Canad. Math. Bull. Vol. **15** (1), 1972

THE RING SCHEME $\mathbf{F}_q$

BY
IAN G. CONNELL

Let A be a ring(1) and $s_2(A)$ the set of idempotents in A. It is a familiar fact that $s_2(A)$ becomes a ring if we define 0, 1 and multiplication as in A, and a new negative and new addition by

$$\ominus x = x, \qquad x \oplus y = x+y-2xy. \tag{1}$$

R. A. Melter [3] made the surprising observation that $s_3(A)$, where in general $s_q(A)=\{x \in A : x^q=x\}$, is a ring if 2 is a unit in A and we define 0, 1 minus and multiplication as in A, and a new addition by

$$x \oplus y = x+y-\tfrac{3}{2}(x^2y+xy^2). \tag{2}$$

The nonobvious facts are that $s_3(A)$ is closed under $\oplus$ and that $\oplus$ is associative when applied to the elements of $s_3(A)$. The $\oplus$ in (1) is actually a formal group over A, and so is associative when applied to any elements of A. However in (2) (and similarly in other cases we shall define) the $\oplus$ is not a formal group, and the associative law depends on the fact that the elements involved are in $s_3(A)$.

We shall derive these and other examples using the following general considerations, a full account of which can be found in [1, Ch. 1]. If S is a scheme and R is a finite ring with q elements then R_S, the direct sum of q copies of S, represents a (commutative) ring scheme. Hence $\mathrm{Hom}_{\text{scheme}/S}(T, R_S)$ is a ring for each scheme T over S.

In affine language, if Ω is a ring and $\Lambda=\Omega^R$ is the direct product of q copies of Ω, then a ring structure is induced on the set $\mathrm{Hom}_{\Omega\text{-algebra}}(\Lambda, A)$ for each Ω-algebra A.

The case we wish to consider is: $R=GF(q)$, where q is any prime power, and $\Omega=\Omega_q=\mathbf{Z}[1/(q-1), \zeta]$ where ζ is a primitive $(q-1)$st root of unity. We choose a generator g of the multiplicative group $GF(q)^*$ and define a mapping $\chi: GF(q) \to \Omega$ by $\chi(0)=0$ and $\chi(g^i)=\zeta^i$, for $0 \le i \le q-2$. For $x \in GF(q)$ let I_x denote the ideal in $\Omega[X]$ generated by the polynomial $X-\chi(x)$ and put $\Omega_x=\Omega[X]/I_x \cong \Omega$. Since

$$(X-\zeta)(X-\zeta^2)\ldots(X-\zeta^{q-2}) = (X^{q-1}-1)/(X-1),$$

we have

$$(1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{q-2}) = q-1,$$

Received by the editors May 19, 1971.

(1) All rings, and algebras over rings, are commutative with 1, and all ring homomorphisms respect 1.

and therefore each factor on the left is a unit in Ω. It follows that the ideals I_x are comaximal, hence their intersection I is generated by $X^q - X$ and, using the notation

$$\Omega[X]/I = \Lambda = \Omega[\lambda : \lambda^q = \lambda],$$

we see that χ induces an Ω-algebra isomorphism

$$\tilde{\chi} : \Lambda \xrightarrow{\sim} \prod_{x \in GF(q)} \Omega_x$$

given by $\tilde{\chi}(\lambda)_x$ (the x-coordinate of $\tilde{\chi}(\lambda)) = \chi(x)$.

REMARK. If Ω' is a ring and R' is a finite ring we call a mapping $\chi' : R' \to \Omega'$ admissible if

(i) $\chi'(xy) = \chi'(x)\chi'(y)$, and
(ii) when $x \neq y$, $\chi'(x) - \chi'(y)$ is a unit in Ω'.

