a maximal ideal in R.

Problem 24. Let R be a commutative ring and let S be the subset of R comprised of all $r \in R$ that are not invertible (i.e. have no multiplicative inverse). Prove that following two statements are equivalent:

(a) R has a unique maximal ideal $\mathfrak{m}$.

(b) S is an ideal in R.

Problem 25. Let R, S be commutative rings and $\psi \colon R \to S$ a ring homomorphism.

(a) Let $\mathfrak{a} \lhd S$ an ideal. Prove that $\psi^{-1}(\mathfrak{a})$ is an ideal in R.

(b) Let $\mathfrak{p} \lhd S$ a prime ideal. Prove that $\psi^{-1}(\mathfrak{p})$ is a prime ideal in R.

Problem 26. Let R be a commutative ring.

(a) Prove that there exists a ring homomorphism $\psi \colon \mathbf{Z} \to R$.

(b) Prove that if $\psi_1, \psi_2 \colon \mathbf{Z} \to R$ are any pair of ring homomorphisms, then $\psi_1 = \psi_2$.

(c) Prove that $\ker \psi = m_R\mathbf{Z}$ for some $m_R \in R$. The positive integer m_R is called the **characteristic** of the ring. Note that if ψ is injective, the characteristic is defined to be 0.

(d) Prove if R is an integral domain, then m_R is either a prime or zero.

(e) Prove that if R is a finite field, then m_R is a prime.

Problem 27. Let R be a commutative such that there exists a prime ideal $\mathfrak{p} \lhd R$ with no nonzero zero divisor. That is, if $a \in \mathfrak{p}$ and $a \neq 0$, then a is not a zero divisor. Prove that R is an integral domain.

Problem 28. Let R be a commutative ring. We say that an ideal $\mathfrak{a}$ of R is **irreducible** if whenever $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$ for ideals $\mathfrak{a}_1, \mathfrak{a}_2 \lhd R$, then $\mathfrak{a} = \mathfrak{a}_1$ or $\mathfrak{a} = \mathfrak{a}_2$. Prove that if $\mathfrak{p}$ is a prime ideal in R, then $\mathfrak{p}$ is irreducible.

Problem 29. Let R be a commutative ring and let $r \in R$ be such that $r^n = 0$ for some positive integer n. Prove that $1 - ra$ is a unit in R for all $a \in R$.

Problem 30. Let R be a commutative ring with $r \in R$ such that $r^2 = r$ and $r \neq 0, 1$. Prove that if $\mathfrak{p}$ is a prime ideal in R, then there exists $s \in \mathfrak{p}$ such that $s^2 = s$ and $s \neq 0, 1$.

Problem 31. Let R be a commutative ring and let $\mathfrak{a}$ be an ideal in R such that $1 + a$ is a unit for all $a \in \mathfrak{a}$. Prove that if $\mathfrak{m}$ is a maximal ideal, then $\mathfrak{a} \subset \mathfrak{m}$.

Problem 32. Let R be a commutative ring and let $r \in R$ be such that $r^n = 0$ for some $n > 0$. Prove that if $\mathfrak{p}$ is a prime ideal in R, then $r \in \mathfrak{p}$.

Problem 33. Let R be a commutative ring and let $x \in R$ be such that $x^n \neq 0$ for all $n \in \mathbf{N}$. Prove that there exists a prime ideal $\mathfrak{p}$ in R with $x \notin \mathfrak{p}$.

Problem 34. Let R be a finite, commutative ring. Prove that if $\mathfrak{p}$ is a prime ideal in R. then $\mathfrak{p}$ is a maximal ideal.

Problem 35. Let R be a commutative ring with $x, y \in R$ such that x is a unit and $y^n = 0$ for some $n > 0$. Prove that $x + y$ is a unit.

Problem 36. Let R be a commutative ring with exactly three ideals $\{0\}, R$, and $\mathfrak{a}$.

(a) Prove that if $x \notin \mathfrak{a}$, then x is a unit.

(b) Prove that if $x \in \mathfrak{a}$, then there exists $r \in R$ with $rx = 0$ and $r \neq 0$.

