# Examen Algebra I 2015-2016

**Theorie** (je krijgt één van de volgende vragen)(de bijvraag krijg je terwijl je vooraan staat

### Vraag A

1. Geef de definitie van een irreducibel en een priemelement (p. 75). Toon aan dat elk priemelement irreducibel is.
2. Bewijs stelling 2.7.14 (p.78).
3. Zij $R = \mathbb{Z}[\sqrt{-13}]$. Bepaal de eenheden van $R$ (opl: 1 en -1, via de normafbeelding $\mathsf{N}$). Bewijs dat $R$ geen UFD is. Beschouw hiertoe het element 2 en bewijs dat dit een irreducibel element is dat niet priem is (opl: $2|14 = (1-\sqrt{-13})(1+\sqrt{-13})$ en via de normafbeelding kan je nagaan dat 2 geen deler is van $1 \pm \sqrt{-13}$).

Bijvraag: Bewijs dat de puntsgewijze stabilisator van een deelverzameling $T$ van $S$ (we beschouwen de actie van $G$ op $S$) een normaaldeler is van de globale stabilisator van $T$.

### Vraag G18

1. Bewijs puntje 2b en 3 van de stellingen van Sylow.
2. Hoeveel Sylow-5-deelgroepen zijn er in $\mathbf{S}_6$?

Bijvraag: Verklaar: $\mathbb{Z}$-modulen en abelse groepen zijn equivalente begrippen. (3.1.4.2, p.88)

### Vraag G?

1. Bewijs puntje 2b van de stellingen van Sylow.
2. Hoeveel Sylow-2-deelgroepen zitten er in $\mathbf{D}_{20}$?

Bijvraag: Bewijs dat elke ring maximale idealen heeft. (p.71)

### Vraag G16

1. Bewijs puntje 1 van de stellingen van Sylow.
2. Zij $G = S_4$ en $P$ een Sylow-2-deelgroep van $G$, bewijs dat $P$ isomorf is met $\mathbf{D}_8$.

### Vraag G?

1. Bewijs puntje 2b en 4 van de stellingen van Sylow.
2. $G$ is een enkelvoudige groep. Bewijs dat elke 2 Sylow-p-deelgroepen triviaal snijden.

Bijvraag: Bewijs: Elk Euclidisch domein is een PID.

### Vraag R4

1. Definieer een Euclidisch domein. (p.63)
2. Bewijs: elk Euclidisch domein is een PID.
3. Bewijs: $\mathbb{Z}[i]$ is een Euclidisch domein.
4. Bewijs dat 7 een priemelement is in $\mathbb{Z}[i]$. (opl: Elk Euclidisch domein is een UFD, dus een irreducibel element is ook een priemelement. Stel $7 = x * y$. Gebruik de normafbeelding: $\mathsf{N}(7) = 49 = \mathsf{N}(x)\mathsf{N}(y)$. De enige mogelijkheden zijn dan ontbinding in $7 * 7$ of $49 * 1$. $7 * 7$ kan niet want $\mathsf{N}(a + bi) = 7 \iff a^2 + b^2 = 7$, wat niet kan met $a, b \in \mathbb{Z}$, dus $x$ of $y$ heeft norm 1 en is dus een eenheid.

Bijvraag: Stel $G, H$ groepen met $|G| = 2013$ en $|H| = 2014$. Hoeveel morfismen zijn er van $G$ naar $H$? (opl: Stel dat $f$ zo'n morfisme is, dan is $\frac{|G|}{|ker(f)|}$ een deler van $|H|$ (isomorfiestelling). Aangezien $\gcd(|G|, |H|) = 1$, moet $|ker(f)| = 2013$ en dus is er slechts één morfisme mogelijk, namelijk alles wordt op 1 afgebeeld)

### Vraag M?

Zij $R$ een PID.

