REVIEW FOR THE SECOND MIDTERM.

ALIREZA SALEHI GOLSEFIDY

1. Some of the concepts that you have to know!

PID, PIR, maximal and prime ideals, field of quotient, irreducible and prime elements, content of a polynomial.

2. Some of the theorems that you have to know!

(1) (a) In a commutative unital ring R, I is a maximal ideal if and only if R/I is a field.
    (b) In a commutative unital ring R, I is a prime ideal if and only if R/I is an integral domain.
    (c) In a commutative unital ring a maximal ideal is always prime.
(2) Division algorithm in $F[x]$ where F is a field.
(3) (a) Let F be a field and I be an ideal in $F[x]$. If $f(x)$ is a polynomial of smallest degree in I, then $I = \langle f(x) \rangle$.
    (b) $F[x]$ is a PID if F is a field.
    (c) $\mathbb{Z}[x]$ is not a PID.
(4) Remainder theorem.
(5) Factor theorem.
(6) A non-zero polynomial of degree n over a field F has at most n zeros in F (with multiplicity).
(7) Evaluation map and results similar to $\mathbb{Q}[x]/\langle x^2+1 \rangle \simeq \mathbb{Q}[i]$.
(8) A polynomial $f \in F[x]$ is maximal if and only if $\langle f \rangle$ is a maximal ideal if and only if $F[x]/\langle f \rangle$ is a field.
(9) (Irreducibility of degree 2 and 3 polynomials over a field) Let F be a field and let $f(x)$ be polynomial of degree 2 or 3 in $F[x]$. Then $f(x)$ is irreducible over F if and only if f has no zero over F.
(10) (Gauss's lemma) Let $f, g \in \mathbb{Z}[x]$. Then $c(fg) = c(f)c(g)$.
(11) (Irreducibility over $\mathbb{Z}$ and $\mathbb{Q}$)
    (a) Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is also reducible over $\mathbb{Z}$.
    (b) Let $f(x) \in \mathbb{Z}[x]$ be a primitive polynomial. Then $f(x)$ is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$.
(12) (Irreducibility test) Let $f(x) \in \mathbb{Z}[x]$ and p be a prime. If $f(x)$ modulo p has the same degree as $f(x)$ and it is irreducible over $\mathbb{Z}/p\mathbb{Z}$, then $f(x)$ is irreducible over $\mathbb{Q}$.

3. Some of the conceptual problems that you have to know!

(1) (Rational root theorem) Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and $a_n \neq 0$. Prove that if r and s are coprime and $f(r/s) = 0$, then $r|a_0$ and $s|a_n$.
(2) (Construct finite fields) If $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ is an irreducible polynomial of degree n, then $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$ is a field of order p^n.
(3) Let p be a prime. Then
    (a) $x^p - x = x(x-1)\cdots(x-p+1)$, as two polynomials over $\mathbb{Z}/p\mathbb{Z}$.
    (b) For any positive integer k, $(x+1)^{p^k} = x^{p^k} + 1$ as two polynomials over $\mathbb{Z}/p\mathbb{Z}$.

Date: 2/29/2012.

(4) Let F be a field. For two non-zero polynomials $f(x), g(x) \in F[x]$, let $\gcd(f(x), g(x))$ be a monic polynomial of largest degree which divides both $f(x)$ and $g(x)$. Prove that there are polynomials $p(x), q(x) \in F[x]$ such that

$$\gcd(f(x), g(x)) = p(x)f(x) + q(x)g(x).$$

(5) How to find the number of solutions of $x^k - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$, where p is a prime.
(6) A non-zero homomorphism from a field to another ring is injective.

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu