Coding theory.

1. Introduction. This chapter covers some topics in coding theory. Overlap with other introductions to coding theory, such as [MacWilliams and Sloane] or [van Lint], is kept to a minimum. Facts from algebra which are required may be found in "Introduction to Algebra, Topology, and Category Theory" [Dowd]; references will be given in the form D.N.M, where N is the chapter number and M is the item (section, theorem, etc.) number.

As in [Dowd], if S is a set then S^c denotes its complement, and for finite S Card(S) denotes the cardinality. Isomorphism will be denoted using $\cong$.

2. Codes. Let $\mathcal{A}$ be a finite alphabet; and for a positive integer n let $\mathcal{A}^n$ denote the set of n-tuples of element of $\mathcal{A}$. A code is simply a subset of $\mathcal{A}^n$. Such codes are sometimes called "block codes", to distinguish them from other varieties. The cardinality of $\mathcal{A}$ is frequently denoted q, and the code is called q-ary (binary for q=2, ternary for q=3, quaternary for q=4). Binary codes have traditionally been of special interest, and remain so. Indeed, applications to binary codes is one reason for considering other q.

As a notational convention, i, j, etc., generally denote coordinate positions, i.e., $1 \leq i \leq n$. Also, v, w, etc., generally denote codewords, i.e., vectors in $\mathcal{A}^n$. As usual, v_i denotes the element of $\mathcal{A}$ in position i of v.

For binary codes, $\mathcal{A}$ may be considered as the field $\mathcal{Z}_2$ of the integers mod 2. The imposition of various algebraic structure on $\mathcal{A}$ leads to various topics of interest. From hereon $\mathcal{A}$ will be a finite ring. This in fact results in no loss of generality, since $\mathcal{A}$ can always be considered to be $\mathcal{Z}_q$, the finite ring of the integers mod q. Some facts have been observed in the case that $\mathcal{A}$ is any Abelian group, however.

Interest in codes over a finite ring has intensified since the early 1990's, when some important applications were discovered (see [Hammons et al]). The theory of finite rings is of interest in itself. Another important specific ring is the finite field of order q, which will be denoted $\mathcal{F}_q$.

$\mathcal{A}^n$ will be considered to be the standard n-dimensional $\mathcal{A}$-module, the operations of addition and scalar multiplication being componentwise. This is the "free $\mathcal{A}$-module on n generators" over $\mathcal{A}$. In the noncommutative case, scalar multiplication is written on the left.

A code $C \subseteq \mathcal{A}^n$ is said to be linear if it is a submodule of $\mathcal{A}^n$, that is, if C is closed under addition and left scalar multiplication. Linear codes are of interest for a variety of reasons, both in mathematical coding theory and engineering applications. Note that when $\mathcal{A}$ is $\mathcal{Z}_q$, an additive subgroup of $\mathcal{A}^n$ is already a linear code.

3. Types of finite rings. In coding theory the most important finite rings are $\mathcal{F}_q$ (which requires that q be a prime power) and $\mathcal{Z}_q$ (in fact for q a prime power). There is a class of rings which includes both, namely the Galois rings $\mathcal{GR}(q, n)$ for a q a prime power and n a positive integer. This is an extension of $\mathcal{Z}_q$ having properties which make it the unique extension with these properties. $\mathcal{Z}_q$ is $\mathcal{GR}(q, 1)$, and $\mathcal{F}_q$ is $\mathcal{GR}(p, r)$ where $q = p^r$.

The Galois rings are important in the structure theory of finite commutative rings. Any finite commutative ring has a unique decomposition as a direct sum of finite local commutative rings. If R is a finite local commutative ring of characteristic q (we will see below that q is a prime power) then R contains a largest Galois extension T of $\mathcal{Z}_q$ (called the coefficient ring), and R is a homomorphic image of a multivariable polynomial ring over T. See [McDonald] or [Bini and Flamini] for proofs of these statements; some facts will be proved below.

More recently, several authors (for example [Day and Rajan]) have considered Galois rings in the context of coding theory. Other classes of finite rings have also been considered, both commutative and noncommutative; these developments are still underway, and represent advances in the theory of finite rings and modules over them.

The Galois rings are in the class of rings known as commutative finite chain rings. Finite chain rings are discussed in [Clark and Drake]. Some authors (for example [Honald and Landjev]) consider codes over arbitrary finite chain rings, and some (for example [Norton and Salagean]) over only commutative ones.

Finite chain rings are in the class known as finite Frobenius rings. Codes over these are considered for example in [Wood].

The ring $\mathcal{Z}_m$ is an example of a principal ideal ring, a ring where every left and right ideal is principal, where a principal left (right) ideal is Ra (aR) for some a. Various classes mentioned above, for example finite chain rings, are principal ideal rings.

In this section some basic facts concerning rings and polynomials over them will be reviewed. Sections 4 to 6 will consider specific types of finite rings. The notation (f) for the principal ideal generated by f in a commutative ring R will be used. We stick with the convention of [Dowd 06] and use $[IJ]$ to denote the ideal product. More generally, for an R-module M $[IM]$ denotes the submodule of M generated by $\{im : i \in I, m \in M\}$.