1. Bewijs stelling 3.5.1.
2. Zij $M$ het $R$-moduul $R/(d)$. Bewijs dat $M$ niet projectief is. Doe dit door te bewijzen dat de natuurlijke surjectie $\pi : R \to M$ geen sectie heeft.
3. Bewijs hieruit dat elk eindig voortgebracht projectief $R$-moduul vrij is.

Bijvraag: Wat weet je over abelse enkelvoudige groepen?

### Vraag M12

Zij $R$ een PID.

1. Geef de definitie van een vrij moduul en van een projectief moduul.
2. Bewijs dat een deelmoduul van een vrij moduul ook weer een vrij moduul is.
3. Geef een voorbeeld van een oneindig voortgebracht $R$-moduul.
4. Toon aan dat elk eindig voortgebracht projectief $R$-moduul vrij is.

Bijvraag: Hoeveel groepen zijn er op isomorfisme na van orde 6?

### Vraag G14

Beschouw de actie van een groep $G$ op een verzameling $S$.

1. Bewijs de baanformule.
2. Zij $H$ een deelgroep van $G$ die transitief werkt op $S$. Bewijs dat voor een vaste $s \in S$ geldt dat $G = G_s H$.
3. Geef een voorbeeld van een oneindige groep $G$ die werkt op een verzameling $S$ op zo'n manier dat er voor elke natuurlijke $n > 0$ geldt dat er een baan $s^G$ is met $|s^G| = n$.

Bijvraag: Geef een voorbeeld van een domein dat geen PID is.

### Vraag R18

1. Zij $R$ een ring en $I, J$ twee idealen die copriem zijn in $R$. Bewijs dat $IJ = I \cap J$.
2. Geldt bovenstaande stelling ook als $I$ en $J$ niet copriem zijn? Indien ja, bewijs. Indien nee, geef een tegenvoorbeeld.
3. Zij $R$ een ring en $I, J$ twee idealen die copriem zijn in $R$. Bewijs dat $R/IJ$ isomorf is met $R/I \times R/J$.
4. Bewijs dat $\mathbb{R}[x]/(x^2+a)$ isomorf is met $\mathbb{C}$ als $a > 0$ en met $\mathbb{R}\times\mathbb{R}$ als $a < 0$. Bewijs dat $\mathbb{R}[x]/(x^2)$ niet isomorf kan zijn met $\mathbb{C}$ en ook niet met $\mathbb{R} \times \mathbb{R}$.

Bijvraag: Wat kan je zeggen over enkelvoudige, abelse groepen?

### Vraag G1

1. Zij $G$ een willekeurige groep, $A$ en $B$ normaaldelers in $G$ en $A \cap B = 1$. Bewijs dat $AB$ een normaaldeler is in $G$ en dat $AB$ isomorf is met $A \times B$.
2. Bewijs dat $\mathbf{C}_{31} \times \mathbf{C}_{65}$ isomorf is met $\mathbf{C}_{2015}$.
3. Bewijs dat $\mathbf{C}_{20} \times \mathbf{C}_{15}$ niet isomorf is met $\mathbf{C}_{300}$.
4. Hoeveel abelse groepen van orde 2015 zijn er (op isomorfisme na)?

Bijvraag: Geef een voorbeeld van een domein dat geen PID is.

## Oefeningen

### Vraag 1

**Stelling.** *Zij $G$ een groep zodat $[G : \mathbf{Z}(G)] = n < \infty$. Dan is $|G'| < \infty$.*

*Bewijs.* Zij $D = \{[g,h] | g,h \in G\}$. Vermits $|G/\mathbf{Z}(G)| = n$, is $|D| \le n^2$.[**1**] We beweren dat een willekeurig element van $G'$ kan geschreven worden als product van hoogstens $\square$[**2**] elementen van $D$. Beschouw daartoe een willekeurige $g \in G'$ en schrijf deze als $g = d_1 d_2 \ldots d_i$ met $i$ minimaal. Indien $i > \square$ dan moet een element $d \in D$ minstens $n+1$ keer voorkomen in dit product. Omwille van de identiteit