Under these conditions we obtain an isomorphism $\tilde{\chi}'$ as above. However one easily sees that the existence of such a χ' already implies that R' is a field, say $GF(q)$, and Ω' is an Ω_q-algebra. Moreover if $\rho : \Omega_q \to \Omega'$ is the structural homomorphism then $\chi' = \rho \circ \chi$. Thus our previous discussion really deals with the most general admissible χ.

We denote by $\mathbf{F}_q$ the ring scheme represented by Spec Λ. Clearly $\mathbf{F}_q$ is of order q over Spec Ω.

PROPOSITION. *The structure of* $\mathbf{F}_q$ *is described by the following* Ω*-algebra homomorphisms*:

(*zero*)	$\xi : \Lambda \to \Omega$	*where*	$\xi(\lambda) = 0$;
(*one*)	$\eta : \Lambda \to \Omega$	*where*	$\eta(\lambda) = 1$;
(*minus*)	$\nu : \Lambda \to \Lambda$	*where*	$\nu(\lambda) = (-1)^q\lambda$;
(*multiplication*)	$\mu : \Lambda \to \Lambda \otimes_\Omega \Lambda$	*where*	$\mu(\lambda) = \lambda \otimes \lambda$;
(*addition*)	$\alpha : \Lambda \to \Lambda \otimes_\Omega \Lambda$	*where*	

$$\alpha(\lambda) = \lambda \otimes 1 + 1 \otimes \lambda + \sum_{i=1}^{q-1} a_i \lambda^i \otimes \lambda^{q-i},$$

$a_1 = a_{q-1} = -q/(q-1)$ *and for* $2 \leq i \leq q-2$

$$a_i = \frac{1}{q-1} \sum_{s=1}^{q-1} \chi(g^{is} + g^{(i-1)s}).$$

Proof. With Ω fixed and E any set, Ω^E gives a contravariant functor from sets to Ω-algebras. Namely, if $\phi : E \to F$ is a mapping of sets then $\Omega^F \to \Omega^E$ is given by $a \mapsto b$ where $(b)_e = (a)_{\phi(e)}$. Now the zero element of $R = GF(q)$ is given by $\bar{\xi} : \text{pt.} \to R$ where pt. denotes a one-element set and the image of $\bar{\xi}$ is $\{0\}$. The induced homomorphism

$$\prod_{x \in R} \Omega_x = \Omega^R \to \Omega^{\text{pt.}} = \Omega$$

https://doi.org/10.4153/CMB-1972-015-5 Published online by Cambridge University Press

is the projection onto the 0-coordinate. Via $\tilde{\chi}$ this gives $\xi: \Lambda \to \Omega$ where $\xi(\lambda)=0$. Similarly η and ν are determined.

For μ and α we use the canonical isomorphism $\Omega^R \otimes_\Omega \Omega^R \xrightarrow{\sim} \Omega^{R\times R}$ where $a \otimes b \mapsto c$ and the (x, y) coordinate of c is $(c)_{x,y}=(a)_x(b)_y$. The case of μ is clear and the verification of the formula for α is an easy calculation(2).

Since $\mathrm{Hom}_{\Omega\text{-algebra}}(\Lambda, A)=s_q(A)$ (via the bijection $\phi \mapsto \phi(\lambda)$) we have:

COROLLARY. *For each prime power q, and for each Ω-algebra A, $s_q(A)$ is a ring if we define* 0, 1 *and multiplication as in A and a new negative and new addition by*

$$\ominus x = (-1)^q x,$$
$$x \oplus y = x+y+\sum_{i=1}^{q-1} a_i x^i y^{q-i},$$

where the a_i are interpreted as elements of A via the structural homomorphism $\Omega \to A$.