3.2 Polynomial problems

Let F be a field and let $F[t]$ be the polynomial ring over F in one variable t.

Problem 37. Let $P(t) = t + 1$ and $Q(t) = t^2 - t + 1$, and view $P, Q \in \mathbf{Q}[t]$.

(a) Compute $\gcd(P, Q)$.

(b) Prove that there exists $n \in \mathbf{Z}$ such that $\gcd(n + 1, n^2 - n + 1) \neq 1$.

Problem 38. Let $P \in F[t]$ and $\beta \in F$. Prove that the following are equivalent:

(a) $P(\beta) = 0$.

(b) $t - \beta$ divides P.

Problem 39. Let $P \in F[t]$ be a degree n polynomial and let

$$\mathrm{Zero}(P) = \{\beta \in F \ : \ P(\beta) = 0\}.$$

Prove that $|\mathrm{Zero}(P)| \leq n$.

Problem 40. Let F be a field, $\beta \in F$, and define $P(t) = t^n - \beta^n$. Prove that $t - \beta$ divides P.

Problem 41. We say $\alpha \in \mathbf{Z}$ is square-free if whenever m^2 divides α, then either $m = \pm 1$. 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 $n > 1$ in $\mathbf{Q}[t]$.

Problem 42. Let $P \in F[t]$ and $\beta \in F$. Define $L(t) = t - \beta$, $\alpha = P(\beta)$, and $Q(t) = P(t) - \alpha$.

(a) Prove that L divides Q.

(b) Prove that $P(t) = R(t)L(t) + \alpha$.

Problem 43. Prove that if P is irreducible over $\mathbf{Q}$ and $\beta \in \mathbf{Q}$, then $P_\beta(t) = P(t+\beta)$ is irreducible over $\mathbf{Q}$.

Problem 44. Let $\alpha = \sqrt{2} + \sqrt{3} \in \mathbf{R}$ and define

$$\mathfrak{m}_\alpha = \{P \in \mathbf{Q}[t] \,:\, P(\alpha) = 0\}.$$

(a) Prove that $\mathfrak{m}_\alpha$ is an ideal in $\mathbf{Q}[t]$.

(b) Find the unique irreducible, monic polynomial $P_\alpha \in \mathfrak{m}_\alpha$ such that $\mathfrak{m}_\alpha = \langle P_\alpha \rangle$.

(c) Prove that $E = \mathbf{Q}[t]/\mathfrak{m}_\alpha$ is a field.

(d) Prove that there exists $\beta \in E$ such that $P_\alpha(\beta) = 0$.

Problem 45. Let $P \in F[t]$ with $P(t) = t^2 + \alpha_1 t + \alpha_0$ and $P(t) = (t - \beta_1)(t - \beta_2)$. Prove that

$$\alpha_1 = -(\beta_1 + \beta_2), \quad \alpha_0 = \beta_1 \beta_2.$$

Problem 46. Let $P \in F[t]$ be given by

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

Define $\mathrm{D}\colon F[t] \to F[t]$ by

$$\mathrm{D}(P) = \sum_{j=1}^{n} j\alpha_j t^{j-1}.$$

(a) Prove that $\mathrm{D}(P+Q) = \mathrm{D}(P) + \mathrm{D}(Q)$.

(b) Prove that $\mathrm{D}(PQ) = \mathrm{D}(P)Q + P\mathrm{D}(Q)$.

Problem 47. For $j > 1$, define $\mathrm{D}^j\colon F[t] \to F[t]$ recursively by $\mathrm{D}^1 = \mathrm{D}$ and $\mathrm{D}^j(P) = \mathrm{D}(\mathrm{D}^{j-1}(P))$. We now assume $F = \mathbf{Q}$.

(a) Prove that $(t-\beta)^2$ divides P if and only if $\mathrm{D}(P)(\beta) = 0$ (i.e. β is a zero of $\mathrm{D}(P)$).

(b) Prove that $(t-\beta)^k$ divides P if and only if $\mathrm{D}^{k-1}(P)(\beta) = 0$.