If R is a commutative ring and $f \in R[x]$, then $R[x]/(f)$ is a ring, and an R-module. Suppose f is monic, and let n denote the degree of f. Since f is monic, by the division law for polynomials over a ring (section D.28.3), every coset of (f) contains a polynomial ρ of degree less than n. Also, since multiplying a monic polynomial by any polynomial cannot decrease its degree, it follows that each coset contains only one such ρ. It follows that $R[x]/(f)$ is isomorphic as an R-module to the free R-module R^n; the map taking $\langle r_0, r_1, \ldots, r_{n-1}\rangle$ to $r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} + (f)$ is an $\mathcal{R}$-module homomorphism, which is surjective and injective.

Recall the following basic facts.

- For an ideal I in a commutative ring R, R/I is a field iff I is a maximal ideal (theorem D.6.3).
- In a principal ideal domain R, the ideal pR is prime iff p is irreducible, in which case pR is maximal (so a principal ideal domain has dimension 1) (theorem D.6.5).
- If F is a field then $F[x]$ is a principal ideal domain (theorems D.7.3 and D.6.5).

Thus, for monic $f \in \cap F_p[x]$, $\mathcal{F}_p[x]/(f)$ is a finite field with p^n elements iff f is an irreducible polynomial of degree n.

There are irreducible polynomials of degree n over $\mathcal{F}_p$. Indeed, with $q = p^n$, $\mathcal{F}_q$ is the splitting field of $x^q - x$ over $\mathcal{F}_p$ (section D.9.6); in particular it exists (and $\mathcal{F}_q$ does not depend on f). Considering all polynomials of degree n over $\mathcal{F}_p$, at least one must be irreducible. An alternative proof uses the explicit expression $(1/n)\sum_{d|n}\mu(n/d)q^d$ (lemma D.9.7) for the number N of irreducble polynomials over $\mathcal{F}_q$. Replacing $\mu(n/d)$ by -1 for $d < n$, $N \geq (1/n)(q^n - (q^n - q)/(q-1)) > 0$.

If Ra is a principal left ideal in a ring R and $a \mapsto \bar{a}$ is an epimorpism from R to a ring S then $S\bar{a}$ is the image of Ra under the epimorphism. It follows that a quotient of a principal ideal ring is a principal ideal ring. In particular, $\mathcal{Z}_m$ for any m is a principal ideal ring. Indeed, any nonzero ideal in $\mathcal{Z}_m$ equals $\mathcal{Z}_m a$ where a is the smallest nonzero element of the ideal; also a is a divisor of m. These facts may be readily seen using the division law in $\mathcal{Z}$, and are left to the reader.

It is also readily verified that if a and b are divisors of m then $\mathcal{Z}_m a \subseteq \mathcal{Z}_m b$ iff $b|a$. The maximal ideals of $\mathcal{Z}_m$ are the ideals $\mathcal{Z}_m a$ where a is a prime divisor of m.

Recall that a commutative ring R is said to be local if it has a unique maximal ideal (section D.20.3); letting M denote the ideal, the field R/M is called the residue class field. By foregoing remarks, $\mathcal{Z}_m$ is a local ring iff m is a prime power $q = p^r$. In this case, the residue class field is $\mathcal{F}_p$; the nonzero ideals are the ideals $\mathcal{Z}p^i$ for $0 \leq i \leq r$.

In any commutative ring R, the nilpotent elements form an ideal (section D.20.8); thus in a local ring they are all contained in the maximal ideal M. If R is also finite the converse is true. Suppose $a \in M$; since R is finite $a^i = a^j$ for some $i > j$, whence $a^j(a^{i-j} - 1) = 0$. But $a^{i-j} - 1$ is a unit (theorem D.20.5), so

$a^j = 0$.

In a finite ring R, the additive subgroup generated by 1 is a subring (indeed $m1 \cdot n1 = (mn)1$), and is a copy of $\mathcal{Z}_n$ for some n, which is the characteristic of R (section D.6.2). If R is a local commutative ring, with maximal ideal M and residue class field of order $q = p^r$ where p is prime, then $p^r 1 \in M$, so $p^{rs}1 = 0$ for some s. It follows that the characteristic of R is a prime power.

Suppose R is a commutative ring, M is an R-module, and K, L are submodules. The set $\{k+L : k \in K\}$ is readily seen to equal $(K+L)/L$. If $J \subseteq R$ is an ideal, then $[J(M/L)]$ is readily seen to equal $\{k+L : k \in [JM]\}$; thus, $J[M/L] = ([JM]+L)/L$.

Nakayama's lemma (theorem D.16.23) states that if R is a commutative ring, $J \subseteq \mathrm{Rad}(R)$ is an ideal, M is a finitely generated R-module, and $[JM] = M$, then $M = 0$. As a corollary, if $L \subseteq M$ is a submodule, and $M = [JM] + L$, then $L = M$. Indeed, $[J(M/L)] = ([JM]+L)/L = M/L$, so M/L is 0; that is, $L = M$.

In a commutative ring, suppose u is a unit, and a is nilpotent. Let k be least such that $a^k = 0$; then $\sum_{i=0}^{k-1}(-1)^i u^{i+1}a^i$ is readily seen to be a multiplicative inverse for $u+a$, showing that $u+a$ is a unit.

The following three lemmas give useful characterizations of the units, zero divisors, and nilpotent elements in $R[x]$ for a commutative ring R.

Lemma 1. A polynomial $f = \sum_{i=0}^{n} a_i x^i$ is a unit in $R[x]$ iff a_0 is a unit in R and a_i for $i > 0$ is nilpotent.