Here are the first few examples:

$$q=2:\quad x\oplus y = x+y-2xy;$$
$$q=3:\quad x\oplus y = x+y-\tfrac{3}{2}(xy^2+x^2y);$$
$$q=4:\quad x\oplus y = x+y-\tfrac{4}{3}(xy^3+x^3y)+\tfrac{2}{3}x^2y^2;$$
$$q=5:\quad x\oplus y = x+y-\tfrac{5}{4}(xy^4+x^4y)+\frac{1+2\sqrt{-1}}{4}(x^2y^3+x^3y^2);$$
$$q=7:\quad x\oplus y = x+y-\tfrac{7}{6}(xy^6+x^6y)+\frac{-5+\sqrt{-3}}{12}(x^2y^5+x^5y^2)$$
$$+\frac{2+\sqrt{-3}}{6}(x^3y^4+x^4y^3);$$
$$q=8:\quad x\oplus y = x+y-\tfrac{8}{7}(xy^7+x^7y)+\frac{-1+\sqrt{-7}}{7}(x^2y^6+x^6y^2)$$
$$+\frac{5-\sqrt{-7}}{14}(x^3y^5+x^5y^3)-\frac{1+\sqrt{-7}}{7}x^4y^4;$$
$$q=9:\quad x\oplus y = x+y-\tfrac{9}{8}(xy^8+x^8y)+\frac{1-2\sqrt{-2}}{8}(x^2y^7+x^7y^2)$$
$$-\tfrac{3}{8}(x^3y^6+x^6y^3)+\frac{-1+2\sqrt{-2}}{8}(x^4y^5+x^5y^4).$$

We gather some simple facts in a proposition.

PROPOSITION. *Let $q=p^n$, p prime, and $\Omega=\Omega_q$.*

(i) *For every scheme S over* Spec Ω, $h(S)=\mathrm{Hom}_{\text{scheme/Spec}\,\Omega}(S, \mathrm{Spec}\,\Lambda)$ *is a ring of characteristic p.*

(ii) *h is idempotent in the following sense: $h(S)$ is canonically an Ω-algebra and there is a canonical ring isomorphism $h(\mathrm{Spec}\,h(S)) \cong h(S)$.*

(2) I am indebted to Professor J. Tate for pointing out to me that $\mathbf{F}_q$ is a constant ring scheme; originally I had verified the ring scheme axioms directly.

https://doi.org/10.4153/CMB-1972-015-5 Published online by Cambridge University Press

(iii) *The coefficients a_i lie in the subfield of* $\mathbf{Q}(\zeta)$ *left fixed by the Frobenius automorphism of* $\mathbf{Q}(\zeta)/\mathbf{Q}$ *attached to* p.

(iv) *For every* i *in the range* $2 \leq i \leq q-2$, $(q-1)a_i$ *has absolute value* $\sqrt{q}$.

Proof. Because $\mathbf{F}_q$ is a ring scheme, the structural homomorphism $\rho: S \to \operatorname{Spec} \Omega$ induces a ring homomorphism $h(\rho): h(\operatorname{Spec} \Omega) \to h(S)$. But the former ring is $GF(q)$, which proves (i).

Definining $\Omega \to GF(q)$ by $\zeta \mapsto g$ and composing this with $h(\rho)$ gives a homomorphism $\omega: \Omega \to h(S)$; $h(S)$ thus becomes an Ω-algebra. Now

$$h(S) = \operatorname{Hom}_{\Omega\text{-algebra}}(\Lambda, A)$$

where $A = \Gamma(S, O_S)$, so $h(S) = s_q(A)$ with the ring operations as defined in the previous corollary([3]). As sets, $s_q(s_q(A)) = s_q(A)$ and (ii) amounts to verifying that the ring operations are the same. Only the case of addition causes any concern, and the result follows from $\omega(a_1) = \omega(a_{q-1}) = 0$, by (i), and

$$\omega(a_i) = \frac{1}{q-1} \sum_{s=1}^{q-1} (g^{is} + g^{(i-1)s}) = 0,$$

for $2 \leq i \leq q-2$.

The Frobenius automorphism σ is given by $\sigma(\zeta) = \zeta^p$. Thus, for $2 \leq i \leq q-2$,

$$\sigma(a_i) = \frac{1}{q-1} \sum_{s=1}^{q-1} \chi((g^{is} + g^{(i-1)s})^p) = \frac{1}{q-1} \sum_{s=1}^{q-1} \chi(g^{ips} + g^{(i-1)ps}) = a_i$$

since ps runs through the integers mod $q-1$ as s does, and this proves (iii).