$$uvw = uwv^w$$

kan $g$ dan ook met evenveel commutators herschreven worden terwijl $d^{n+1}$ erin voorkomt. Stel dat $d = [x,y]$, dan is $[x,y]^n \in \mathbf{Z}(G)$[**3**] zodat

$$\begin{aligned} d^{n+1} &= y[x,y]^n y^{-1}[x,y] = y[x,y]^{n-1}[x,y]y^{-1}[x,y] \\ &= y[x,y]^{n-1}x^{-1}y^{-1}xyy^{-1}x^{-1}y^{-1}xy \\ &= y[x,y]^{n-1}x^{-1}y^{-2}xy^2y^{-1} \\ &= y[x,y]^{n-1}[x,y^2]y^{-1} \end{aligned}$$

Dit bewijst dat $d^{n+1}$ een product is van $n$ commutators. [**4**] Dit bewijst onze bewering [**5**] en besluit het bewijs. [**6**] $\square$

[**1**] Hoe volgt $|D| \le n^2$?

[**2**] Wat moet je invullen in $\square$ om hier iets zinvol van te maken?

[**3**] Waarom is $[x,y]^n \in \mathbf{Z}(G)$?

[**4**] Waarom is het rechterlid een product van $n$ commutators?

[**5**] Welke bewijsstrategie wordt hier impliciet toegepast?

[**6**] Geef een concrete bovengrens voor $|G'|$.

## Vraag 2

Beschouw een groep $G$ met deelgroepen $H, K \le G$ zodat $G = HK$. Toon aan:

1. Er bestaat een $Q \in \mathrm{Syl}_p(G)$ zodat $Q \cap H \in \mathrm{Syl}_p(H)$.
   [Analoog bestaat $R \in \mathrm{Syl}_p(G)$ zodat $R \cap K \in \mathrm{Syl}_p(K)$.]
2. Er bestaat een $P \in \mathrm{Syl}_p(G)$ zodat $P \cap H \in \mathrm{Syl}_p(H)$ én $P \cap K \in \mathrm{Syl}_p(K)$.
3. Voor die $P$ geldt: $P = (P \cap H)(P \cap K)$.

## Vraag 3

Beschouw een commutatieve ring met eenheid $R \neq 0$. Zij $S = \{x \in R | x^2 = x\}$. Beschouw verder de bewerking $u \oplus v := u + v - 2uv$.

1. Bewijs dat $(S, \oplus, \cdot)$ een commutatieve ring met eenheid is.

2. Bewijs dat $S^{\times} = \{1\}$ en $1 \oplus 1 = 0$.
3. Bewijs dat elk priemideaal in $S$ index 2 heeft.
4. Toon aan dat als $R$ een eindig aantal idempotenten heeft, dit aantal een macht van 2 is.
5. Geef de idempotente elementen in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

**Vraag 4**

Zij $R$ een ring en $A, B$ twee $R$-modulen.

1. Toon aan dat $\mathrm{Hom}(A, B)$ op natuurlijke wijze de structuur van een $R$-moduul heeft. (Definieer optelling en scalaire vermenigvuldiging en kies twee axioma's uit om na te gaan.)
2. Zij $\varphi : A \to B$ een morfisme en $X$ een derde $R$-moduul, toon dan aan dat
$$\Phi_X : \mathrm{Hom}(X, A) \to \mathrm{Hom}(X, B) : u \mapsto \varphi \circ u$$
een morfisme van $R$-modulen is.
3. Geef bewijs of tegenvoorbeeld: als $\varphi$ injectief is, dan is $\Phi_X$ injectief voor elk $R$-moduul $X$.
4. Geef bewijs of tegenvoorbeeld: als $\varphi$ surjectief is, dan is $\Phi_X$ surjectief voor elk $R$-moduul $X$.