Proof: Suppose a_0 is a unit and a_i for $0 < i \le n$ is nilpotent. Consider the recursion

$$b_0 = a_0^{-1}, \quad b_k = -a_0^{-1} \sum_{1 \le l \le k} a_l b_{k-l}.$$

Each b_i may be written as a sum of terms $a_0^{-t}\mathbf{a}^\nu$ where $\mathbf{a}^\nu$ is a monomial in the values a_i for $0 < i \le n$. After b_n, the minimum total weight of the monomials increases. It follows that eventually the terms all become 0. The polynomial $\sum_k b_k x^k$, up to a sufficiently high degree, is then a multiplicative inverse for f. Conversely suppose $g = \sum_k b_k x^k$ is a multiplicative inverse for f, where f has degree n and g has degree m. Then $a_0 b_0 = 1$, so a_0 is a unit. We claim that if $n > 0$ then a_n is nilpotent in R. Given this, $a_n x^n$ is nilpotent in $R[x]$, so by an observation preceding the lemma, $\sum_{i=0}^{n-1} a_i x^i$ is a unit in $R[x]$, and it follows inductively that a_i is nilpotent for $i > 0$. To prove the claim, we prove by induction that $a_n^{r+1} b_{m-r} = 0$ for $0 \le r \le m$; since b_0 is a unit, $a_n^{m+1} = 0$. The basis $r = 0$ follows from $fg = 1$. For the induction step, $f^{r+1}g = f^r$. The coefficient of $x^{(r+1)n+(m-r)}$ in f^r is 0, and in $f^{r+1}g$ is $a_n^{r+1}b_{m-r}$ plus terms which are 0 by induction.

Lemma 2. A polynomial f is a zero divisor in $R[x]$ iff $af = 0$ for some $a \in R$.

Proof: One direction is trivial. For the other, let g be of least degree such that $fg = 0$, where f has degree n and g has degree m. We claim that, with $f = \sum_i a_i x^i$, $a_{n-r}b_m = 0$, and $a_{n-r}g = 0$, inductively on r. Clearly $a_n b_m = 0$; but then $a_m g$, being a polynomial of degree less than m which annihilates f, must be 0. Inductively, $a_{n-r}b_m$ equals 0 becasue it is the coefficient of the leading term, after terms known to be 0 are dropped; and $a_{n-r}g = 0$ follows as before. Thus, $a_0 g = 0$, from which it follows that g is a constant.

Lemma 3. A polynomial $f = \sum_{i=0}^{n} a_i x^i$ is nilpotent in $R[x]$ iff a_i is nilpotent in R for all i.

Proof: If f is nilpotent then $1+f$ is a unit, so by lemma 1 a_i is nilpotent for $i > 0$; a_0 is nilpotent also, since $a_0^t = 0$ if $f^t = 0$. If each a_i is nilpotent, the jth power of f is a sum of terms, each of whose coefficients is a product of j coefficients of f, so for j suffiuciently large they are all 0.

4. Galois rings. In this section we let R denote a local finite commutative ring, with maximal ideal M and residue class field K. We let $a \mapsto \bar{a}$ denote the canonical epimorphism from R to K; and $f \mapsto \bar{f}$ its extension, mapping to $R[x]$ to $K[x]$. As noted in section 3, M is the set of nilpotent elements of R; it is also the set of zero-divisors, since if $a \notin M$ then a is a unit.

Let $M[x]$ denote the ideal of polynomials, all of whose coefficients are in M. Note that it is the ideal in $R[x]$ generated by M, and the inverse image of 0 under $f \mapsto \bar{f}$. It is also the ideal of zero divisors: By

lemma 2 if f is a zero divisor there is an $a \in R$ such that $af = 0$. Each coefficient of f must thus be a zero divisor in R, whence in M; that is, $f \in M[x]$. Finally, by lemma 3 each $f \in M[x]$ is nilpotent.

For $f \in R[x]$, the ideal $M[x] + (f)$ (or equivalently $M + (f)$) is those polynomials which differ from a multiple of f by a polynomial in $M[x]$. Clearly, given f there is a monic g with $M + (f) = M + (g)$; simply drop leading terms of f until the leading coefficient is a unit, and multiply by the inverse of the unit.

Lemma 4. An ideal $N \subseteq R[x]$ is maximal iff it is of the form $M + (f)$ where $f \in R[x]$ is monic and $\bar{f}$ is irreducible.

Proof: Let N be a maximal ideal. Since $1 \notin N$, $N \cap R$ is proper, whence $N \cap R \subseteq M$. If there were $a \in M - (N \cap R)$ then a could be added to N; so $N \cap R = M$. Now, $\bar{N}$ is maximal in $K[x]$, so, $\bar{N} = (\bar{f})$ in $K[x]$, where $f \in N$. Thus, $M + (f) \subseteq N$; further f may taken as monic. If $g \in N$ then $\bar{g} = \bar{h}\bar{f}$ for some $h \in R[x]$, and $\overline{g - hf} = 0$, so $g - hf \in M[x]$, so $g \in M + (f)$. Since R is finite it is Noetherian, whence $R[x]$ is Noetherian (theorem D.7.9). An ideal $M + (f)$ with f monic and $\bar{f}$ irreducible must be contained in some maximal ideal $M + (f')$ where also f' is monic and $\bar{f}'$ is irreducible. Then $\bar{f}' | \bar{f}$, so since $\bar{f}$ is irreducible, $\bar{f}' = \bar{f}$.