Problem 48. We say that $P \in \mathbf{C}[t]$ has a **repeated root** if there exists $\beta \in \mathbf{C}$ such that $(t-\beta)^2$ divides P. Prove the following are equivalent:

(a) P has no repeated roots.

(b) $\gcd(P, \mathrm{D}(P)) = 1$.

Problem 49. Prove the following are equivalent:

(a) Every irreducible polynomial $P \in F[t]$ has a root in F. That is $P(\beta) = 0$ for some $\beta \in F$.

(b) For every $n > 0$ and every monic polynomial $Q \in F[t]$ of degree n, there exists $\beta_1, \dots, \beta_n \in F$ such that

$$Q(t) = \prod_{j=1}^{n} (t - \beta_j) = (t-\beta_1)(t-\beta_2)\dots(t-\beta_n).$$

(c) Every irreducible polynomial in $F[t]$ has degree at most 1.

Problem 50. Let $P_1, P_2 \in F[t]$ be monic, irreducible polynomials with $P_1 \neq P_2$. Prove that $\gcd(P_1, P_2) = 1$.

Problem 51. Let F be a field and $P \in F[t]$ with $\deg(P) = n$. We define

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

(a) Prove that if

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

then

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

(b) Prove that $\alpha \neq 0$ 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 with $\deg(P) > 1$ and $P = P_{\mathrm{rec}}$, then $\deg(P)$ is even.

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

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

or

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

for some $\alpha \in F$.

Problem 52. Let $P \in F[t]$ be given by

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

Prove the following are equivalent:

(a) $t - 10$ divides P.

(b) $10^n \alpha_n + 10^{n-1} \alpha_{n-1} + \cdots + 10\alpha_1 + \alpha_0 = 0$

Problem 53. Let $t-1, 2t-1 \in \mathbf{Q}[t]$ be rational polynomials.

(a) Compute $\gcd(t-1, 2t-1)$.

(b) Determine the possible values of $\gcd(n-1, 2n-1)$ for $n \in \mathbf{Z}$.

Problem 54. Let F be a field and let $\psi \colon F[x] \to F$ by defined by

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

where

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

(a) Prove that ψ is a ring homomorphism and onto.

(b) Find the unique irreducible, monic polynomial $P_0 \in F[t]$ such that $\ker(\psi) = \langle P_0 \rangle$ where

$$\langle P_0 \rangle = \{Q \in F[t] \; : \; P_0 \text{ divides } Q\}.$$

Problem 55. Let $P \in F[t]$ be given by

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

Prove the following are equivalent:

(a) $t-1$ divides P.

(b) $\alpha_0 + \alpha_1 + \cdots + \alpha_n = 0$

Problem 56. Let $\psi \colon F[t] \to F$ be a surjective ring homomorphism and let $\mathfrak{a} = \ker \psi$. Prove that there exists a unique monic, degree 1 polynomial $P_{\mathfrak{a}} \in \mathfrak{a}$ such that $\langle P_{\mathfrak{a}} \rangle = \mathfrak{a}$.

Problem 57. Let $P \in \mathbf{Z}[t]$ with

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

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 $\mathbf{Q}$.

Problem 58. 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 $j = 1, \dots, r$.

Problem 59. Let $\psi \colon F[t] \to F$ be a surjective ring homomorphism. Prove that there exists $\beta \in F$ such that

$$\ker(\psi) = \{P \in F[t] \; : \; P(\beta) = 0\}.$$

Problem 60. Let $P_1, P_2 \in F[t]$. Prove that

$$\langle \gcd(P_1, P_2) \rangle = \langle P_1 \rangle \langle P_2 \rangle$$

where the right hand side is the smallest ideal in $F[t]$ containing both P_1, P_2.

Problem 61. Let $p \in \mathbf{N}$ be a prime. Prove that

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

is irreducible in $\mathbf{Q}[t]$.

Problem 62. Let $P \in F[t]$ be given by

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

Prove the following are equivalent:

(a) $t+1$ divides P.

(b) $\alpha_0 - \alpha_1 + \cdots + (-1)^n \alpha_n = 0$