To prove (iv) we use the Gauss sum

$$\tau(\psi) = \sum_{x \in GF(q)} \psi(x) e(x)$$

where ψ is any nontrivial character on $GF(q)^*$ ($\psi(0) = 0$), $e(x) = \exp(2\pi i S(x)/p)$ and S denotes the trace from $GF(q)$ to $GF(p)$. As in [2] one calculates $\overline{\tau(\psi)}\, \tau(\psi) = q$ and $\tau(\bar{\psi})\tau(\psi) = \psi(-1)q$ where the bar denotes complex conjugate. (Extending from the case $q = p$ in [2] to $q = p^n$ presents no difficulties.) One easily sees that

$$\begin{aligned}(q-1)a_i &= (-1)^{qi} \sum_{x \in GF(q)} \bar{\chi}^i(x)\chi(1-x) \\ &= (-1)^{qi} \pi(\bar{\chi}^i, \chi),\end{aligned}$$

and again as in [2] one finds that

$$\pi(\psi, \chi) = \frac{\tau(\psi)\tau(\chi)}{\tau(\psi\chi)}$$

([3]) Because $\Lambda = \Omega^q$, $h(S)$ can also be identified with the set of ordered q-tuples of mutually orthogonal idempotents in A with sum 1; in terms of S, these correspond to ordered q-tuples $(S_1, \ldots, S_q)$ of closed subschemes (some of which may be empty) which are mutually disjoint and whose union is S.

(when none of ψ, χ, $\psi\chi$ is the trivial character). Since each of the τ's has absolute value $\sqrt{q}$, the result follows.

The $\pi(\psi, \chi)$ are known as Jacobi sums. Since χ is a generator of the character group of $GF(q)^*$, the general Jacobi sum is $\pi(\chi^i, \chi^j)$ where i and j are integers mod $q-1$.

(We define $\chi^i(0)=0$ even when $i\equiv 0 \bmod q-1$ as in [4]; in [2], $\chi^0(0)$ is defined to be 1 and therefore there is a slight discrepancy between our π's and those in [2] when $ij\equiv 0 \bmod q-1$.) Let $x \in GF(q)^*$ and for $s=1, 2, \ldots, q-1$ define

$$\chi^s(1+x) = a(s, 1)\chi(x)+a(s, 2)\chi^2(x)+\cdots+a(s, q-1)\chi^{q-1}(x).$$

(If $x=g^u$ this is just

$$\begin{aligned}(\zeta^u \oplus 1)^s &= (\zeta^u+1+a_1\zeta^u+\cdots+a_{q-1}\zeta^{(q-1)u})^s \\ &= a(s, 1)\zeta^u+\cdots+a(s, q-1)\zeta^{(q-1)u};\end{aligned}$$

thus $a(1, t)=a_t$ for $2\le t\le q-2$ and $a(1, t)=a_t+1=-1/(q-1)$ when $t=1, q-1$ except that $a(1, 1)=a_1+2=0$ when $q=2$.)

For $1\le t\le q-1$, multiplying by $\chi^{-t}(x)$ and adding over x we obtain

$$\begin{aligned}a(s, t) &= \frac{1}{q-1}\sum_{x\in GF(q)}\chi^s(1+x)\chi^{-t}(x) \\ &= \frac{1}{q-1}\chi^{-t}(-1)\sum_{x\in GF(q)}\chi^s(1-x)\chi^{-t}(x) \\ &= \frac{(-1)^{qt}}{q-1}\pi(\chi^s, \chi^{-t}).\end{aligned}$$