For the rest of the section, $S \supseteq R$ denotes an extension of R, which is a finite local commutative ring, with maximal ideal N and residue class L. Since S is a finitely generated R-module, and R is local, by Nakayama's lemma, $[MS]$ is proper, whence $M \subseteq [MS] \subseteq N$, by the maximality of N. It follows that the map $r + M \mapsto r + N$ is a well-defined homomorphism from K to L (section D.20.7).

Lemma 5. The map $r + M \mapsto r + N$ is injective.

Proof: Clearly $M \subseteq R \cap N$. There are $x, y \in R - M$ such that $xy = 1$ (theorem D.20.5). If $R \cap N$ is not proper then $R \subseteq N$, whence $x, y \in N$, a contradiction (theorem D.20.5). Since $R \cap N$ is proper and M is maximal, $R \cap N \subseteq M$, and so $R \cap N = M$ (N lies above M). The lemma follows (section D.20.7).

If $[MS] = N$ the extension $S \supseteq R$ is said to be unramified. This need not be the case. Suppose $R = \mathcal{Z}_2$, and consider $S = R[x]/(f)$ in the two cases $f = x^2 + x + 1$ and $f = x^2 + 1$. In the first case, f is irreducible and $S = \mathcal{F}_4$. In the second case, S is $\mathcal{Z}_4$ (the isomorphism takes x to 3 and $x + 1$ to 2). S has the unique nonzero proper ideal $N = \{0, x + 1\}$ and is a local ring; but $[MS] = 0$. A notion of separability can be defined for extensions of this type; and an extension shown to be separable iff it is unramified. We omit further discussion, and refer the reader to [McDonald].

K may be considered a subfield of L by ignoring the embedding $r + M \mapsto r + N$. The map $a \mapsto \bar{a}$ from S to N restricts to the map from R to M,

Lemma 6. If f is monic and $\bar{f}$ is irreducible then $R[x]/(f)$ is local and unramified over R.

Proof:

$$\frac{R[x]/(f)}{(M + (f))/(f)} \cong \frac{R[x]}{M + (f)} \cong \frac{K[x]}{(\bar{f})}$$

(section D.6.2). Writing S and N for the numerator and denominator of the first quotient, S/N is a field, so N is a maximal ideal. Also, $[MS] = M[x]/(f) = (M + (f))/(f) = N$. If J is any maximal ideal in S then J corresponds to a maximal ideal of $R[x]$ which contains (f) (section D.6.2); let this be $M + (f')$, as in lemma 4. By an argument in the proof of lemma 4, $\bar{f}' = \bar{f}$. Thus, S is local; and we have already shown that the extension is unramified.

As observed in section 3, for any n there is an irreducible polynomial ϕ of degree n over K; it may assumed to be monic. Since $K[x]/(\phi)$ is a finite field with cardinality $\mathrm{Card}(K)^n$ it is isomorphic to L. Let f be any monic polynomial in $R[x]$ with $\bar{f} = \phi$. By the lemma, $R[x]/(f)$ is an unramified local commutative extension of R, with n the dimension of L over K; it will be seen below that it is unique.

Lemma 7. If $S \supseteq R$ is unramified then $S = R[a]$ for some $a \in S$.

Proof: Extensions of finite fields are separable (section D.9.6), and by lemma 5 L can be considered an extension of K, so there is an $\alpha \in L$ so that $L = K[\alpha]$ (theorem D.9.2). By hypothesis, then, there is a coset

$a + [MS]$ where $a \in S$, which generates $S/[MS]$ over $(R + [MS])/[MS]$). It follows that $S = R[a] + [MS]$. The lemma follows by Nakayama's lemma, as noted in section 3.

Note that the proof shows that if $K[\bar{a}] = L$ then $K[a] = S$. To simplify the notation, let M^i denote the ideal $[M^i]$, with $M^0 = R$. By Nakayama's lemma, of $M^i = M^{i+1}$ then $M^i = 0\text{m}$ and it follows that the ideal M^i form a strictly descending chain, which in a finite ring eventually becomes 0, say when $i = t$. For any $i > 0$ there is a canonical epimorphism $R/M^i \mapsto R/M^{i-1}$. The kernel is M^{i-1}/M^i. It is readily verified that $\text{Card}(R) = \prod_{i=1}^{t} \text{Card}(M^{i-1}/M^i)$.

Lemma 8. If $S \supseteq R$ is unramified and the dimension of L over K is n then $\text{Card}(S) = \text{Card}(R)^n$.

Proof: By the remarks preceding the lemma, it suffices to show that for $i > 0$, $\text{Card}(N^{i-1}/N^i) = \text{Card}(M^{i-1}/M^i)^n$. Letting $(r+M)(x+M^i) = rx+M^i$ for $r \in R$ and $x \in M^{i-1}$, yields a well-defined action of R/M on M^{i-1}/M^i, since $rx \in M^i$ if $r \in M$. Suppose $\{x_1+M^i, \ldots, x_l+M^i\}$ is a basis for the vector space M^{i-1}/M^i over R/M; we claim that it is also a basis for N^{i-1}/N^i over S/N, proving the theorem. Since ideal multiplication is associative, (section D.6.6), $N^{i-1} = [SM^{i-1}]$. Thus, given $y \in N^{i-1}$, $y = \sum_j s_j m_j$ where $s_j \in S$, $m_j \in M^{i-1}$. So $y + M^i = \sum_j \sum_k s_j x_k + M^i$, and $y + N^i = \sum_j \sum_k s_j x_k + N^i$.

