

Inhaltsverzeichnis

1. Einleitung	1
2. Darstellung und Arithmetik endlicher Körper	3
2.1. Faktorringe	4
2.2. Matrizen	6
2.3. Implementierung der Arithmetik von $\mathbb{K}_{13^2}$ für den Prozessor dsPIC33	11
2.4. Primitive Elemente	20
2.5. Implementierung der Arithmetik von $\mathbb{K}_{2^8}$ für AVR	24
3. Bestimmung irreduzibler Faktoren von Polynomen über endlichen Körpern	29
3.1. Die einfachste Methode: Division mit allen möglichen Teilern	29
3.2. Ein Verfahren basierend auf den Teilern von $X^{q^n} - X$	30
3.3. Das Verfahren von Berlekamp	33
4. Lineare Codes	43
4.1. Lineare Codes als Exakte Sequenzen	44
4.2. Einfache lineare Codes	45
4.3. Die Fehlermetrik	49
4.4. Lineare Codes auf Polynombasis	53
4.4.1. Lineare Codes mit Generator- und Paritätsprüfungspolynom	55
4.4.2. Implementierung eines binären Codes für AVR	61
4.4.3. Lineare Codes mit Nullstellen des Erzeugerpolynoms	70
4.5. Zyklische Codes	80
4.6. Generatorpolynome für vier Informationsbit	87
4.7. Generatorpolynome für acht Informationsbit	91
5. Polynomarithmetik und lineare Gleichungssysteme mit AVR	95
5.1. Arithmetik in $\mathbb{K}_2[X]$	97
5.1.1. Addition	98
5.1.2. Multiplikation	102
5.1.3. Division	126
5.1.4. Der größte gemeinsame Teiler	169
5.2. Lösung linearer Gleichungssysteme mit Koeffizienten in $\mathbb{K}_{2^8}$	173
6. Algebraische Grundlagen	191
6.1. Kongruenzrelationen und Teilbarkeit	192
6.2. Primzahlen I	214
6.3. Ringe	223
6.3.1. Die Ringaxiome	223
6.3.2. Teilringe	229

6.3.3. Ringhomomorphismen	231
6.3.4. Konstruktion von Ringen mit der Teilerrestfunktion	238
6.4. Primzahlen II	245
6.5. Integritätsbereiche und Körper	250
6.6. Teilbarkeit in Ringen	259
6.7. Polynome I	268
6.8. Euklidische Ringe	277
6.9. Polynome II	294
6.10. Vektorräume	307
6.10.1. Untervektorräume	309
6.10.2. Freie und erzeugende Vektorfamilien	311
6.10.3. Körperwechsel	318
6.10.4. Vektorraumhomomorphismen	321
6.10.5. Der Faktorraum	325
6.10.6. Exakte Sequenzen	332
6.10.7. Dualer Vektorraum und dualer Homomorphismus	335
6.10.8. Lineare Abbildungen und Matrizen	339
6.10.9. Lineare Gleichungssysteme	346
6.10.10. Die Matrix von VANDERMONDE	356
6.11. Blockmatrizen	358
6.12. Konstruktion von Ringen und Körpern mit Polynomkongruenzen	361
6.13. Primitive Elemente endlicher Körper	384
6.14. Klassifizierung endlicher Körper	393
6.15. Polynome III	397
6.16. Äquivalenzrelationen	402
6.17. Ideale	407
A. Anhang	423
A.1. Die Bestimmung der Minimalpolynome über $\mathbb{K}_q$ von Elementen aus $\mathbb{K}_{q^m}$	423
A.2. Der Körper $\mathbb{K}_{2^4}$	425
A.3. Der Körper $\mathbb{K}_{2^8}$	426
A.4. Fehlerlokalisierungspolynome	431
A.5. Binäre modulare Potenzierung	432
A.6. AVR-Nomenklatur und AVR-Makros	433
Literaturverzeichnis	437
Index	439