We should mention Stickelberger's formula (cf. [4, p. 490]): Let P be a prime ideal in $\mathbf{Z}[\zeta]$ lying over p (where q is a power of p) such that in the isomorphism $\mathbf{Z}[\zeta]/P\cong GF(q)$, ζ corresponds to g. Then, provided $s\not\equiv t \bmod q-1$, the ideal generated by $(q-1)a(s, t)$ in $\mathbf{Z}[\zeta]$ has the prime ideal factorization

$$((q-1)a(s, t)) = (\pi(\chi^s, \chi^{-t})) = P^{w(s,t)}$$

where $w(s, t)$ is the following element in the group ring $\mathbf{Z}[G]$, $G=\mathrm{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q})$:

$$w(s, t) = \sum_{\substack{i \bmod q-1 \\ (i, q-1)=1}}\left(\left[\frac{i(t-s)}{q-1}\right]-\left[\frac{it}{q-1}\right]-\left[\frac{-is}{q-1}\right]\right)\sigma_i^{-1},$$

where square brackets denote the integral part and $\sigma_i \in G$ is defined by $\sigma_i(\zeta)=\zeta^i$. (The exceptional cases are: $a(s, s)=-1/(q-1)$ for $1\le s\le q-2$, $a(q-1, q-1)=(q-2)/(q-1)$.)

If $q=p^n$, $\mathrm{Gal}\,(GF(q)/GF(p))$ consists of the elements σ^j, $1\le j\le n$ where $\sigma(x)=x^p$. It is easily seen that the ring scheme morphism $\mathbf{F}_q \to \mathbf{F}_q$ induced by σ^j is described by the Ω-algebra homomorphism $\Lambda \to \Lambda$ given by $\lambda \mapsto \lambda^{p^j}$.

Now let $\alpha: GF(q) \to GF(q^n)$ and $\beta: \Omega_q \to \Omega_{q^n}$ be ring inclusions, and let $\mathbf{F}'_q$ denote the ring scheme obtained from $\mathbf{F}_q$ by extending the base to Spec Ω_{q^n}; $\mathbf{F}'_q$ is represented by $\Lambda'_q = \Omega_{q^n}[\lambda' : \lambda'^q = \lambda']$. Then α induces a morphism $\mathbf{F}'_q \to \mathbf{F}_{q^n}$. If we impose the natural compatibility condition that

$$\begin{array}{ccc} GF(q) & \xrightarrow{\alpha} & GF(q^n) \\ \downarrow & & \downarrow \\ \Omega_q & \xrightarrow{\beta} & \Omega_{q^n} \end{array}$$

commute, where the vertical maps are the chosen χ's, this morphism is described by the Ω_{q^n}-algebra homomorphism $\Lambda_{q^n} \to \Lambda'_q$ given by $\lambda \mapsto \lambda'$; again we omit the simple verification.

For example, the addition law for $q=9$ given above collapses to the law for $q=3$ if we impose the relations $x^3 = x$, $y^3 = y$. (The above compatibility condition is automatically satisfied as far as the list goes.)

We conclude with some examples showing how the above ideas can be extended, leading in general to nonconstant ring schemes. First of all, $\mathbf{F}_q$ can be regarded over Spec Ω' where $\Omega' = \mathbf{Z}[1/(q-1), a_1, \ldots, a_{q-1}]$ and part (iii) of the previous proposition shows that in general this ring is smaller than Ω. For example, our definitions give $s_4(A)$ a ring structure for all algebras A over $\mathbf{Z}[\frac{1}{3}]$. However there are examples such as the following which are not explained in this way. $A = \mathbf{Z}/10\mathbf{Z}$ is not an algebra over $\Omega_3 = \mathbf{Z}[\frac{1}{2}]$, yet $s_3(A) = \{0, 1, 4, 5, 6, 9 \bmod 10\}$ is a ring, indeed the ring $\mathbf{Z}/6\mathbf{Z}$, if we define

$$x \oplus y = x + y + x^2y + y^2x.$$

To take the simplest case, suppose we set $\Omega = \mathbf{Z}[a, b]$ and $\Lambda = \Omega[\lambda]$ with relations among a, b, λ to be determined so that Ω is a subring of Λ and, with $\nu(\lambda) = b\lambda$, $\alpha(\lambda) = \lambda \otimes 1 + 1 \otimes \lambda + a\lambda \otimes \lambda$ and ξ, η, μ as before

(i) the ring scheme axioms are satisfied, and
(ii) $\xi, \ldots, \alpha$ are Ω-algebra homomorphisms.