Suppose R/M is isomorphic to $\mathcal{F}_q$. From the proof, it follows that $\text{Card}(M^{i-1}/M^i)$ is a power of q, whence $\text{Card}(R)$ is. In particular, the order of a finite commutative local ring is a prime power.

Theorem 9. If $S \supseteq R$ is unramified then $S = R[x]/(f)$ where f is monic and $\bar{f}$ is irreducible.

Proof: Let a be such that $S = R[a]$; then $L = K[\bar{a}]$. Let $f \in R[x]$ be monic, with $\bar{f}$ the minimal polynomial (section D.10.4) of $\bar{a}$ over K. Letting $n = \deg(f)$, n is the degree of $\bar{f}$, and the dimension of L over K. Let $Q = \{g(a) : g \in R[x], \deg(g) < n\}$. If $s = h(a)$ for some $h \in R[x]$, then by the division law for polynomials over a ring, $h = fh_1 + h_2$ where $\deg(h_2) < n$. It follows that as R-modules, $R[a] = Q + [MS]$. By Nakayama's lemma, $R[a] = Q$. In particular, $f(a) = g(a)$ for some $g \in R[x]$ with $\deg(g) < n$. Since $\overline{f(a)} = 0$, the coefficients of g must be in M, else $\bar{a}$ satisfies a nonzero polynomial of degree less than n. Let $f_2 = f - g$; then f_2 is monic, and $\bar{f}_2 = \bar{f}$ whence $\bar{f}_2$ is irreducible. Further $f_2(a) = 0$; thus, the evaluation map (section D,7.2) $f \mapsto f(a)$ from $R[x]$ to $R[a]$ yields a ring epimorphism $R[x]/(f_2) \mapsto R[a]$. By remarks in section 3, $\text{Card}(R[x]/f_2) = \text{Card}(R)^n$. By lemma 8, it follows that the epimorphism is an isomorphism.

Note that, with a and n as in the proof, S is freely generated over R by $1, a, \ldots, a^{n-1}$. This follows by lemma 8.

Theorem 10. If $S1, S_2 \supseteq R$ are unramified, with the same L, then there is an isomorphism $\sigma : S_1 \mapsto S_2$ fixing R pointwise.

Proof: Let $\alpha \in L$ be such that $L = K[\alpha]$. Let $a_i \in S_i$ be such that $\bar{a}_i = \alpha$. Then $S_i = R[a_i]$; indeed, as observed above S is freely generated by $\{1, \ldots, a^{n-1}\}$, where L is n dimensional over K. It follows that there is a (unique) σ with $\sigma(a_1) = a_2$.

Recall that in a commutative ring R, ideals I and J are comaximal if $I + J = R$ (section D.6.6). For principal ideals (f) and (g), this is clearly so iff there are $r, s \in R$ with $rf + sg = 1$; and in a principal ideal domain such as $K[x]$ this is so iff f and g are relatively prime (section D.6.3).

In the case of a finite local commutative ring, (f) and (g) are comaximal iff $(\bar{f})$ and $(\bar{g})$ are. Indeed, if $rf + sg = 1$ then $\bar{r}\bar{f} + \bar{s}\bar{g} = 1$; and if $\bar{r}\bar{f} + \bar{s}\bar{g} = 1$ then $rf + sg = 1 + m$ where $m \in M[x]$, and since m is nilpotent $1 + m$ is a unit, as observed in section 3.

Lemma 11. For R a finite local commutative ring, suppose $\bar{f} = \gamma_1\gamma_2$ where $f \in R[x]$, $\gamma_1, \gamma_2 \in K[x]$, and γ_1, γ_2 are relatively prime. Then there are $g_1, g_2 \in R[x]$ with $f = g_1 g_2$ and $\bar{g}_i = \gamma_i$ for $i = 1, 2$.

Proof: Polynomials h_{i1}, h_{i2} will be defined, such that $\bar{h}_{ij} = \gamma_j$ for $j = 1, 2$, and $f = h_{i1}h_{i2} + m$ where $m \in M^{2^i}[x]$. For $i = 0$, choose any h_{01}, h_{02} with $\bar{h}_{0j} = \gamma_j$ for $j = 1, 2$. Inductively, choose $\lambda_1, \lambda_2 \in R[x]$ with $\lambda_1 h_{i1} + \lambda_2 h_{i2} = 1$, and set $h_{i+1,1} = h_{i1} + \lambda_2 m$ and $h_{i+1,2} = h_{i2} + \lambda_1 m$. Then $\bar{h}_{i+1,j} = \gamma_j$ for $j = 1, 2$; and $h_{i+1,1}h_{i+1,2} = f + \lambda_1\lambda_2 m^2$.

Lemma 12. Suppose $f \in R[x]$ is such that $\bar{f}$ is not the zero polynomial. Then there are a monic $f_m \in R[x]$, a unit $a \in R$, and $g \in M[x]$, such that $f = (1+g)af_m$.

