MATH 521A: Abstract Algebra

Preparation for Final Exam

R, S are rings, not necessarily commutative or with identity

F is a field.

1. Carefully define the terms gcd, ring, integral domain, field, $F[x]$, $\mathbb{Z}_n$, irreducible element, prime element, ideal, maximal ideal, prime ideal.

2. Carefully the state the following theorems: division algorithm in $\mathbb{Z}$, division algorithm in $F[x]$, fundamental theorem of arithmetic, remainder theorem, Gauss's lemma, rational root test, Eisenstein's criterion, first isomorphism theorem.

3. Let $a, b, m, n \in \mathbb{N}$, with $\gcd(m, n) = 1$. Prove that the modular system $\{x \equiv a \pmod{m}, x \equiv b \pmod{n}\}$ has a solution, and this solution is unique modulo mn.

4. Prove the division algorithm in $\mathbb{Z}$.

5. Let $a, b, m \in \mathbb{Z}$. Prove that $m \gcd(a, b) = \gcd(ma, mb)$ if and only if (a) $m > 0$; and (b) a, b are not both 0.

6. Let $S \subseteq R$. Prove that S is a subring if and only if (a) $S \neq \emptyset$; and (b) for all $x, y \in S$, $xy \in S$ and $x - y \in S$.

7. Let $a \in R$. Prove that $aR = \{ar : r \in R\}$ is a subring of R.

8. We call $r \in R$ *idempotent* if $r^2 = r$. Suppose R has 1, and let $x \in R$ be idempotent. Prove that $1 - x$ is idempotent.

9. Suppose R is a finite integral domain. Prove that R is a field.

10. Let $\phi : F \to R$ be a ring homomorphism. Prove that either (a) for all $x \in F$, $\phi(x) = 0$; or (b) ϕ is injective.

11. Let $\phi : R \to S$ be a ring isomorphism. Prove that R has an identity if and only if S has an identity.

12. Let $f(x) = x^3 - 6x^2 + x + 4, g(x) = x^5 - 6x + 1$, both in $\mathbb{Q}[x]$. Use the extended Euclidean algorithm to find $\gcd(f, g)$ and to find polynomials s, t such that $\gcd(f, g) = fs + gt$.

13. Define $R \subseteq \mathbb{Z}_2[x]$ via $R = \{f(x) : f(0)f(1) = 0\}$. Prove or disprove that R is a subring.

14. Let $a, b \in F$. Prove that $\gcd(x+a, x+b) = 1$ in $F[x]$ if and only if $a \neq b$.

15. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Suppose there is a prime p where $p|a_1, p|a_2, \ldots, p|a_n$ but $p \nmid a_0$ and $p^2 \nmid a_n$. Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

16. Set $f(x) = x^2 + 2 \in \mathbb{Z}_4[x]$. Prove that $f(x)$ is irreducible, and not prime.

17. Let $p(x) \in F[x]$. Prove that $p(x)$ is irreducible if and only if the ideal $(p(x))$ is maximal in $F[x]$.

18. Prove that (n) is a prime ideal of $\mathbb{Z}$, if and only if n is either prime or zero.

19. Construct a field with nine elements, and list all the elements.

20. Let $f(x), p(x) \in F[x]$, with $\gcd(f(x), p(x)) = 1$. Prove that there is some $g(x) \in F[x]$ such that $f(x)g(x) \equiv 1 \pmod{p(x)}$.

21. Find the equivalence classes and rules for addition and multiplication in $\mathbb{Q}[x]/(x^2 - 1)$. Find all the units and zero divisors.

22. Set $I = \{a_0 + a_1 x + \cdots + a_n x^n : a_0 + a_1 + \cdots + a_n = 0\}$. Prove that this is an ideal of $F[x]$, and principal.

23. Let $R = \mathbb{Z}[x]$, $I = (x - 1)$. Prove that I is prime, and not maximal.

24. Let $R = \mathbb{Z}[x]$, p prime. Let $I = \{pa_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_i \in \mathbb{Z}\}$. Prove that I is an ideal, and maximal.