The axiom for left negatives, namely the commutativity of the diagram

$$\begin{array}{ccccc} \Lambda & \xrightarrow{\alpha} & \Lambda \otimes_\Omega \Lambda & \xrightarrow{\nu \otimes 1} & \Lambda \otimes_\Omega \Lambda \\ {\scriptstyle \xi}\downarrow & & & & \downarrow{\scriptstyle \text{diag.}} \\ \Omega & & \xrightarrow[\text{canon.}]{} & & \Lambda \end{array}$$

gives $\lambda + b\lambda + ab\lambda^2 = 0$; similarly the left distributive law gives $a(\lambda^2 - \lambda) \otimes \lambda \otimes \lambda = 0$ or, applying $1 \otimes \eta \otimes \eta$, $a(\lambda^2 - \lambda) = 0$. (The remaining axioms are automatically satisfied.) Substituting $a\lambda^2 = a\lambda$ in the first equation we have $\lambda(1 + b + ab) = 0$ which is equivalent, via η, to $1 + b + ab = 0$; in particular b is a unit. Now in order that ν be a homomorphism we must have $a(b^2\lambda^2 - b\lambda) = 0$ which, in view of above facts,

is equivalent with $b=-1-a$ and $(a+1)^2=1$. The remaining mappings ξ, η, μ, α are seen to be homomorphisms and we finally arrive at:

$$\Omega = \mathbf{Z}[a:(a+1)^2 = 1], \qquad \Lambda = \Omega[\lambda:a\lambda^2 = a\lambda].$$

If A is an Ω-algebra then

$$\mathrm{Hom}_{\Omega\text{-algebra}}(\Lambda, A) = \{x \in A:\bar{a}x^2 = \bar{a}x\}$$

(where $\bar{a}$ denotes the image of a in A) has a ring structure. For example, if $\bar{a}=0$ we obtain the original ring; and if $\bar{a}=-2$ we obtain the ring of elements which are idempotent mod 2.

Here is a final example. Let

$$\Omega = \mathbf{Z}[a:4a = 2], \qquad \Lambda = \Omega[\lambda:(2a-1)(\lambda^2+\lambda) = 0, \lambda^3 = \lambda]$$

and let A be an Ω-algebra. Then

$$\mathrm{Hom}_{\Omega\text{-algebra}}(\Lambda, A) = \{x \in A:(2\bar{a}-1)(x^2+x) = 0, x^3 = x\}$$

is a ring if we define 0, 1, $-$ and multiplication as in A, and a new addition

$$x \oplus y = x+y+(\bar{a}-2)(x^2y+xy^2).$$

This includes the original case $s_3(A)$, where $\bar{a}=\frac{1}{2}$, and the example $s_3(\mathbf{Z}/10\mathbf{Z})$ mentioned earlier, where $\bar{a}=3 \bmod 10$. The characteristic of this ring is 2, 3 or 6 when, respectively, $2=0$ in A, 2 is a unit in A, otherwise.

References

1. M. Demazure and A. Grothendieck, *Schémas en Groupes*, Fasc. 1, Séminaire de Géométrie Algébrique, Inst. Hautes Études Sci. Publ. Math., Paris, 1963.

2. H. Hasse, *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin, 1950.

3. R. A. Melter, *Problem for solution No. 104*, Canad. Math. Bull. (5) **8** (1965), p. 669.

4. A. Weil, *Jacobi Sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **73** (1952), 487–495.

McGill University,
Montreal, Quebec