Proof: Let n be the degree of $\bar{f}$. For $g \in R[x]$ let g_i denote the coefficient of x^i. For $j \geq 1$ we construct$f_j \in R[x]$ and $g_j \in M[x]$, $h_j \in M^j[x]$, such that $\deg(f_j) = n$, $f_{jn}$is a unit, and $f = (1+g_j)f_j + h_j$. By hypothesis $f = f_1 + h$ where the leading coefficient of f_1 is a unit and $h \in M[x]$; let $g_1 = 0$ and $h_1 = h$. Inductively, by the division law for polynomials in $R[x]$, h_j can be written as $qf_j + r$ where $\deg(r) < n$. Let $f_{j+1} = f_j + r$, $g_{j+1} = g_j + q$, and $h_{j+1} = -(g_j + q)r$; then $\deg(f_{j+1}) = n$, $f_{j+1,n}$is a unit, and $f = (1+g_{j+1})f_{j+1} + h_{j+1}$. Since $h_a = \sum_{b+c=a} q_b f_{j,c}$ for $a \geq n$, $h_a \in M^j$, and f_{jn} is a unit, it follows inductively for $a = \deg(q), \ldots 0$ that $q_a \in M^j$. It then follows that $r = h_j - qf_j$ is in M^j also. It now follows that $g_{j+1} \in M$ and $h_{j+1} \in M^{j+1}$. Now choose j large enough that $M^j = 0$, so $f = (1+g_j)f_j$. Let $a = f_{jn}$, $f_m = a^{-1}f_j$, and $g = g_j$.

Recall that the multiplicity of a root a of a polynomial $f \in K[x]$ is the highest power of $x - a$ which divides f. Roots of irreducible polynomials over a finite field have multiplicity 1 (section D.9.6).

Lemma 13. Suppose $f \in R[x]$ is monic, and $\alpha \in L$ is a root of $\bar{f}$ of multiplicity 1. Then there is a unique $a \in S$ with $\bar{a} = \alpha$ and $f(a) = 0$.

Proof: By hypothesis $\bar{f} = (x - \alpha)\gamma$ where $x - \alpha$ and γ are relatively prime. By lemma 11, $f = (x - a_1 + m)g_1$ where $\bar{a}_1 = \alpha$, $\bar{g}_1 = \gamma$, and $m \in M[x]$. By lemma 12 there are $a \in R$ and u a unit in $R[x]$, such that $\bar{a} = \bar{a}_1$ and $x - a_1 + m = u(x - a)$. Let $g = ug_1$; then $f = (x - a)g$, whence $f(a) = 0$. If also $f(a_2) = 0$ and $\bar{a}_2 = \alpha$ then $0 = f(a_2) = (a_2 - a)g(a_2)/$ But $\overline{g}(a_2) = \bar{g}(\alpha)$, and $\bar{g}(\alpha) \neq 0$, so $g(a_2) \notin M$, so $g(a_2)$ is not a zero divisor, so $a_2 = a$.

Theorem 14. Suppose $S \supseteq R$ is unramified, and $T \subseteq R$ is some other finite local commutative extension, where the residue class field is also L. Suppose $\tau : L \mapsto L$ is an automorphism fixing K pointwise. Then there is a unique homomorphism $\sigma : S \mapsto T$ fixing R pointwise, which induces τ. Further, τ is an isomorphism iff T is an unramified extension of R.

Proof: Choose $\alpha \in L$ and a monic $f \in R[x]$, with $L = K[\alpha]$ and $\bar{f}$ the minimal polynomial of α (section D.9.1). By lemma 12 there is a unique $a \in S$ with $\bar{a} = \alpha$ and $f(a) = 0$. By remarks after theorem 9, $S = K[a]$, and in fact S is freely generated by $1, a, \ldots, a^{n-1}$ where n is the degree of f. Suppose $\tau(\alpha) = \beta$; since τ fixes K, $\bar{f}(\beta) = \bar{f}(\alpha) = 0$; and also $L = K[\beta]$. Again by lemma 13, there is a unique $b \in T$ with $\bar{b} = \beta$. A homomorphsim $\sigma : S = R[a] \mapsto T$ which fixes R is determined, where $\sigma(a) = b$. Further, for $s \in S$, $\overline{\sigma(s)} = \tau(\bar{s})$, since this holds for $s \in R$ and for $r = a$, Thus, σ is a homomorphism fixing R and inducing τ. Further, for any such σ $\overline{\sigma}(a) = \bar{b}$, so by lemma 1o $\sigma(a)$ is determined, whence σ is. If σ is an isomorphism then clearly T is unramified. Suppose $T \supseteq R$ is unramified. Then T is freely generated by $1, b, \ldots, b^{n-1}$, and it follows that σ is an isomorphism.

Corollary 15. Suppose $S \supseteq R$ is unramified. Then the group of automorphisms of L fixing K pointwise is isomorphic to the group of automorphisms of S fixing R pointwise.

Proof: The map $\tau \mapsto \sigma$ of the theorem is readily verified to be a group isomorphism.

This group is in fact the cyclic group of order n, where n is the dimension of L over K (section D.9.6).

The Galois ring $\mathcal{GR}(q, n)$ for a $q = p^r$ a prime power and r, n positive integers may be defined to be the unique unramified extension of $R = \mathcal{Z}_q$, where $K = \mathcal{F}_p$ and $L = \mathcal{F}_{p^n}$. It may be defined in various other ways; see [Bini and Flamini] for a survey.

By the fact that the extension is unramified, the maximal ideal of $\mathcal{GR}(q, n)$ is $p\mathcal{GR}(q, n)$.

