Outline

See “Prelim Workshop Lectures Notes” for review of basic definitions. (S85 14, F06 4A)

Fields $\subseteq$ Euclidean Domains $\subseteq$ PIDs $\subseteq$ UFDs $\subseteq$ integral domains (S03 9A, 6.10.5, 6.10.15)

- Using a Euclidean algorithm to determine gcd and remainder. Examples such as $\mathbb{Z}$, $k[x]$ where $k$ a field, and the Gaussian integers.
- Prime and maximal ideals. Characterization by quotients. Prime ideal is maximal in PID.
- Local rings. A ring is local iff the set of non-units forms an ideal.
- An element is prime $\leftrightarrow$ irreducible in UFD. Only $\rightarrow$ in general integral domain.
- Quadratic integer rings

Polynomials (F05 4A, 6.11.2, 6.11.9, 6.11.24, 6.11.28)

- Euclidean algorithm for $k[x]$ when $k$ a field. In $R[x]$ for general $R$, can use division algorithm to divide by $f(x)$ when leading coefficient of $f$ is a unit.
- Formulas for coefficients in terms of roots (“Vieta’s formulas”)
- Cyclotomic polynomials/irreducible factorization of $x^n - 1$
- Rational root theorem
- Gauss’ lemma
- Proving irreducibility of polynomials: Eisenstein’s criterion. Show irreducibility over $\mathbb{Z}_p[x]$ for any prime $p$ that does not divide leading coefficient. Substitute $x$ for $x + \alpha$ for some $\alpha$ and consider the resulting polynomial. If degree 2 or 3: reducible polynomial must have a root in the underlying ring. If degree 4: assume factorization into quadratic polynomials with undetermined coefficients, show there is no solution (and also check no root).

Problems

Spring 1985 14 Let $F$ be a field and let $M_n(F)$ be the ring of $n \times n$ matrices with coefficients in $F$. Prove that $M_n(F)$ has no nontrivial (two-sided) ideals. What can you conclude about ring homomorphisms from $M_n(F)$?

Spring 2003 9A Let $R$ be the set of complex numbers of the form

$$a + 3bi, \ a, b \in \mathbb{Z}.$$ 

Prove that $R$ is a subring of $\mathbb{C}$, and that $R$ is an integral domain but not a unique factorization domain.
Fall 2005 4A. Let $m$ and $n$ be positive integers. Prove that the ideal generated by $x^m - 1$ and $x^n - 1$ in $\mathbb{Z}[x]$ is principal.

Fall 2006 4A. Let $R$ be a finite commutative ring with unity which has no zero-divisors and contains at least one element other than 0. Prove that $R$ is a field.

6.10.5 Let $F$ be a field and $X$ a finite set. Let $R(X, F)$ be the ring of all functions from $X$ to $F$, endowed with pointwise operations. What are the maximal ideals of $R(X, F)$?

6.10.15 Let $R$ be a principal ideal domain and let $I$ and $J$ be nonzero ideals. Show that $IJ = I \cap J$ if and only if $I + J = R$.

6.11.2 By the fundamental theorem of algebra, the polynomial $x^3 + 2x^2 + 7x + 1$ has three complex roots, $\alpha_1, \alpha_2$ and $\alpha_3$. Compute $\alpha_1^3 + \alpha_2^3 + \alpha_3^3$.

6.11.9 Let $I$ be the ideal in $\mathbb{Z}[x]$ generated by 5 and $x^3 + x + 1$. Is $I$ prime?

6.11.24 Let $f_n(x) = x^{n-1} + x^{n-2} + \ldots + x + 1$. Show that $f_n(x)$ is irreducible in $\mathbb{Q}[x]$ if $n$ is prime. What if $n$ is composite?

6.11.28 Factor $x^4 + x^3 + x + 3$ completely in $\mathbb{Z}_5[x]$. 