Suppose $f \in \mathcal{Z}_q[x]$ is monic of deggree n and $\bar{f}$ is irreducible. Each element of $\mathcal{GR}(q, n)$ has a unique expression as $r_0 + \cdots + r_{n-1}x^{n-1}$ where the r_i are in $\mathcal{Z}_q$. These expressions are added as polynomials. They are multiplied by multiplying as polynomials, and then reducing mod f. The "multiplication table" depends on f, but the ring is the same, up to isomorphism. A polynomial is in the maximal ideal iff all of its coefficients are in $p\mathcal{Z}_q$.

An alternative representation of the elements will be given below.

5. Finite chain rings.

Recall that in a (not necessarily commutative) ring, a unit is an element which has a two-sided multiplicative inverse. It suffices that it have a left inverse and a right inverse; indeed, if $lx = 1$ and $xr = 1$ then $l = lxr = r$. Also recall that a division ring is a ring where every nonzero element has a multiplicative inverse.

Theorem 16. Let R be a ring; the following are equivalent.

1. There is a unique maximal left ideal.
2. There is a unique maximal right ideal.
3. The non-units form a two-sided ideal.

Proof: Let U_L denote the left invertible elements; the argument of theorem D.20.5 can be adapted to show that the following are equivalent.

a. There is a unique maximal left ideal.
b. U_L^c is a left ideal.
c. U_L^c is an additive subgroup.
d. If $x + y = 1$ then either $x \in U_L$ or $y \in U_L$.

Further, in this case U_L^c is the unique maximal left ideal. Assuming this to be the case, adapting the argument of theorem D.16.21 shows that $U_L = U$. It follows that $U_R = U$ also, for if $x \in U_R$ then $xr = 1$ for some r, whence $r \in U_L = U$, whence x is a two-sided inverse for r, and r is a left inverse for x. Thus, U_R^c is an additive subgroup, so by symmetry $U_L^c = U^c = U_R^c$ is the unique maximal right ideal, and is thus a two-sided ideal. Finally, suppose U^c is a two-sided ideal; then if $x + y = 1$, either $x \in U$ or $y \in U$, whence certainly either $x \in U_L$ or $y \in U_L$.

A ring with the properties of the theorem is called local. If M is the ideal of non-units, then R/M is a division ring. This follows similarly to the commutative case (theorem D.6.3): If $x \notin M$ then $1 = lx + m$ where $l \in R$ and $m \in M$, whence $l + I$ is a left inverse for $x + M$ in R/M. Similarly $x + M$ has a right inverse.

Nakayama's lemma, that if M is finitely generated and $[JM] = M$ where $J = \mathrm{Rad}(R)$ then $M = 0$, holds for arbitrary R. Indeed, suppose $\{x_1, \ldots, x_m\}$ is a generating set of M of least size. If $M \neq 0$ then $m > 0$. Since $[JM] = M$, $x_m = j_1x_1 + \cdots + j_mx_m$ where $j_i \in J$, so $(1 - j_m)x_m = j_1x_1 + \cdots + j_{m-1}x_{m-1}$. But since $j_m \in \mathrm{Rad}(R)$ $1 - j_m$ is a unit (lemma D.16.21), which gives a contradiction.

As in the commutative case, if R is local and finite then the ideals M^i where M is the maximal ideal form a strictly descending chain, which is eventually 0.

Theorem 17. Let R be a finite ring; the following are equivalent.

1. The left (right) ideals of R form a chain.
2. R is local, and the maximal left (right) ideal is principal.

Further, if R has these properties, and the maximal left ideal is Ra, then every left ideal is of the form Ra^i for some i; and similarly on the right.

Proof: First we prove 1L⇒2L. Clearly the largest proper left ideal is the unique maximal left ideal; call this M. Suppose $x \in M - M^2$; then $Rx \subseteq M$ and $M^2 \not\subseteq Rx$, so $Rx \subseteq M^2$. If $M^2 \subseteq J \subseteq M$ in R then $0 \subseteq J/M^2 \subseteq M/M^2$ in R/M^2. But $(R/M^2)/(M/M^2) \cong R/M$, which is a division ring (in fact a finite field, by theorem D.14.25), and hence has no nonzero proper left ideals. Since $Rx \neq M^2$, $Rx = M$. Now suppose 2L holds. The action $(r + M)(x + M^2) = rx + M^2$ makes M/M^2 is a vector space over the field R/M. $M = Ra$ for some a; if $a \in M^2$ then $M = 0$, and 1L is trivial, so suppose not. M/M^2 is one dimensional ($a + M^2$ is a basis). The action $(r + M)(x + M^2) = xr + M^2$ makes M/M^2 a vector space over R/M also, which is also one dimensional, so $M = aR$ (since $a + M^2 \neq M^2$). Supposing $M = aR + M^i$ where $i \geq 2$,

$M^i = aR + M^{2i-1}$, so $M = aR + M^{2i-1}$. Since M is nilpotent, $M = aR$ follows. It then follows that $M^i = Ra^i$ for any i. Suppose $r \in Ra^i - Ra^{i+1}$; then $r = ua^i$ where $u \notin M$, and by theorem ?1 u is a unit. It follows that $Rr = Ra^i$, and so every left ideal is Ra^i for some i. This shows that 1L, in fact the stronger property stated at the end of the theorem, holds; also 2R holds. By symmetry, 1R is equivalent to 2R. and 1R implies 2L.

A ring with the properties of the theorem is called a finite chain ring. Note that it is a principal ideal ring. Galois rings have been observed to have property 2 of the theorem, indeed, for $\mathcal{GR}(p^r, n)$, the maximal ideal is $p\mathcal{GR}(p^r, n)$. Thus, a Galois ring is a commutative finite chain ring. Its nonzero ideals are $p^i\mathcal{GR}(p^r, n)$ for $0 \leq i < r$. This was observed in section 3 for $\mathcal{Z}_q$, and can be proved without introducing chain rings; but the more general result sheds additional light on the fact and avoids redundancy.

In the proof of the theorem, it is shown that in a finite chain ring with maximal ideal Ra, every element is of the form ua^i for some i and unit u. In particular, every element of $\mathcal{GR}(p^r, n)$ is of the form up^i, where $0 \leq i < r$ and u is a unit.

The above observations can be used to give an alternative "p-adic" representation of elements of $\mathcal{GR}(q, n)$. Let Σ be a system of representatives of the cosets of the maximal ideal $p\mathcal{GR}(p^r, n)$. Each element $x \in \mathcal{GR}(q, n)$, $x = s_0 + px_1$ where $s_0 \in \Sigma$, in a unique manner. Continuing inductively, $x = s_0 + ps_1 + \cdots + p^{r-1}s_{r-1}$ where each $s_i \in \Sigma$, in a unique manner.

There is a particular choice for Σ which has additional properties. Some preliminary observations are needed.

It follows by Hensel's lemma (lemma D.28.8 and remarks following) that if $f, g, h \in \mathcal{Z}[x]$ are monic, g, h are relatively prime mod p, and $f \equiv gh \bmod p^k$, then there are monic $g', h' \in \mathcal{Z}[x]$ such that $g \equiv g' \bmod p^k$, $h \equiv h' \bmod p^k$, g', h' are relatively prime mod p, and $f \equiv g'h' \bmod p^{k+1}$. Further, g', h' are unique mod p^{k+1}.

Recall that in $\mathcal{F}_{p^n}$, every nonzero element is a root of $x^N - 1$ where $N = p^n - 1$, and $x^N - 1$ factors over $\mathcal{F}_p$ into the monic irreducible polynomials other than x, whose degree d is a divisor of n (section D.9.6). The multiplicative group of $\mathcal{F}_{p^n}$ is cyclic (section D.9.6); a generator is called a primitive element. Among the irreducible factors, some have primitive elements as roots, and are called primitive irreducible polynomials. For example, over $\mathcal{F}^2$,

$$x^{15} - 1 = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1);$$

the first two factors are primitive (see [Lidl and Niederreiter], table C).

By Hensel's lemma, this lifts uniquely to a factorization over $\mathcal{Z}_q$ where $q = p^r$. If f is a factor, where $\bar{f}$ is primitive, and α is a root of $\bar{f}$ in $\mathcal{F}_{p^n}$, then by lemma 13 f has a unique root ξ in $\mathcal{GR}(q, n)$ such that $\bar{\xi} = \alpha$. Note that $\xi^N = 1$ in $\mathcal{GR}(q, n)$. Since $\bar{\xi}$ generates the multiplicative group of $\mathcal{F}_{p^n}$, $\{0, 1, \xi, \xi^2, \ldots, \xi^{N-1}\}$ forms a system of coset representatuives for $p\mathcal{GR}(q, n)$ in $\mathcal{GR}(q, n)$. Further, the map $\alpha^i \mapsto \xi^i$ is an isomorphic embedding of the multiplicative group of $\mathcal{F}_{p^n}$ in $\mathcal{GR}(q, n)$.

In summary, if ξ is as above then each element of $\mathcal{GR}(p^r, n)$ has a unique expression in either of the following two forms.

- $r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}$ where $r_i \in R$.
- $s_0 + ps_1 + \cdots + p^{r-1}s_{r-1}$ where $s_i \in \{0, 1, \xi, \xi^2, \ldots, \xi^{N-1}\}$.

References.

[Bini and Flamini] G. Bini and F. Flamini, *Finite Commutative Rings and their Applications*, Kluwer Academic Publishers, 2002.

[Clark and Drake] W. Clark and D. Drake, "Finite Chain Rings", Abhandlungen Mathematische Seminar University of Hamburg 39 (1973), 147–153.

[Dey and Rajan] B. Dey and B. Rajan, "Affine Invariant Extended Cyclic Codes Over Galois Rings", IEEE Transactions on Information Theory 50 (2004), 691–698.

[Dowd] M. Dowd, *Introduction to Algebra, Topology, and Category Theory*, www.hyperonsoft.com, 2006.

[Hammons et al], A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The Z_4 linearity of Kerdock, Preparata, Goethals and related codes", IEEE Trans. Inform. Theory 40 (1994), 319–1994.

[Honald and Landjev] T. Honald and I. Landjev, "Linear Codes over Finite Chain Rings", preprint.

[Lidl and Niederreiter] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley Publishing Co., 1983.

[MacWilliams and Sloane] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, North Holland, 1977.

[McDonald] B. McDonald, *Finite rings with identity*, Marcel Dekker, 1974.

[Norton and Salagean] G. Norton and A. Salagean, "On the structure of linear and cyclic codes over finite chain rings", Applicable algebra in engineering, communication and computing 10 (2000), 489–506.

[van Lint] H. van Lint, *Introduction to Coding Theory*, Springer, 1999.

[Wood] J. Wood, "Duality for Modules over Finite Rings and Applications to Coding Theory", preprint.